Protocol Bundle 1.140.0

Release Notes

Revision History

Revision

Document revision	Document reference	Date
1.0	Q14T2104	09/01/2015

Legal Notice

Table of Contents

1. Protocol Bundle 1.140.0

1.1. What's new in the Protocol Bundle 1.140.0

1.1.1. Major enhancements in this release

15 new Protocols added, 2 deprecated. See Section 1.2, “Protocol Updates”

24 new Event Attributes added, 10 modified. See Section 1.3, “Attributes”

Summary of major enhancements :

- Added classification for the OnLive gaming application (cloud gaming), for the Vine video streaming platform, and for the Mypocket mobile application (cloud storage),
- Added support for the last versions of Teamviewer,
- Improved classification coverage of the 050plus VoIP application,
- New metadata was added in the http plug-in (headers, proxy detection), in the amqp and dhcp protocol plug-ins.

Note:

- For “source” customers: http-host only signatures were moved to “pdata/pdd/http_upper”, and the deprecated ones to “pdata/pdd/deprecated”.
- For ixE 4.19.0 users: advanced packet fragmentation support for HTTP (classification and metadata) needs ixE 4.19.1 to be fully supported.
- For ixE 4.19.x users: do not hook all the attributes of the http plug-in when using the Qosmos Flow Manager for packet offloading.

1.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.
- ixEngine 4.19.x versions 4.19.0-20 and higher.

1.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

1.1.4. Supported Platforms

1.1.4.1. Complete Protocol Bundle

The Complete version of the Protocol Bundle has been validated on the following Platforms :

x86 platforms

- x86 32-bit User mode LSB 3.x and 4.x, AMP and SMP
- x86 64-bit User mode LSB 3.x and 4.x, AMP and SMP
- x86 32-bit FreeBSD 9, AMP and SMP, with an External Flow Manager
- x86 64-bit FreeBSD 9, AMP and SMP, with an External Flow Manager
- x86 64-bit FreeBSD 8, SMP, with an External Flow Manager
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 64-bit Windows SMP with an External Flow Manager
- x86 64-bit Darwin SMP with an External Flow Manager

Specific high-performance platforms

- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium Networks OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium Networks OCTEON II CN68XX - SDK version 2.3
- Broadcom MIPS 32
- Power PC e500v2 - Freescale SDK 1.2
- Tilera TILE-Gx, Linux 64-bit AMP - MDE version 4.0.0

1.1.4.2. Classification Protocol Bundle

The Classification version of the Protocol Bundle has been validated on the following Platforms:

64-bit

- Octeon2 Cavium SE - SMP, with an External Flow Manager

- Octeon2 Linux - SMP, with an External Flow Manager
- x86 LSB - AMP, with an External Flow Manager
- x86 LSB - SMP, with an External Flow Manager

32-bit

- PPC e500v2 Linux - AMP, with an External Flow Manager

1.2. Protocol Updates

1.2.1. New Protocols

The following new protocols have been added in this version:

Table 1. New protocols added in this version

Proto ID	Protocol	Description
2437	ccproxy	CCProxy is a windows based software proxy.
2449	cedexis	Cedexis provides analytics solutions for CDN and Clouds services.
2438	distcc	Distributed C Compiler protocol.
2450	filerio	FileRIO is a file sharing service. (http://www.filerio.in)
2451	hootsuite	Hootsuite is a social media management system.
2439	java_rmi	Classifies the Java Remote Method Invocation (RMI) protocol.
2440	lava_lava	Lava Lava is a Chinese language based Instant Messaging application.
2445	mixpanel	Mixpanel provides advertising services for mobile platforms.
2452	mypocket	My Pocket is a service that enables the user to send his smartphone data into the personal cloud. Data storage and sharing among users form part of the services provided. On the smartphone, there's an application to manage photos, videos, address book, and can be accessed via the WEB browser from a computer over the internet.
2442	onlive	Onlive is a platform of cloud gaming.
2441	sip_soap	SIP-SOAP is an extension to the standard SIP protocol allowing for SOAP messages to be passed over a SIP connection.
2446	smartadserver	Smart AdServer provides advertising services.
2447	tanx	Taobao Ad Network and Exchange provides advertising services.
2448	videosz	Porn content website.
2444	vine	Vine is a short-form video sharing service.

1.2.2. Deprecated Protocols

The following protocols have been deprecated in this version:

Table 2. Deprecated protocols in this version

Proto ID	Protocol	Description
1509	axifile	AXifile is a file sharing service. (http://www.axifile.com). This protocol plug-in is deprecated.
846	seesmic	This protocol plug-in classifies the http traffic to the host seesmic.com. It also classifies the ssl traffic to the Common Name .seesmic.com. This protocol is now classified as Hootsuite.

1.3. Attributes

This section describes the updates to Attributes.

1.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

1.3.1.1. Event Attributes added in this version

Table 3. Added Event Attributes

Protocol	New event attribute	Description
amqp	arguments	Arguments of the AMQP request.
amqp	class	Class of AMQP request.
amqp	correlation_id	Identifier used to correlate the application.
amqp	end	Indicates the end of a top level event.
amqp	exchange_type	Mode of AMQP exchange.
amqp	properties	Properties of the data exchanged between the client and the server.
amqp	replyto	Addresse of the reply queue.
amqp	request	An AMQP request
amqp	routing_key	Virtual address used to route a message.
amqp	server_major_version	Major version of the protocol used by the server.
amqp	server_minor_version	Minor version of the protocol used by the server.
amqp	type	Type of AMQP request.
dhcp	xid	Transaction ID, a random number chosen by the client, used by the client and server to associate requests and responses.
http	accept_language	Contains the languages accepted by the browser (ACCEPT-LANGUAGE HTTP header).
http	age	Contains the sender's estimate of the amount of time since the response was generated at the origin server (AGE HTTP header).
http	cache_control	Contains the current request/response chain cache-control directives (CACHE-CONTROL HTTP header).
http	content_language	Contains the content languages (CONTENT-LANGUAGE HTTP header).
http	content_transfer_encoding	Corresponds to HTTP's Transfer-Encoding header. Contains the content encoding (TRANSFER-ENCODING HTTP header).
http	date	Contains the date of the response (DATE HTTP header).
http	etag	Contains the current value of the entity tag for the requested variant (ETAG HTTP header).

Protocol	New event attribute	Description
http	expires	Contains the expiration date of the response (EXPIRES HTTP header).
http	pragma	Contains the current request/response chain pragmas (PRAGMA HTTP header).
http	proxied_traffic	Flag raised to indicate that the traffic is proxied. It will be raised as soon as possible and on the first server packet in the case of proxies that require a specific classification (asproxy, vtunnel ...). It will be raised in many different cases: we find one of HTTP's standard headers that implies an HTTP proxy (Proxy-Authenticate, Proxy-Authorization), we have a CONNECT method/request, we are above socks4 or socks5, the uri is an absolute one (http://foo.bar), we classified a protocol above HTTP which is tagged as anonymizer. We do not guarantee that all the proxy-detected requests are anonymization/evasion attempts: some applications will make genuine connections over HTTP using proxy stacks to implement data tunnels for example.
http	set_cookie	Contains a cookie stored by the server (SET-COOKIE HTTP header).

1.3.2. Event Attributes modified in this version

The following Event Attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 4. Modified Event Attributes

Protocol	Event attribute	Changes
amqp	major_version	session_fix, both, uint32, no_parent

Protocol	Event attribute	Changes
		session_fix, both, uint8, no_parent
amqp	method	session_mod, both, string_index, no_parent
		session_prt, both, string_index, request
amqp	minor_version	session_fix, both, uint32, no_parent
		session_fix, both, uint8, no_parent
amqp	response_time	session_mod, both, timeval, no_parent
		session_prt, both, timeval, request
amqp	revision	session_fix, both, uint32, no_parent
		session_fix, both, uint8, no_parent
s1ap	ep_ie_code	session_mod, both, uint8, ep_ie
		session_mod, both, uint16, ep_ie
sip	media_attr_ addr_end_offset	session_prt, both, uint32, media_attr
		session_prt, both, int32, media_attr
sip	media_attr_ addr_start_offset	session_prt, both, uint32, media_attr
		session_prt, both, int32, media_attr
sip	media_attr_ port_end_offset	session_prt, both, uint32, media_attr
		session_prt, both, int32, media_attr
sip	media_attr_ port_start_offset	session_prt, both, uint32, media_attr
		session_prt, both, int32, media_attr

1.4. Improvements, Bug Fixes, and Known Issues

1.4.1. Functional Improvements

Ticket ID	Description
RTC#22937	**[flashplugin_update] improved classification over http**
RTC#22934	**[xboxlive] improved classification over https using dns**
RTC#22903	**[blogger] added classification over google**
RTC#22876	**[baidu] improved classification over video cdn**
RTC#22863	**[ppstream] improved classification**
RTC#22845	**[kik] added classification over blogger**
RTC#22603	**[google_maps] improved classification**
RTC#22818	**[pandora] improved classification over udp**
RTC#22782	**[tumblr] added classification on user_agent**
RTC#22671	**[tu] added classification over youtube**
RTC#22665	**[kakaostory] added classification on the host story-api.kakao.com**
RTC#22659	**[itunes] improved classification**
RTC#22479	**[google_earth] improved classification on https**
SF#09677 - RTC#22393	**New attribute in HTTP to indicate proxied traffic**
RTC#22302	**[steam] improved classification over http and udp**
RTC#22233	**[youtube] improved classification over http and https**
RTC#22584	**[apns] improved classification over http**
RTC#21399	**New protocol Vine has been added (Video Streaming classification).**
RTC#22173	**[amazon_aws] Updated Protocol Classification on android**
RTC#22164	**[dailymotion] updated Protocol Classification**
RTC#22085	**[flashplugin_update] Update Protocol Classification**
RTC#21920	**[qq] improved classification over tcp on android device**
RTC#21896	**[wechat] improved classification over tcp and udp**
SF#09736 - RTC#21678	**Rtp streams associated to 050Plus is now classified as rtp.050plus**
RTC#21599	**[kakaotalk]improved classification over tcp and rtp**
RTC#21498	**[AMQP]: added new attributes**
SF#09566 - RTC#21190	**[teamviewer] added support for version 9 and 10 on several platforms**
SF#09549 - RTC#20907	**New metadata XID (transaction ID) added for DHCP protocol.**
RTC#1773	**[onlive] protocol added (cloud gaming classification).**

1.4.2. Bug Fixes

- SF#09031 - RTC#17972 - **[doc][perfect_dark] perfect_dark does not contain any bottom_layers in protocols.xml (should be spid)**

Bug Info	Description
Reported against	ProtocolBundle-1.82.0-20

Bug Info	Description
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	spid is missing as bottom layer for perfect_dark

- SF#09076 - RTC#18117 - **[http] http extraction issue on segmented packets**

Bug Info	Description
Reported against	ProtocolBundle-1.92.0-2x
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Http extraction issue on segmented packets

- SF#000010034 - RTC#23234 - **[IMAP] Infinite loop in uimap_add_priv_filename_rfc2231**

Bug Info	Description
Reported against	ProtocolBundle-1.120.0-20
Platform	All
Effect of bug	Infinite Loop
Expected versus actual behavior	infinite loop in IMAP plugin

- SF#09418 - RTC#20476 - **[050plus] Check the latest version**

Bug Info	Description
Reported against	ProtocolBundle-1.140.0-2x
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Take traces of the latest 050plus version

- SF#09587 - RTC#21037 - **[base] duration equals always 0**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	base:duration extraction is bugged

- SF#09899 - RTC#22469 - **[lync] add dns_cache based classification**

Bug Info	Description
Reported against	ProtocolBundle-1.120.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	add dns_cache based classification of Lync

- SF#09858 - RTC#22470 - **[box_net] missing classification of download box.net traffic**

Bug Info	Description
Reported against	ProtocolBundle-1.30.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	missing classification of download box.net traffic

- SF#09917 - RTC#22497 - **[webex] Webex over UDP is not detected**

Bug Info	Description
Reported against	ProtocolBundle-1.120.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Webex over UDP not identified

- SF#09825 - RTC#22552 - **[windows_update] traffic classified as HTTP**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[windows_update] improve classification

- SF#09967 - RTC#22587 - **[mysql] force server side on first packet without syn/synack/ack**

Bug Info	Description
Reported against	ProtocolBundle-1.120.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	force server side on first packet without syn/synack/ack

- SF#09886 - RTC#22616 - **[RTP] [CODEC_NAME] EVRCB is wrongly recognized as H264**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	EVRCB is wrongly recognized as H264 when no SIP session is present.

- SF#010127 - RTC#23300 - **[Teamviewer] UDP session not classified as Teamviewer**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-20
Platform	All
Effect of bug	Not Applicable

Bug Info	Description
Expected versus actual behavior	UDP session not classified as Teamviewer

1.4.3. Known Issues

- SF#09967 - RTC#22587 - **[mysql] force server side on first packet without syn/synack/ack**

Bug Info	Description
Reported against	ProtocolBundle-1.120.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	force server side on first packet without syn/synack/ack
Workaround	No workaround

- RTC#23332 - **[runescape] classification anomaly**

Bug Info	Description
Reported against	ProtocolBundle-1.140.0-2x
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification loss on login/start game workflow.
Workaround	No workaround

- RTC#23302 - **[bittorrent] : classification anomaly**

Bug Info	Description
Reported against	ProtocolBundle-1.140.0-2x
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification loss on certain specific workflows.
Workaround	No workaround

- RTC#23332 - **[thunder]: classification anomaly**

Bug Info	Description
Reported against	ProtocolBundle-1.140.0-2x
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification regression on certain specific workflows.
Workaround	No workaround

2. Protocol Bundle 1.130.0

2.1. What's new in the Protocol Bundle 1.130.0

2.1.1. Major enhancements in this release

29 new Protocols added, 1 deprecated. See **Section 2.2, “Protocol Updates”**

15 new Event Attributes added, 7 modified. See **Section 2.3, “Attributes”**

Main Features

- Classification for the XCAP (XML Configuration Access Protocol) protocol in VoLTE,
- Classification for the WCCP (Web Cache Communication Protocol) Cisco protocol,
- Classification for several mobile applications like “mobilemarket” and “find_my_iphone”,
- Classification for the Mubi VOD streaming platform,
- Improved classification coverage of the *Basic DPI* ixEngine mode,
- Upgraded DNS Caching support to IPv6 query type,
- New metadata was added in tns, mount, dcerpc plug-ins.

Other Enhancements

- SPID classification support over SOCKS layers (e.g. bittorrent),
- Ability to run IPv6 address matching in *DNS-Cache*,
- Ability to use the HTTP Content (POST and responses) to match patterns in PDATA,
- Other functional improvements and bug fixes, listed in **Section 2.4, “Improvements, Bug Fixes, and Known Issues”**

2.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.
- ixEngine 4.19.x versions 4.19.0-20 and higher.

2.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

2.1.4. Supported Platforms

2.1.4.1. Complete Protocol Bundle

The Complete version of the Protocol Bundle has been validated on the following Platforms :

x86 platforms

- x86 32-bit User mode LSB 3.x and 4.x, AMP and SMP
- x86 64-bit User mode LSB 3.x and 4.x, AMP and SMP
- x86 32-bit FreeBSD 9, AMP and SMP, with an External Flow Manager
- x86 64-bit FreeBSD 9, AMP and SMP, with an External Flow Manager
- x86 64-bit FreeBSD 8, SMP, with an External Flow Manager
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 64-bit Windows SMP with an External Flow Manager
- x86 64-bit Darwin SMP with an External Flow Manager

Specific high-performance platforms

- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium Networks OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium Networks OCTEON II CN68XX - SDK version 2.3
- Broadcom MIPS 32
- Power PC e500v2 - Freescale SDK 1.2
- Tilera TileGx - MDE version 4.0.0

2.1.4.2. Classification Protocol Bundle

The Classification version of the Protocol Bundle has been validated on the following Platforms:

64-bit

- Octeon2 Cavium SE - SMP, with an External Flow Manager
- Octeon2 Linux - SMP, with an External Flow Manager
- x86 LSB - AMP, with an External Flow Manager
- x86 LSB - SMP, with an External Flow Manager

32-bit

- PPC e500v2 Linux - AMP, with an External Flow Manager

2.2. Protocol Updates

2.2.1. New Protocols

The following new protocols have been added in this version:

Table 5. New protocols added in this version

Proto ID	Protocol	Description
2431	abs_cbnnews	Filipino news portal.
2422	auto24	Estonian classified ads website specialised in motor vehicles and spare parts.
2433	bazos	Classified ads website in czech republic.
2417	cubadebate	Cuban news portal.
2436	eksisozluk	Turkish forum on various topics. Includes occasional video streaming.
2420	elblog	El Salvadorian news portal.
2411	find_my_iphone	Application developped by Apple to find a lost iOS device.
2418	icrt	Cuban institute of radio and television website.
2429	kolektiv	Montenegrien website on media and lifestyle.
2430	kstna	Jordanian job offer website.
2415	lajmi	Albanian news portal.
2424	lider_bet	Georgian online betting and gaming platform.
2414	llp	LLP is a protocol encapsulating messages. LLP is classified when it carries messages HL7 version 2.
2435	milanuncios	Spanish classified ads website.
2410	mobilemarket	Mobile Market is an online Android and iOS software store developed by China Mobile. This plugin classifies traffic from Mobile Market Android application.
2412	mubi	Mubi is a video streaming platform for mobile devices and PC.
2421	neti	Estonian web search portal.
2416	onclickads	Web traffic to Ads Media servers for targeted advertising purposes.
2434	ppomppu	Southern Korean forum on hightech, food, society and lifestyle.
2423	tahiti_infos	Tahitian news portal.
2428	think	Macedonian news portal.
2432	tocmai	Romanian classified ads website.
2419	tothemaonline	Cypriote news portal.
2427	ts	Kyrgystani video streaming website.
2443	vxlan	vxlan is a network virtualization technology that uses vlan-like encapsulation over udp
2409	wccp	WCCP is a Cisco protocol that specifies interactions between one or more routers and one or more web-caches.

Proto ID	Protocol	Description
2425	web	Famous german web portal. Includes several services among web search, ecommerce, webmail and news.
2413	xcap	Xcap (XML Configuration Access Protocol) protocol in VoLTE environnement is used to setup, enable or disable the Supplementary Services available for a user.
2426	zougla	Cypriote news portal.

2.2.2. Deprecated Protocols

The following protocols have been deprecated in this version:

Table 6. Deprecated protocols in this version

ID	Name	Description
1099	google_desktop	Google Desktop is a desktop search software made by Google, with indexed document metadata.

2.3. Attributes

This section describes the updates to Attributes.

2.3.1. Event Attributes added in this version

Table 7. Added Event Attributes

Protocol	New event attribute	Description
amqp	revision	Protocol's revision.
dcerpc	call_id	ID of the call.
dcerpc	context_id	ID of the context.
mount	end	Indicates the end of a top level event.
mount	fhandle	Parent for all attributes related to file handle.
mount	filehandle	file handle metadata uncoded
mount	flavor	Authentification supported by the server
mount	flavors	Number of authentification flavors supported by the server
mount	length_fhandle	Length of the file handle
mount	path	Parent for all attributes related to path.
mount	path_length	Length of the data path string.
mount	path_value	Value of the data path string.
mount	status	Information status on the request process.
tns	content_length	Length in header field.
tns	mtu	Maximum Transmission data Unit size.

2.3.2. Event Attributes modified in this version

The following Event Attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 8. Modified Event Attributes

Protocol	Event attribute	Changes
rpc	message_type	pkt, both, string_index, no_parent
		session_mod, both, string, no_parent
rpc	procedure	pkt, client, uint32, no_parent
		session_mod, client, uint32, no_parent
rpc	program	pkt, both, uint32, no_parent
		session_mod, client, uint32, no_parent
rpc	program_version	pkt, both, uint32, no_parent
		session_mod, client, uint32, no_parent
rpc	state	pkt, both, uint32, no_parent
		session_mod, server, uint32, no_parent
rpc	version	pkt, both, uint32, no_parent
		session_mod, client, uint32, no_parent
rpc	xid	pkt, both, uint32, no_parent
		session_mod, both, uint32, no_parent

2.4. Improvements, Bug Fixes, and Known Issues

2.4.1. Functional Improvements

Ticket ID	Description
SF#09705 - RTC#21853	**[http] added proto tune max_header_size**
RTC#21844	**[ppstream] updated protocol classification**
RTC#22010	**[youku] updated protocol classification over http on referer and request uri**
RTC#21950	**[sina_weibo] updated protocol classification over http request uri simg.s.weibo.com**
RTC#21777	**[mailru] updated protocol classification on mradx host over SSL**
RTC#21692	**[nba] improved classification over http and https**
RTC#21689	**[mypeople_messenger] improved classification over daum using user_agent**
RTC#21910	**[vimeo] improved classification over akamai**
RTC#21433	**[line] improved classification over rtp**
RTC#21679	**[kik] improved classification over http on user_agent or referer**
RTC#21658	**[cnn] added classification over freewheel**
RTC#21613	**[instagram] added classification over akamai**
RTC#21251	**[badoo]improved classification over tcp**
RTC#21541	**[youtube] improved classification over http**
RTC#20661	**[aim] improved classification over https**
SF#09378 - RTC#20904	**[llp] Lower Layer Protocol added**
RTC#21164	**[line] improved classification over udp**
RTC#19960	**[http] improve is_webdav metadata**
SF#09049 - RTC#19707	**[dcerpc] new metadata: call_id and context_id added for dcerpc**
SF#08881 - RTC#19689	**[tns] new metadata: content length and MTU added for TNS protocol**

Ticket ID	Description
RTC#20593	**[mypeople_messenger] improved classification over tcp**
RTC#20586	**[tango] improved classification over tcp**
RTC#17060	**[mubi] new protocol added: Mubi**
SF#07810 - RTC#18347	**[mobilemarket] New protocol Mobilemarket added.**
SF#08307 - RTC#16183	**[wccp] add protocol classification: the WCCP V2.0 protocol specifies interactions between one or more routers and one or more web-caches**
RTC#17907	**[find_my_iphone] added classification for Find My iPhone**

2.4.2. Bug Fixes

- RTC#22127 - **[http] Cannot extract Host: header name+value when there is a leading whitespace**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Discards leading whitespace on first HTTP header

- SF#09196 - RTC#18907 - **[thunder] not correctly classified**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[Thunder]: not correctly classified Customer says flow: udp.port == 13850 && udp.port == 9609 should be classified as Thunder

- RTC#19052 - **[pb1.90][stab]crash ulayer_store_lookup_create in utftp**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Crash
Expected versus actual behavior	

- SF#09830 - RTC#22026 - **speedtest not recognized**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All

Bug Info	Description
Effect of bug	Classification Anomaly
Expected versus actual behavior	some speedtest workflows are classified as unknown

- SF#09584 - RTC#21120 - **[AMQP]: amqp is classified as unknown**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[AMQP]: amqp classified as unknown

- SF#09567 - RTC#21034 - **[IMAP] imap does not get classified on first 5 packets**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[IMAP]:imap does not get classified on first 5 packets

- SF#09537 - RTC#20960 - **[teamviewer] misclassified in https**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	teamviewer misclassified in https

- SF#09203 - RTC#20014 - **[bittorrent] uTP sessions are not classified (when network setting changed in the middle of the download)**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Bittorrent uTP session not classified when network settings changed after download started

- SF#09183 - RTC#19760 - **[skype] skype login is not blocked with https disabled**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[skype] skype login blocking with https disabled

2.4.3. Known Issues

- SF#08798 - RTC#17180 - **[ftp] response truncated (muli-lines not supported)**

Bug Info	Description
Reported against	ProtocolBundle-1.70.0-21
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Extraction of multi-lines response should supported in FTP.
Workaround	No workaround

- SF#09249 - RTC#17022 - **[rtcp] rtcp is not classified and bad behavior of rtp**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[rtcp] improve rtcp classification and rtp behavior
Workaround	No workaround

- RTC#15778 - **[pdata] allow per pdd file pdata configuration**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	
Workaround	No workaround

- SF#09267 - RTC#19423 - **[SF9267] Incorrect HTTP method**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Incorrect HTTP method
Workaround	No workaround

- SF#09564 - RTC#20888 - **[srvloc] add Attribute Request classification support**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[srvloc] add Attribute Request classification support
Workaround	No workaround

- RTC#21648 - **[mobilink][spdy][zlib]Reduce dynamic allocations in order to avoid heap fragmentation.**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-22
Platform	All
Effect of bug	Performance Anomaly
Expected versus actual behavior	Mobilink and spdy performs huge allocations and memory release on each classification packets. Use static buffers instead in order to avoid too much heap usage.
Workaround	No workaround

- SF#09134 - RTC#18938 - **[aim] attributes about transferred file not extracted**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-22
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	[AIM]: attributes about transferred file not extracted
Workaround	No workaround

- SF#09728 - RTC#21525 - **[smtp] attach_content_decoded no longer extracted**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	attach_content_decoded extraction regression
Workaround	No workaround

- RTC#20748 - **[http] several http method are not raised : MKACTIVITY, MKWORKSAPCE, TRACE**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-20
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	The follwoing http methods are not raised : MKACTIVITY, MKWORKSAPCE, TRACE
Workaround	No workaround

- SF#09367 - RTC#19676 - **[Protobook] List supported RTP codecs for mos_session and rfactor computation**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-20
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	List supported RTP codecs for mos_session and rfactor computation

Bug Info	Description
Workaround	No workaround

- SF#09678 - RTC#22031 - **DNS traffic classified as SIP**

Bug Info	Description
Reported against	ProtocolBundle-1.120.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Disable the l3l4 mechanism when we disable the multiplexing support in SIP.
Workaround	disable sip

- SF#09978 - RTC#22615 - **[skype][qik] fix classification conflict**

Bug Info	Description
Reported against	ProtocolBundle-1.130.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[skype][qik] fix classification conflict
Workaround	No workaround

3. Protocol Bundle 1.120.0

3.1. What's new in the Protocol Bundle 1.120.0

3.1.1. Major enhancements in this release

41 new Protocols added. See Section 3.2, “Protocol Updates”

14 new Event Attributes added. See Section 3.3, “Attributes”

Summary of major enhancements :

- Added new detection of DNS evasion applications e.g. IODINE, VPNOVERDNS.
- Added Video Quality Indicators metadata for Hulu and Amazon Video (MS Silverlight).
- Added new detection of Instant Messaging applications e.g. ZALO and FEILIAO.
- Added detection of the proprietary VMWare Horizon View remote control protocol.
- Optimized and enhanced the "DNS Caching" classification capabilities.

3.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.
- ixEngine 4.19.x versions 4.19.0-20 and higher.

3.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don’t have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

3.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit User mode LSB 3.x and 4.x, AMP and SMP
- x86 64-bit User mode LSB 3.x and 4.x, AMP and SMP
- x86 32-bit FreeBSD 9, AMP and SMP, with an External Flow Manager
- x86 64-bit FreeBSD 9, AMP and SMP, with an External Flow Manager
- x86 64-bit FreeBSD 8, SMP, with an External Flow Manager
- x86 32-bit Solaris 10 AMP with an External Flow Manager

Specific high-performance platforms

- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium Networks OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium Networks OCTEON II CN68XX - SDK version 2.3
- Broadcom MIPS 32
- Power PC e500v2 - Freescale SDK 1.2
- Tilera TileGx - MDE version 4.0.0

3.2. Protocol Updates

3.2.1. New Protocols

The following new protocols have been added in this version:

Table 9. New protocols added in this version

Proto ID	Protocol	Description
2398	4chan	4chan is an image-based bulletin board where people can share and comment on images.
2399	4tube	4tube is a free adult video sharing Web site, similar in concept, but unrelated to YouTube.
2346	8021ad	802.1ad is a protocol which allows sending VLAN membership information of a frame.
2400	99acres	99Acres is a popular Real Estate portal in India.
2401	aajtak	AAJTAK is a popular site in India used for streaming videos.
2402	aceproject	AceProject is a free collaboration-oriented project management software with features such as Gantt charts, time tracking and expense tracking.
2373	afreeca	This protocol plug-in classifies the http and TCP traffic to the host .afreeca.com.
2407	aiccu_tic	AICCU (Automatic IPv6 Connectivity Client Utility) is a cross-platform utility for automatic IPv6 tunnels configuration.
2403	ammyy_admin	Ammyy Admin is a remote desktop application.
2404	amoebaos	AmoebaOS is an online operating system, providing a cloud-based desktop.
2405	animoto	Animoto automatically produces video pieces from photos, video clips, and music.
2388	aqlame	Mauritanian news portal.
2406	asana	Asana is a web and mobile application designed to improve the way teams communicate and collaborate.
2376	battlenet	Online multiplayer gaming server.
2396	clip	Vietnamese multimedia streaming website.
2370	crackle	crackle is an entertainment network and studio that distributes free movies, television shows and original programming.
2379	el_balad	Egyptian news portal.
2381	elwatannews	Egyptian news portal.
2371	feiliao	feiliao is a Chinese instant messaging application. This plug-in classifies file transfers and chats.
2377	indeksonline	Albanian news portal.
2392	inquirer	Philippino news portal.
2375	iodine	Iodine is a solution which provides tunneling through the standard DNS protocol. This plugin classifies only raw UDP mode and DNS NULL Resource Records in bidirectionnal mode.

Proto ID	Protocol	Description
2385	jamaica_gleaner	Jamaican news portal.
2393	kupujemprodajem	Serbian classified ads website.
2387	life	Taiwanese media and lifestyle website.
2380	lun	Chilian news and entertainment portal.
2397	marebpress	Yemeni news portal.
2384	nextmedia	Media and lifestyle website for Hong Kong and Taiwan.
2378	primewire	Video streaming website.
2382	protothema	Cypriot news portal.
2390	shabiba	Omanian news portal.
2383	tiempo	Honduran news portal.
2389	timesofoman	Omanian news portal.
2394	trinituner	Automotive publications and community website in Trinidad and Tobago.
2391	tune	Pakistani multimedia and lifestyle website.
2395	ukr	Ukrainian portal for news, media and lifestyle.
2372	vmware_horizon_view	Vmware Horizon View is a commercial desktop-virtualization product developed by VMware. This plugin classifies pcoip streams over UDP, between virtual machines and Mac/Windows clients
2374	vpnoverdns	Vpnoverdns is a solution which provides tunneling through the standard DNS protocol.
2386	weather4all	Macedonian weather forecast website.
2345	zalo	Zalo is a vietnamese mobile IM application created by VNG Corporation with audio/image file send feature. The HTTP/HTTPS traffic generated by this application may either be classified as Zalo or Zing.
2408	zumodrive	ZumoDrive is a cloud-based file synchronization and storage service.

3.2.2. Deprecated Protocols

No protocols have been deprecated in this version.

3.3. Attributes

This section describes the updates to Attributes.

3.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

3.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

3.3.1.2. Event Attributes added in this version

Table 10. Added Event Attributes

Protocol	New event attribute	Description
capwap	bssid	EUI-48 MAC address of the radio receiving the packet.
capwap	bssid_64	EUI-64 MAC address of the radio receiving the packet.
capwap	dr	It is the data rate of the packets received by the WTP in units of 0.1 Mbps.
capwap	end	Indicates the end of a top level event.
capwap	frame_info	Parent attribute containing wireless specific information.
capwap	rssi	It is the received signal strength indication, in dBm..
capwap	snr	It is the signal to noise ratio of the received IEEE 802.11 frame, in dB.
hulu	end	Indicates the end of a top level event.
hulu	video	Parent attribute containing video metadata.
hulu	video_datarate	Video bitrate in kilobits per second.
rtmp	encryption	Name of the encryption used.
silverlight	end	Indicates the end of a top level event.
silverlight	video	Parent attribute containing video metadata.
silverlight	video_datarate	Video bitrate in kilobits per second.

3.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

3.3.3. Event Attributes modified in this version

No Event Attributes have been modified in this version.

3.4. Improvements, Bug Fixes, and Known Issues

3.4.1. Functional Improvements

Ticket ID	Description
SF#08332 - RTC#18383	**[capwap] enhanced classification based on custom port number (based on RFC 5415).**
SF#69506950,6489,8937 - RTC#6045	**[zalo] added new protocol (instant messaging).**
RTC#18924	**[qq] improved classification over TCP**
RTC#17054	**[crackle] added new protocol**
RTC#19030	**[youku] improved classification over tcp**
RTC#19179	**[owa] added the support of the 2010 version.**
SF#09170 - RTC#19336	**[capwap] added new metadata**
SF#07811 - RTC#18386	**[feiliao] added new protocol (chinese IM).**
SF#08964 - RTC#18538	**[afreeca] added new protocol over HTTP and TCP.**
SF#09017 - RTC#18541	**[vpnoverdns] added new protocol.**
RTC#18607	**[kakaotalk] improved classification over TCP**
RTC#19493	**[spotify] improved classification over tcp for v4.0.1.0 on windowsphone**
RTC#19512	**[skype] improved classification over tcp on kindlefire device**
RTC#18992	**[thunder/bittorrent] improved classification over tcp**
RTC#18998	**[mapi] added MAPI support over HTTP (MSRPC)**
RTC#19704	**[maaii] improved classification over https**
SF#09404 - RTC#19819	**[kakaotalk] added classification for RTP streams over kakaotalk.**
RTC#20078	**[qq] improved classification over tcp on android device**
RTC#19832	**[viber] improved classification over udp**
RTC#20045	**[ppstream] improved classification over udp**

3.4.2. Bug Fixes

- SF#09406 - RTC#20148 - **[youtube] improved classification for traffic-blocking workflows when using Internet Explorer.**

Bug Info	Description
Reported against	ProtocolBundle-1.70.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	When using IE and blocking traffic, youtube behaves differently and avoids classification.

- SF#07947 - RTC#15684 - **[lync] Classification issue for RTP and STUN sessions over SSL and using port #443**

Bug Info	Description
Reported against	ProtocolBundle-1.71.0-20

Bug Info	Description
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	lync poorly classified over STUN and RTP.

- SF#09213 - RTC#19123 - **classification mismatch between wow/battlenet and bittorrent/unknown.**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	tbd

- SF#09175 - RTC#18797 - **classification mismatch between T38 and RTP.**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	classification mismatch between T38 and RTP.

- SF#09395 - RTC#19779 - **RSH not classified when 'port' is not filled in rsh header**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	RSH not classified when 'port' is not filled in rsh header

- SF#09448 - RTC#20347 - **[openvpn] no classification on username/password authenticated servers**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	-

- SF#09403 - RTC#20062 - **ssl.spdy.facebook not classified when https is disabled**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	facebook classification affected by disabled https

- SF#09254 - RTC#20055 - **[rtsp] classified not raised because of "is_upper_proto" not empty**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All SMP
Effect of bug	Classification Anomaly
Expected versus actual behavior	[rtsp/rdt] classified not raised for rtsp

- SF#09405 - RTC#19854 - **[juniper] Jondo is not classified when session begins with too many s2c packets**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Jondo is not classified

- SF#06654 - RTC#19701 - **[ppfilm] ppfilm video stream not detected**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	ppfilm video stream not classified

- SF#09354 - RTC#19782 - **[netflix] improve classification of netflix when using Android**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	netflix classification issues on Android.

- SF#09354 - RTC#19712 - **[netflix] add classification over bmff**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	add classification of netflix over bmff

- SF#09310 - RTC#19586 - **[rtp] fix rtp:codec_name**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-20
Platform	All

Bug Info	Description
Effect of bug	Extraction Anomaly
Expected versus actual behavior	rtp:codec_name attribute issue.

- SF#09489 - RTC#20473 - **Classified flag not raised for RTSP session**

Bug Info	Description
Reported against	ProtocolBundle-1.140.0-2x
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classified flag not raised for RTSP session

3.4.3. Known Issues

There are no Known Issues in this version.

4. Protocol Bundle 1.110.0

4.1. What's new in the Protocol Bundle 1.110.0

4.1.1. Major enhancements in this release

27 new Protocols added. See Section 4.2, “Protocols”

4 Event Attributes added, 3 modified. See Section 4.3, “Attributes”

Several functional improvements and bug fixes. See Section 4.4, “Improvements, Bug Fixes, and Known Issues”

Summary of major enhancements :

- The new classifications are focused on media streaming applications (PC and Mobile Devices) like “viewster”, “exacqvision”, “beetalk”.
- This release also includes the full support for the legacy SSLv2 headers parsing (metadata extraction and classification over SSL).
- It also features a noticeable CPU usage improvement on Octeon-based platforms.

Note:

1. The extraction is changed to provide advanced decoding for the following (see also Qosmos_Protocol_Bundle_Protobook_1.110.0) :
   - Q_HTTP_URI_DECODED
   - Q_HTTP_URI_GET_DECODED
   - Q_HTTP_URI_POST_DECODED
   - Q_HTTP_URI_PATH_DECODED
   - Q_HTTP_POST_VARIABLE_DECODED
2. The Q_HTTP_URI_PARAM_VALUE value decoding is rolled-back to its original PB 1.17.0 behavior : raw value, no URI decoding.
3. SCTP-based stack classification support is limited to EXTFLOW mode when using ixE’s Flow Manager, will also work with an External Flow Manager supporting SCTP.

4.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

- ixEngine 4.19.x versions 4.19.0-20 and higher.

4.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

4.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3

4.2. Protocols

4.2.1. New Protocols

The following new protocols have been added in this version:

Table 11. New protocols added in this version

Proto ID	Protocol	Description
2353	bancopopular	Puertorican online banking website.
2351	beetalk	beetalk is an instant messaging software for mobile.
2366	bigeye	Ugandan entertainment website.
2365	clicanoo	Reunion island news portal.
2356	emag	Romanian classified ads website.
2349	exacqvision	Exacqvision is a software used for video surveillance.
2358	expressen	Swedish news portal.
2340	freewheel	FreeWheel provides ad management and monetization, a private marketplace for premium television inventory, and advisory services for video streaming industry.
2352	gigacircle	Taiwanese blogging platform.
2360	hihi2	Website specialised in international soccer.
2362	linio	Latino American ecommerce portal.
2348	liverail	This protocol plug-in classifies LiveRail which is an online video advertising platform
2364	ltt	Libya Telecom and Technology company website.
2367	mapy	Czech republic localization webiste.
2342	mocean	MOcean is a advertising agency.
2344	nielsen	Nielsen is a global information and measurement company that enables companies to understand consumers and consumer behavior.
2368	ovaciondigital	Uruguayan sports and multimedia website.
2359	r10	Turkish forum on multiple subjects.
2355	raya	Palestinian news portal.
2361	rudaw	Kurd news portal.
2350	stickyads	Stickyads is a video platform for publishers in Europe.,Classification over http.
2354	tukif	French adult content website.
2343	turner	Turner is a video streaming solution provider for audio/video content web services.
2363	vetogate	Egyptian news portal.
2347	viewster	Viewster delivers free video.,Classification over http.
2357	vuiviet	Vietnamese online entertaiment portal.
2341	xiaomi	Xiaomi is a privately owned Chinese electronics company. It designs, develops, and sells smartphones, mobile apps, and consumer electronics.

4.2.2. Deprecated Protocols

No protocols have been deprecated in this version.

4.3. Attributes

This section describes the updates to Attributes.

4.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

4.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

4.3.1.2. Event Attributes added in this version

Table 12. Added Event Attributes

Protocol	New event attribute	Description
http	forward_addr6	IPv6 DNS address to which the client is redirected.
http	forward_redline6	IPv6 address found in the "x-forward-redline" HTTP header, used for forwarding.
irc	filesize	Size (byte) of the transferred file.
radius	length	Indicates the length of the packet. Octets outside the range of the Length field MUST be treated as padding and ignored on reception

4.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

4.3.3. Event Attributes modified in this version

The following Event Attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 13. Modified Event Attributes

Protocol	Event attribute	Changes
hi5	uid	session_mod, both, buffer, account
		session_mod, both, string, account
imap	file_type	session_mod, both, buffer, attach
		session_mod, both, string, attach
rtp	end_session	session_mod, both, string, no_parent
		session_mod, both, uint8, no_parent

4.4. Improvements, Bug Fixes, and Known Issues

4.4.1. Functional Improvements

Ticket ID	Description
RTC#16203	**[WeChat] Added classification on Symbian device over tcp**
SF#08041 - RTC#12402	**[http] added handling of IPv6 addresses on callback for Q_HTTP_FORWARD_ADDR**
RTC#9780	**[ssl] added support for sslv2 header**
SF#08882 - RTC#17141	**[radius] Added new metadata "Length"**
RTC#18091	**[libhttp] Forced Advanced DPI on HTTP CONNECT**
SF#09187 - RTC#18957	**[tcp] set time_pkt_unseq for TCP keep-alive packets**
RTC#18932	**[tango] added handling of tcp traffic on ios platform**
RTC#19111	**[wechat] improved classification over udp**
RTC#19010	**[irc_transfer]: added metadata end-of-flow marker**
RTC#19847	**[xvideos] improved classification over trafficfactory**
RTC#19844	**[xnxx] improved classification over trafficfactory**
RTC#19841	**[hardsextube] improved classification**

4.4.2. Bug Fixes

- SF#000008878 - RTC#17442 - **[SF8878][DOC][Skydrive] protocol description**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-21
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Skydrive description is outdated as this service was replaced by onedrive

- SF#08951 - RTC#17184 - **[pop3] response truncated (muli-lines not supported)**

Bug Info	Description
Reported against	ProtocolBundle-1.72.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Extraction of multi-lines response should be supported in POP3.

- SF#08798 - RTC#17180 - **[ftp] response truncated (muli-lines not supported)**

Bug Info	Description
Reported against	ProtocolBundle-1.70.0-21
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Extraction of multi-lines response should be supported in FTP.

- SF#08921 - RTC#17162 - **[RTP]: RTP Signature Problem, Payload Type should not be included.**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Payload-Type should not be included in RTP signature.

- SF#09052 - RTC#18043 - **[rexpand] rexpand does not correctly implement PCRE & pdb_customize crashes on unsupported pattern**

Bug Info	Description
Reported against	ProtocolBundle-1.82.0-20
Platform	All
Effect of bug	Crash
Expected versus actual behavior	pdb_customize cannot fully support PCRE, sometimes crash occurs on unrecognized pattern

- SF#09215 - RTC#19081 - **[capwap] classification issues**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-2x
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	TBD

- SF#09019 - RTC#17814 - **[stun] wrong classification because 'candidate identifier' is limited to 4 bytes**

Bug Info	Description
Reported against	ProtocolBundle-1.81.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[stun] 'candidate identifier' no more limited to 4 bytes

- SF#09012 - RTC#17708 - **[smb] Missing krb5_blob**

Bug Info	Description
Reported against	ProtocolBundle-1.82.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	krb5_blob is not extracted

- SF#08970 - RTC#17498 - **[LinkedIn] : linkedIn attributes extracted as data**

Bug Info	Description
Reported against	ProtocolBundle-1.81.0-20

Bug Info	Description
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	LinkedIn attributes not extracted

- SF#09112 - RTC#18331 - **[SF9112][MY_YAHOO] my_yahoo classified as yahoo**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-22
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	m_yahoo over ssl is classifeed as yahoo

- SF#09073 - RTC#18274 - **[smb] add extraction of file_id on open_andx response command**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	add extraction of file_id on open_andx response command

- RTC#18201 - **[smb] failed to rebuild file transferred over smb**

Bug Info	Description
Reported against	ProtocolBundle-1.82.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	

- SF#09131 - RTC#18598 - **[SF9131] dns cache does not check protocol availablility (copied from ixe task).**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Crash
Expected versus actual behavior	sample_flow crashes with SEGFAULT against DNS traffic

- SF#08998 - RTC#18874 - **[radius] improve classification of Access-Accept packets**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification issue if Access-Accept packets contains a User-Name

- SF#09197 - RTC#18871 - **[protobook] Update tcp:count_flags description**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	# # #

- SF#09148 - RTC#18676 - **[IRC]: ixEngine unable to detect IRC . It is being classified as "UNKNOWN"**

Bug Info	Description
Reported against	ProtocolBundle-1.40.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	IRC classification problem: ixEngine unable to detect IRC . It is being classified as "UNKNOWN"

- SF#09342 - RTC#19573 - **[appsdk] error message not displayed if no LISP interpreter is installed**

Bug Info	Description
Reported against	ProtocolBundle-1.50.0-23
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	fix error message when no lisp interpreter is available.

- RTC#19566 - **[rexpand] crash on regexp "[az-az]"**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-2x
Platform	All
Effect of bug	Crash
Expected versus actual behavior	

4.4.3. Known Issues

- SF#74237423 - RTC#7068 - **[SF 7423] [http] normalization cases not supported (duplicated slashes, empty query, dot-segtments)**

Bug Info	Description
Reported against	ProtocolBundle-1.40.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	duplicated slashes, empty query and dot-segtments cases are not supported
Workaround	No workaround

- RTC#17638 - **[http]: BASELINE-CONTROL method not raised**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-21
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	http method BASELINE-CONTROL is not extracted anymore
Workaround	none

- SF#09157 - RTC#18573 - **[google_gen] [df_offload] not raised as it is supposed to be**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	x86 SMP
Effect of bug	Classification Anomaly
Expected versus actual behavior	remove google_gen declassification feature
Workaround	No workaround

- SF#09031 - RTC#17972 - **[doc][perfect_dark] perfect_dark does not contain any bottom_layers in protocols.xml (should be spid)**

Bug Info	Description
Reported against	ProtocolBundle-1.82.0-20
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	spid is missing as bottom layer for perfect_dark
Workaround	No workaround

- RTC#19403 - **[basic_dpi] incorrect info in source-code documentation**

Bug Info	Description
Reported against	ProtocolBundle-1.100.0-21
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	
Workaround	No workaround

- SF#09354 - RTC#19813 - **[netflix] video_title/video_id extraction when on mobiles**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-2x
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	N/A
Workaround	No workaround

- SF#09367 - RTC#19676 - **[Protobook] List supported RTP codecs for mos_session and rfactor computation**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-2x
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	List supported RTP codecs for mos_session and rfactor computation
Workaround	No workaround

- SF#09320 - RTC#19544 - **[TDS]: Protocol classified as uknown instead of TDS**

Bug Info	Description
Reported against	ProtocolBundle-1.110.0-2x
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[TDS]: Protocol classified as uknown instead of TDS
Workaround	No workaround

5. Protocol Bundle 1.100.0

5.1. What's new in the Protocol Bundle 1.100.0

5.1.1. Major enhancements in this release

22 new Protocols added. See Section 5.2, “Protocol Updates”

122 new Event Attributes added. See Section 5.3, “Attributes”

Summary of major enhancements :

- Classification added for “fetion” (IM/VoIP), “minecraft pocket”, “bleep” (also known as BitTorrent Chat), or “twitch” (popular video broadcasting platform) applications,
- Specific classification of the media streams related to the Facebook mobile messaging application was added (“Facebook Messenger”),
- Extended metadata extraction was added in IAX protocol, including IAX2 “Trunk” Messages metadata,
- Advanced support was added to the “dtls” plug-in, improving classification and enabling the classification of “sRTP” (secured RTP profile) media streams over it,
- SSL sessions storage system was improved and optimized (mostly memory usage) allowing more SSL sessions contexts to be handled by the ixEngine,
- New protocols classification and metadata extraction (see table immediately below).

Note:

1. In the SSL plug-in, the “Common Name” metadata previously stored from previous TCP streams is no longer extracted in continued SSL sessions. The classification of these continued sessions is kept.
2. The proto-tune “peering_disabled” from the “ip” plug-in should not be used in production environment (for internal testing only).

Ticket ID	Description
RTC#18027	**[qq]improve classification over tcp for windows8 application**
RTC#17658	**[youku] improve classification over udp**
RTC#17458	**[qq] missing classification over tcp**
RTC#17364	**[wechat] missing classification on video call (udp stream)**
SF#08969 - RTC#17255	**[qosmos][docs] Application 'UNKNOWN' is asked to be in group 'UNASSIGNED' in qm_application_groups.xml**
SF#08873 - RTC#16589	**[sgcarmart] Add classification and metadata extraction**
SF#08870 - RTC#16553	**[qoo10] add protocol and metadata extraction**
RTC#17159	**[ppstream] improve classification**
RTC#17051	**[iax] trunk support in IAX2 messages**
SF#08754 - RTC#15618	**[twitch] New protocol**

Ticket ID	Description
RTC#16878	**[spotify] improve classification over tcp (run_06)**
SF#08903 - RTC#16722	**[sistic] Add classification and metadata extraction**
SF#08902 - RTC#16719	**[propertyguru] Add classification and metadata extraction**
SF#08869 - RTC#16643	**[golden_village] add protocol and metadata extraction**
SF#08872 - RTC#16603	**[jobsdb] Add classification and metadata extraction**
SF#08871 - RTC#16600	**[hungrygowhere] Add classification and metadata extraction**
SF#08062 - RTC#14508	**[dns] new metadata for dns entry sections**
SF#08300 - RTC#13413	**[VoIP Protocols] New metadata service stats_info**
SF#08868 - RTC#16533	**[toggle] add protocol and metadata extraction**
SF#08867 - RTC#16506	**[tigerair] add protocol and metadata extraction**
SF#08866 - RTC#16502	**[zuji] add protocol and metadata extraction**
SF#07807 - RTC#16207	**[139mail] add protocol classification**
RTC#11108	**[iax] new generic header metadata extraction**
SF#07181 - RTC#12205	**[bleep] new protocol for BitTorrent Chat**
SF#6011,SF#7809,SF#4550 - RTC#1975	**[fetion] add new protocol Fetion (Instant Messaging)**
SF#06063 - RTC#327	**[nntp] extract attachment metadata**

5.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.
- ixEngine 4.19.x versions 4.19.0-26 and higher.

5.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don’t have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

5.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3

5.2. Protocol Updates

5.2.1. New Protocols

The following new protocols have been added in this version:

Table 14. New protocols added in this version

Proto ID	Protocol	Description
2338	139mail	139mail is a chinese webmail powered by China Mobile.
2334	appsflyer	AppsFlyer provides measurement and tracking services for mobile platform application developers.
2335	apsalar	Apsalar provides analytics and advertising solutions for mobile application developers.
2324	beatport	On-line music shop website. This plug-in classifies both search and music download workflows.
2337	bleep	Bleep is a fully encrypted and distributed instant messaging protocol created by the BitTorrent team. This protocol plug-in supports both text and voice discussions.
2329	boldchat	BoldChat is an instant messaging platform for businesses (by LogMeIn).
2322	brightcove	Brightcove is a provider of cloud services for video.
2319	crashlytics	Crashlytics is a mobile company building crash reporting for iOS and Android.
2331	facebook_messenger	Facebook Messenger is a text and voice messaging application for mobile devices. This plug-in classifies audio call sessions only.
2339	fetion	Fetion is a Chinese instant messaging application provided by China Mobile. This plug-in classifies file transfers, chat and audio calls.
2336	gravatar	Gravatar allows picture-based user identification.
2333	inmobi	InMobi provides advertising services for mobile platforms.
2327	irods	iRods is an open source massive data management and storage software.
2326	minecraft_pocket	Minecraft is a game about placing blocks and going on adventures.
2330	okcupid	OkCupid is an online dating website. This plug-in both classifies browsing and file upload workflows.
2323	plentyoffish	Free online dating site, popular primarily in Canada, the UK, Australia, and the United States. This plug-in classifies both browsing and file upload workflows.
2310	propertyguru	Singaporean property sale and rental searching website.
2309	sistic	Sistic is a singaporean online events tickets booking website.
2320	trafficfactory	Traffic Factory provides an advertisement engine. It is generated based on user location and targeted device.

Proto ID	Protocol	Description
2328	twitch	This signature detects video stream from twitch.tv. Twitch.tv is a live video streaming service focused on video games.
2321	visadd	VisAdd provides provides an advertisement services.
2325	vtun	Software that creates virtual tunnels over TCP/IP networks.

5.2.2. Deprecated Protocols

The following protocols have been deprecated in this version:

Table 15. Deprecated protocols in this version

Proto ID	Protocol	Description	Comments
314	megaupload	Megaupload was an online solution to store, send and share files. Megaupload was shut in January 2012.	

5.3. Attributes

This section describes the updates to Attributes.

5.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

5.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

5.3.1.2. Event Attributes added in this version

Table 16. Added Event Attributes

Protocol	New event attribute	Description
aim	message_raw	Message raw value.
dns	section_type	Type of section for each DNS answer.
facetime	service_stats	Composite attribute containing the packet metrics used for each new service type detection. Note: this attribute won't be extracted in case of session expiration (eg. when the current service is not ended properly by the user).
golden_village	cinema	Cinema's name.
golden_village	day	Date of the film show.
golden_village	end	Indicates the end of a top level event.
golden_village	film	Movie title.
golden_village	query	Contains query metadata sent to the server.
golden_village	time	Film show time (hhmm).
gotomypc	end	Indicates the end of a top level event.
gotomypc	service	Current service identification string.
gotomypc	service_id	Composite 32-bit integer value defining the service currently used. The first byte (LSB) gives the generic service definition, the second byte gives an advanced service definition for specific cases (example: File Transfer).
gotomypc	service_info	Parent entry for service information metadata. The service type is resolved by a statistical method (behavior analysis), with periodic revaluation. The revaluation period as well as other service detection parameters are modifiable using proto-tunes.
hungrygowhere	cuisine	Cuisine's type seeked.
hungrygowhere	end	Indicates the end of a top level event.
hungrygowhere	foodtype	Type of food offered.
hungrygowhere	location	Restaurant location's type.
hungrygowhere	name	Name of the restaurant.

Protocol	New event attribute	Description
hungrygowhere	place_type	Location's type seeked.
hungrygowhere	query	Contains query metadata sent to the server.
hungrygowhere	query_raw	Contains the query sent to the search engine as indicated in the URL.
hungrygowhere	query_text	Query sent to the search engine.
hungrygowhere	restaurant	Parent attribute containing restaurant metadata.
iax	element	This parent attribute contains a list (of type TLV, type length value) of data relative to a packet of type "Full" whose message_id is "IAX".
iax	element_id	Identifier of the information coming from a packet of type "Full" whose message_id is "IAX".
iax	element_name	Name of the information coming from a packet of type "Full" whose message_id is "IAX".
iax	element_value	Value of the information coming from a packet of type "Full" whose message_id is "IAX".
iax	end	Indicates the end of a top level event.
iax	message	This parent attribute contains the data link to a packet of type "Full".
iax	message_id	For full IAX2 frames, message_id is the type of a frame.
iax	message_name	For full IAX2 frames, message_name is the name of a frame.
iax	packet_type	Packet type.
iax	subclass_id	The command number for a "message_name" type packet.
iax	subclass_name	The command string for a "message_name" type packet.
iax	trunk	This parent attribute contains data concerning a packet of type "Trunk".
iax	trunk_call	This parent attribute contains data linked to a call.
iax	trunk_call_data_len	Trunk call data length in bytes.
iax	trunk_call_data_offset	Trunk call data offset in bytes in the UDP Stream.
iax	trunk_call_number	Trunk call source call number.
iax	trunk_command	Flags for options that apply to a trunked call.
iax	trunk_meta	Meta command which indicates whether or not the Meta Frame is a trunk.
iax	trunk_timestamp	Timestamp (in ms) after the start of this call, indicating the time at which this trunk packet was transmitted.
jobsdb	end	Indicates the end of a top level event.
jobsdb	max_salary	Maximum salary expected.

Protocol	New event attribute	Description
jobsdb	min_salary	Minimum salary expected.
jobsdb	query	Contains query metadata sent to the server.
jobsdb	query_raw	Contains the query sent to the search engine as indicated in the URL.
jobsdb	query_text	Query sent to the search engine.
jobsdb	query_type	Sort of query sent to the search engine.
line	service_stats	Composite attribute containing the packet metrics used for each new service type detection. Note: this attribute won't be extracted in case of session expiration (eg. when the current service is not ended properly by the user).
mplus_messenger	service_stats	Composite attribute containing the packet metrics used for each new service type detection. Note: this attribute won't be extracted in case of session expiration (eg. when the current service is not ended properly by the user).
nntp	attach	Parent entry, for attach fields in a message.
nntp	attach_content	Attached file content.
nntp	attach_filename	Attachment name.
nntp	end	Indicates the end of a top level event.
qoo10	cart	Parent attribute containing information about a product added in a cart.
qoo10	cart_item_id	product id added in the cart.
qoo10	category_id	Id of the category.
qoo10	category_name	Category name the product belongs to.
qoo10	end	Indicates the end of a top level event.
qoo10	query	Contains query metadata sent to the server.
qoo10	query_raw	Contains the query sent to the search engine as indicated in the URL.
qoo10	query_text	Query sent to the search engine.
qoo10	subcategory_id	Id of the subcategory.
qoo10	subcategory_name	Subcategory name the product belongs to.
qoo10	view	Parent attribute containing viewed item metadata.
qoo10	view_category_id	Category Id of the viewed item.
qoo10	view_category_name	Category name of the viewed item.
qoo10	view_item_id	Id of the viewed item.
qoo10	view_item_name	Name of the viewed item.
qoo10	view_subcategory_id	Subcategory Id of the viewed item.
qoo10	view_subcategory_name	Subcategory name of the viewed item.
sgcarmart	car	Parent attribute containing vehicle'description.
sgcarmart	category	Vehicle category.

Protocol	New event attribute	Description
sgcarmart	end	Indicates the end of a top level event.
sgcarmart	model	Model of the vehicle.
sgcarmart	price	Sell price of the car.
sgcarmart	query	Contains query metadata sent to the server.
sgcarmart	query_raw	Contains the query sent to the search engine as indicated in the URL.
sgcarmart	query_text	Query sent to the search engine.
sgcarmart	type	vehicle type.
skype	service_stats	Composite attribute containing the packet metrics used for each new service type detection. Note: this attribute won't be extracted in case of session expiration (eg. when the current service is not ended properly by the user).
smb	host	Server name (NTLMSSP).
smb	krb5_blob	Data contained in the KRB5 security blob.
stun	remote_address_ipv4	IPv4 address of the distant peer as seen from the STUN relay server.
tango	service_stats	Composite attribute containing the packet metrics used for each new service type detection. Note: this attribute won't be extracted in case of session expiration (eg. when the current service is not ended properly by the user).
tds	login_encrypted	This attribute is set to one if the login phase is encrypted. Implemented conforming to the Microsoft 2014 MS-TDS official specification (http://msdn.microsoft.com/en-us/library/dd304523.aspx); beware, the behaviour may be different with old releases of MS SQL Server not supporting the standard.
tigerair	departure_date	Departure date.
tigerair	end	Indicates the end of a top level event.
tigerair	flight_search	Parent attribute containing flight search metadata.
tigerair	from_airport	Departure airport.
tigerair	nr_adult	Number of adults passenger.
tigerair	nr_child	Number of children passenger.
tigerair	nr_infant	Number of infant passenger.
tigerair	return_date	Return date.
tigerair	to_airport	Destination airport.
toggle	category	Category of the video.
toggle	end	Indicates the end of a top level event.
toggle	query	Contains query metadata sent to the server.
toggle	query_raw	Contains the query sent to the search engine as indicated in the URL.

Protocol	New event attribute	Description
toggle	query_text	Query sent to the search engine.
toggle	query_type	Sort of query sent to the search engine.
toggle	video	Parent attribute containing video metadata.
toggle	videoid	Id of the streamed video.
wechat	service_stats	Composite attribute containing the packet metrics used for each new service type detection. Note: this attribute won't be extracted in case of session expiration (eg. when the current service is not ended properly by the user).
whatsapp	service_stats	Composite attribute containing the packet metrics used for each new service type detection. Note: this attribute won't be extracted in case of session expiration (eg. when the current service is not ended properly by the user).
zuji	departure_date	Departure date.
zuji	end	Indicates the end of a top level event.
zuji	flight_search	Parent attribute containing global flights search metadata.
zuji	flight_stop	Parent attribute containing one flight search metadata.
zuji	from_airport	Departure airport.
zuji	from_city	Departure city.
zuji	from_country	Departure country.
zuji	nr_adult	Number of adults passenger.
zuji	nr_child	Number of children passenger.
zuji	nr_infant	Number of infant passenger.
zuji	return_date	Return date (wrong value if trip_type is OneWay or Multistop).
zuji	search_id	Id of the flight search.
zuji	to_airport	Destination airport.
zuji	to_city	City destination.
zuji	to_country	Country destination.
zuji	trip_type	Type of the trip (one way, return or multi city/stopover).

5.3.2. Event Attributes deprecated in this version

The following Event Attributes have been deprecated:

Table 17. Deprecated Event Attributes

Protocol	Deprecated event attributes	Comments
smb	domain	session_mod, client, string, request
		session_mod, both, string, request
youtube	description	session_prt, client, string, video
		session_prt, both, string, video

Protocol	Deprecated event attributes	Comments
youtube	tags	session_prt, client, string, video
		session_prt, both, string, video
youtube	title	session_prt, client, string, video
		session_prt, both, string, video
youtube	url	session_prt, client, string, video
		session_prt, both, string, video
youtube	videoid	session_prt, client, string, video
		session_prt, both, string, video

5.3.3. Event Attributes modified in this version

No Event Attributes have been modified in this version.

5.4. Bug Fixes and Known Issues

5.4.1. Bug Fixes

- SF#08305 - RTC#13621 - **[SMTP] Attribute attach_content has extra character at the end/**

Bug Info	Description
Reported against	ProtocolBundle-1.40.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Remove extra character at the end of the attachment.

- SF#09007 - RTC#17961 - **Pdata - icmp based custom signature is not working**

Bug Info	Description
Reported against	ProtocolBundle-1.40.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Custom signature based on both icmp:typeval and icmp:code is not working.

- SF#09018 - RTC#17837 - **[asn1] Type on more than one byte is wrongly tested**

Bug Info	Description
Reported against	ProtocolBundle-1.81.0-20
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	[asn1] Type on more than one byte is wrongly tested

- SF#09062 - RTC#18098 - **[MEgaco/H248] Extra character in extraction of h248_text:call_id**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-21
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	[MEgaco/H248] Extra character in extraction of h248_text:call_id (the extra character seems to be context_id)

- SF#08976 - RTC#17399 - **[edonkey] Wrong classification over HTTP**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Wrong classification for the protocol edonkey over http

- SF#000007001 - RTC#15021 - **[smb] NTLM attributes extraction issue**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-21
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	New attributes related to NTLM added in SMB protocol

- SF#09123 - RTC#17314 - **[ldap] unitary test failed**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Fixed LDAP unitary attribute extraction.

- SF#08988 - RTC#18171 - **[viber] improve classif**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[viber] improved classification

- SF#09079 - RTC#18197 - **[spdy] ssl is not a bottom layer of spdy**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-21
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	[spdy] ssl is mentionned as a bottom layer of spdy

- SF#09030 - RTC#17884 - **[protocols.xml] Virtual protocols don't contain list of bottom layers (over_list)**

Bug Info	Description
Reported against	ProtocolBundle-1.82.0-20
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	"Over" tags missing for virtual protocols in PB 1.81, 1.82, ...

- SF#08972 - RTC#17345 - **[aim] aim does not handle 2-byte messages properly + minor feature request (full message)**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-22
Platform	All

Bug Info	Description
Effect of bug	Extraction Anomaly
Expected versus actual behavior	[AIM] Message UTF-16 handling fixed; Full message event added

5.4.2. Known Issues

- SF#09031 - RTC#17972 - **[doc][perfect_dark] perfect_dark does not contain any bottom_layers in protocols.xml (should be spid)**

Bug Info	Description
Reported against	ProtocolBundle-1.82.0-20
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	spid is missing as bottom layer for perfect_dark
Workaround	No workaround

- SF#09037 - RTC#18009 - **[PB -1.80.0-23]: tcp:wrong_crc causes failed extraction of other protocol attributes**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-22
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	When tcp:wrong_crc attribute is included in the analysis job, ixEngine fails to extract other protocol attributes of the second half-session in the attached trace file. For example all ip protocol attributes are missing. When running the same analysis job with PB1.62.0-20 this does not happen.
Workaround	No workaround

- RTC#17651 - **[youtube] can't extract description, title**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-22
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Youtube attributes title and description are not extracted
Workaround	No workaround

- SF#08889 - RTC#16676 - **[INTFLOW][reass] seq number tracking issue when uapp_cnx created with RST packet**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-22
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	[INTFLOW][reass] fixed seq number tracking issue when uapp_cnx created with RST packet
Workaround	No workaround

6. Protocol Bundle 1.90.0

6.1. What's new in the Protocol Bundle 1.90.0

6.1.1. Major enhancements in this release

12 new Protocols added, and 1 deprecated. See Section 6.2, “Protocols”

2 new Event Attributes added, 10 deprecated, and 2 modified. See Section 6.3, “Attributes”

- The availability of a new DNS caching feature for extended classification.
- The support of the secured profile of rtcp protocol (srtcp).
- The support of IPSEC clear payload encapsulation (for ixE INTFLOW),
- Optimizations in HTTP packets parsing for non-proxy requests (for ixE INTFLOW)
- New protocols classification and metadata extraction (See also Section 6.2.3, “Additional Protocol Modifications”).

Note:

- The `DNS Cache` feature is enabled (by default) by a new proto-tune located in the DNS protocol (cf. Protobook).

  This feature uses captured DNS answers to predict and improve classification of certain protocols (example: gtalk, thunder, skype).
- The `Q_HTTP_COOKIE` metadata extraction is changed: the Cookie HTTP header full value is now extracted at once in this attribute.

Additional notes:

- The new optimized “http declassification on non-proxy requests” feature (ixEngine Internal-Flow-mode only) causes some valid regressions in legacy protocols (soap, groupwise, zimbra),
- Changes to the viber protocol are causing false positive and negative classifications, a fix is planned for the next release.

6.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.
- ixEngine 4.19.x versions 4.19.0-20 and higher.

Note:

Issues specific to ixEngine version 4.19.0:

- Please refer to the *ixEngine 4.19.0 Developer's Manual* for information about *Basic DPI*.
- *Basic DPI* restrictions and important notes are documented in the Protobook (example: http plug-in).
- HTTP Cookie *Basic DPI* extraction is not up-to-date compared to the new Q_HTTP_COOKIE extraction.
- Some classification issues remain with ixEngine 4.19.0, to be corrected with a future PB minor release, concerning : nfs, bbm_audio (stun), bbm_video (stun), line (stun), lync (stun), amazon_video (rtmp), soap, funshion, rpc.

6.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don’t have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

6.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2

- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3

6.2. Protocols

6.2.1. New Protocols

The following new protocols have been added in this version:

Table 18. New protocols added in this version

Proto ID	Protocol	Description
2283	5pmweb	5pmweb is a web-based project and task management software for teams.
2293	dhcp6	The DHCPv6 protocol is used to automatically configure the network parameters of a station in an IPv6 network.
2307	golden_village	Singaporian online cinema ticket booking.
2305	hungrygowhere	Singaporean fooding website.
2304	jobsdb	Job seeking website.
2308	mailru_agent	Mail.ru Agent is a cross-platform mobile messaging application supporting text, audio and video. It is featured by Mail.ru.
2296	qoo10	Singaporian online fashion and trend shopping market.
2306	sgcarmart	Singaporean online car market.
2291	teltel	VOIP software which allows calling other teltel users.
2297	tigerair	Singaporian online travel agency.
2295	toggle	Singaporian video streaming website.
2298	zuji	Singaporean online travel agency.

6.2.2. Deprecated Protocols

The following protocols have been deprecated in this version:

Table 19. Deprecated protocols in this version

Proto ID	Protocol	Description	Comments
719	esp	The esp protocol (Encap Security Payload) is found over the IP layer (IANA protocol number: 50). See IPsec.	

6.2.3. Additional Protocol Modifications

Ticket ID	Description
SF#000007751 - RTC#10271	**[ipsec] support for Null encrypted ESP payload detecting an encapsulation**
SF#07909 - RTC#11118	**[mailru_agent] Classification and metadata extraction**
SF#07908 - RTC#11121	**[ssl] metadata of cipher_suite_id**
RTC#11147	**[http][declassify] http declassification prevented for non-proxy traffic**

Ticket ID	Description
RTC#15190	**[chat_on] improve classification over tcp**
RTC#15236	**[gnutella] improve classification over udp**
RTC#15386	**[line] improve classification over udp**
RTC#15404	**[mypeople_messenger] improve classification over udp**
RTC#15471	**[iqiyi] added new UDP stream classification**
RTC#15750	**[skype]improve classification on android over tcp**
RTC#16464	**[ustream] improve classification over udp and tcp**

6.3. Attributes

This section describes the updates to Attributes.

6.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

6.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

6.3.1.2. Event Attributes added in this version

Table 20. Added Event Attributes

Protocol	New event attribute	Description
ip	resolv_name	Private attribute of the classification engine.
ssl	cipher_suite_id	Id of the cipher suite handled by the server.

6.3.2. Event Attributes deprecated in this version

The following Event Attributes have been deprecated:

Table 21. Deprecated Event Attributes

Protocol	Deprecated event attributes	Comments
line	call	Parent entry, empty, for fields belonging to the call (caller, callee, etc.).
line	call_duration	Call duration.
line	call_id	Call id, extracted for each call.
line	callee	Contains the identity (or the phone number) of the called party for a call.
line	caller	Contains the identity (or the phone number) of the initiator of the call.
line	caller_addr	Address which could be used by the initiator of the call.
line	start_time	Start date of the call.
line	user_agent	Name of the software used.
live_hotmail	contact	Complete contact.
paltalk_transfer	sender	Contains the identity of the sender of a file transfer.

6.3.3. Event Attributes modified in this version

The following Event Attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 22. Modified Event Attributes

Protocol	Event attribute	Changes
s1ap	ep_ie	session_prt, both, string, ep
		session_prt, both, parent, ep
s1ap	ep_ie_rab	session_mod, both, string, ep_ie
		session_mod, both, parent, ep_ie

6.4. Bug Fixes and Known Issues

6.4.1. Bug Fixes

- SF#72457245,8704,8720 - RTC#6629 - **[rtcp] classification issue in case of Lync usage (srtcp)**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	The SRTCP part of Lync workflow isn't completely correctly detected. This development adds support for the secure profile classification in the rtcp plug-in.

- SF#07109 - RTC#9448 - **[ultrasurf] Ultrasurf cannot be blocked - Clavister**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-2x
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[ultrasurf] Ultrasuft cannot be blocked

- SF#08184 - RTC#13221 - **[teamspeak_v3] poor classification of teamspeak_v3 traffic**

Bug Info	Description
Reported against	ProtocolBundle-1.31.0-20.002
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Poor classification of teamspeak_v3 traffic

- SF#08288 - RTC#13348 - **[speedtest] improve classification**

Bug Info	Description
Reported against	ProtocolBundle-1.40.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[speedtest] improve speedtest classification

- SF#06567 - RTC#13502 - **[https] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	HTTPS classification issue

- RTC#14035 - **[l2tp] [octeon2] inversion of tunnel_id and call_id values**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	OCTEON2
Effect of bug	Extraction Anomaly
Expected versus actual behavior	

- RTC#14806 - **[pdl][doc] "udp" and "tcp" missing as bottom layers of apple_airplay**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-2x
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	"udp" and "tcp" missing as bottom layers of apple_airplay

- SF#08801 - RTC#15807 - **[appstore] missing classification**

Bug Info	Description
Reported against	ProtocolBundle-1.62.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Missing appstore classification

- RTC#15310 - **[krb5] fix typo**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-2x
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	[krb5] fix typo

- SF#08775 - RTC#15704 - **[ssl]Attribute organization_name is wrongly extracted**

Bug Info	Description
Reported against	ProtocolBundle-1.72.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	ssl:organization_name should be extracted from the Certificates/Certificate/signedCertificate/subject (not from the Certificates/Certificate/signedCertificate/issuer)

- SF#08797 - RTC#15709 - **[http] Attributes http:uri_xxx are not extracted for a simple request in http version 0.9**

Bug Info	Description
Reported against	ProtocolBundle-1.72.0-20
Platform	All

Bug Info	Description
Effect of bug	Extraction Anomaly
Expected versus actual behavior	HTTP uri atributes are not extracted for a simple request in http v 0.9

- SF#08695 - RTC#15826 - **[build] fix some protocol dependency issues**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-2x
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	[build] fix some protocol dependdency issues

- SF#08800 - RTC#15833 - **pcanywhere.com is not classified**

Bug Info	Description
Reported against	ProtocolBundle-1.72.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	pcanywhere.com is not classified

- RTC#16143 - **[SF8825]Failed to detect Bittorrent Sessions in live setup.**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Failed to detect Bittorrent

- SF#08830 - RTC#16200 - **http:video_type=mp2t is extracted for each packet**

Bug Info	Description
Reported against	ProtocolBundle-1.72.0-20
Platform	All
Effect of bug	Performance Anomaly
Expected versus actual behavior	http:video_type=mp2t is extracted for each packet

- SF#09021 - RTC#17818 - **[hudong] reported depracted in PB1.42 documentation but not in PB code**

Bug Info	Description
Reported against	ProtocolBundle-1.80.0-22
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	hudong not depracted as it was stated in the PB 1.42 release note.

6.4.2. Known Issues

- SF#69376937,7243 - RTC#3365 - **[SF6937][ul3l4_cache_print_state] [print_LINE] better output**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	improve ul3l4_cache_print_state output
Workaround	No workaround

- SF#74237423 - RTC#7068 - **[SF 7423] [http] normalization cases not supported (duplicated slashes, empty query, dot-segtments)**

Bug Info	Description
Reported against	ProtocolBundle-1.40.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	duplicated slashes, empty query and dot-segtments cases are not supported
Workaround	No workaround

- SF#07658 - RTC#9444 - **[http][bmff] datarate extraction seems to be missing**

Bug Info	Description
Reported against	ProtocolBundle-1.30.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	ask for help on http/bmff
Workaround	No workaround

- SF#08004 - RTC#11976 - **[thunder] improve classification of thunder 5.xx**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	x86 OCTEONPLUS OCTEON2 SMP AMP
Effect of bug	Classification Anomaly
Expected versus actual behavior	Improve thunder classification.
Workaround	No workaround

- SF#08039 - RTC#12708 - **[SF 8039] Possible memory leak in the appsdk module**

Bug Info	Description
Reported against	ProtocolBundle-1.31.0-20.002
Platform	All
Effect of bug	Memory Leak
Expected versus actual behavior	Possible memory leak in the appsdk module

Bug Info	Description
Workaround	No workaround

- SF#08325 - RTC#14719 - **[skype] audio call service not detected**

Bug Info	Description
Reported against	ProtocolBundle-1.40.0-22
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	skype audio call service detection does not provide bidir records.
Workaround	N/A

- SF#08930 - RTC#14729 - **[doc] Proto tune tcp:enable_reassembly documentation is outdated**

Bug Info	Description
Reported against	ProtocolBundle-1.62.0-21
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	[doc] tcp:enable_reassembly proto tune documentation outdated
Workaround	No workaround

- SF#07000 - RTC#14816 - **[krb5] Incorrect bounds over ldap**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-2x
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	KRB5 bounds inside LDAP are wrong
Workaround	No workaround

- SF#08622 - RTC#14819 - **[doc][proto_getlist] Lists of bottom layers are incomplete**

Bug Info	Description
Reported against	ProtocolBundle-1.70.0-20
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	Lists of bottom layers are incomplete
Workaround	No workaround

- SF#08695 - RTC#15726 - **[build] fix CFG_ZLIB=n build**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-2x
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	[build] fix CFG_ZLIB=n build

Bug Info	Description
Workaround	No workaround

- SF#08704 - RTC#17546 - **[rtcp] Packet type : Payload-specific is not rightly classified as RTCP**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-2x
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[rtcp] Packet type : Payload-specific is rightly classified as RTCP
Workaround	No workaround

- RTC#17919 - **Basic-dpi limitations**

Bug Info	Description
Reported against	ProtocolBundle-1.90.0-2x
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Classification limitations with Basic DPI on aim, baidu, baofeng, bittorrent, facetime, ftp, gmail, google_ads, google_gen, google_toolbar, gotomeeting, ppfilm, qq, rtmp, silverlight, skype, spdy, spotify, ssh, thunder, ultrasurf, yahoo, ymail, apple_airprint, babycenter, bbm_audio, bbm_video, deezer, gnutella, ica, jabber, mmse, netflix, opera_update, owa, phproxy, rss, sharepoint_admin, sharepoint_document, shoutcast, soap, wechat, windows_live, capwap, conviva, dimp, filetopia, groupwise, http_tunnel, ircs, jedi, leboncoin, msn, nba, shazam and uusee (see ProtoBook for details).
Workaround	No workaround

7. Protocol Bundle 1.82.0

7.1. What's new in the Protocol Bundle 1.82.0

7.1.1. Major enhancements in this release

13 new Protocols added. See Section 7.2, “Protocol Updates”

Summary of major enhancements :

Ticket ID	Description
RTC#12516	**[carbonite] added support of HTTP layer**
RTC#12535	**[wrike] added support of HTTP layer**
RTC#12568	**[goplan] added support of HTTP layer**
RTC#14121	**[inneractive] added protocol**
RTC#14834	**[adobe] added demdex classification**
RTC#15585	**[samsung] added protocol**
RTC#16301	**[nba] improved classification**
RTC#16361	**[google_plus] improved classification**
RTC#16519	**[odnoklassniki]improved classification**
RTC#16542	**[itunes] improved classification**
RTC#16569	**[mailru] added classification on mradx host**
RTC#16577	**[blogger] improved classification**
RTC#16609	**[plurk] added classification on iOS**
RTC#16637	**[google_earth] improved classification**
RTC#16707	**[depositfiles] improved classification**
RTC#16762	**[steam] improved classification over akamai**

7.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

7.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don’t have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

7.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

7.2. Protocol Updates

7.2.1. New Protocols

The following new protocols have been added in this version:

Table 23. New protocols added in this version

Proto ID	Protocol	Description
2314	carbonite	This signature detects Carbonite, a service that manages online backups.
2301	crittercism	Crittercism is a mobile application for performance management.
2302	digitalriver	Digital River is a public company that provides internet commerce services.
2311	egloos	Egloos is a South Korean blog hosting website.
2300	flurry	Flurry provides services to optimize customer's mobile experience through apps and personalized ads.
2316	goplan	Goplan is an online project management and collaboration tool for individuals and teams.
2299	inneractive	Inneractive is a monetizer for cross-platform mobile applications.
2318	nate_mail	Nate Mail is a South Korea webmail.
2312	naver_blog	Naver Blog is a South Korean blog hosting website.
2317	sabameeting	Saba Meeting is a web conferencing and desktop sharing service.
2303	samsung	Samsung is a South Korean multinational company.
2315	wrike	Wrike is web-based project management software that gives you full visibility and control over your projects.
2313	yodiz	Yodiz is online Agile Project Management tool.

7.3. Attributes

There are no new Attributes to report in this version.

7.4. Bug Fixes and Known Issues

7.4.1. Bug Fixes

There are no Bug Fixes in this version.

7.4.2. Known Issues

There are no new Known Issues to report in this version.

8. Protocol Bundle 1.81.0

8.1. What's new in the Protocol Bundle 1.81.0

8.1.1. Major enhancements in this release

14 new Protocols added. See Section 8.2, “Protocol Updates”

Summary of major enhancements :

Ticket ID	Description
RTC#7128	**[wsop] Added new protocol World Series of Poker WSOP (Game)**
RTC#7131	**[zombie_tsunami] Added new protocol Zombie Tsunami (Game)**
RTC#7132	**[6play] Added new protocol 6play (Audio/Video)**
RTC#12202	**[magicjack] Added new protocol for classification only**
RTC#12538	**[VIEWPATH] Added support over HTTP**
RTC#12541	**[ROBOFORM] Added support over HTTP**
RTC#12557	**[DESKAWAY] HTTP Traffic is not detected.**
RTC#13912	**[openstreetmap] Added new protocol openstreetmap**
RTC#13925	**[criteo] Added new protocol criteo**
RTC#14381	**[adobe] Added new protocol adobe**
RTC#14880	**[videoplaza] Added new protocol videoplaza**
RTC#14974	**[zendesk] Added new protocol zendesk**
RTC#15298	**[google_maps] Updated description**
RTC#15324	**[psn] Added classification**
RTC#15337	**[cnet] Improved classification (France)**
RTC#15401	**[mitalk] Improved classification**
RTC#15407	**[Silverlight] Added classification based on file extension**
RTC#15440	**[cnet] Added classification on cbsistatic.com**
RTC#15443	**[chat_on] Added classification over amazon_aws**
RTC#15486	**[twitpic] Improved classification**
RTC#15518	**[orangemail] Added classification on old host**
RTC#15524	**[tu] Added ssl Classification**
RTC#15540	**[windows_update] Added Classification**
RTC#15590	**[samsung_apps] Improved classification (run_05)**
RTC#15633	**[dailymotion] Improved classification**
RTC#15642	**[orangemail] Added host classification**
RTC#15657	**[ymsg_webmessenger] Improved classification**
RTC#15810	**[ymail2] Improved classification**
RTC#15813	**[ymail_mobile_new] Updated description**
RTC#16021	**[ymail_mobile_new] Improved classification (run_06)**
RTC#16367	**[psn] Improved classification over https**

8.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

8.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot-swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

8.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1

- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

8.2. Protocol Updates

8.2.1. New Protocols

The following new protocols have been added in this version:

ID	Name	Description
2292	6play	French mobile application provifing live tv broadcast and catchup TV.
2280	adobe	Adobe Systems is a computer software company. It develops graphic designer software and Audio and Video editing and visual effects. This plug-in classifies traffic to the website.
2279	criteo	Criteo is a personalized retargeting company.
2287	deskaway	DeskAway is web-based team and project management software that makes it easy to organize, manage and track projects from a central location.
2288	google_safebrowsing	Google Safe Browsing is a web-service and API for checking web pages against threats. This signature detects a Google Safebrowse Submission.
2284	magicjack	MagicJack is a VoIP service for home and business use, available as a mobile application and also with a proprietary device (magicJack PLUS).
2278	openstreetmap	OpenStreetMap is an open geographical database.
2286	roboform	Roboform is a password management and web form filling program.
2277	truste	TRUSTe is the leading online privacy management services provider offering a broad suite of consumer, advertising, mobile, cloud and data privacy solutions.
2281	videoplaza	Videoplaza provides tools to broadcasters, publishers and networks to maximise their advert revenues from their video content.
2285	viewpath	Viewpath is an online project management and collaboration tool.
2289	wsop	Mobile game.
2282	zendesk	Zendesk is a cloud-based customer service platform, that includes ticketing, self-service options, and customer support features.
2290	zombie_tsunami	Mobile game.

8.2.2. Deprecated Protocols

No protocols have been deprecated in this version.

8.3. Attributes

This section describes the updates to Attributes.

8.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

8.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

8.3.1.2. Event Attributes added in this version

No Event Attributes have been added in this version.

8.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

8.3.3. Event Attributes modified in this version

No Event Attributes have been modified in this version.

8.4. Bug Fixes and Known Issues

8.4.1. Bug Fixes

- RTC#15318 - **[viber] add amazon_aws in the path**

Bug Info	Description
Reported against	ProtocolBundle-1.71.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification Anomaly.

- RTC#15410 - **[apple_hls]missing classification**

Bug Info	Description
Reported against	ProtocolBundle-1.71.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification Anomaly.

- RTC#15454 - **[ymail2] wrongly classified as ymail_mobile_new**

Bug Info	Description
Reported against	ProtocolBundle-1.72.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	ymail2 encrypted traffic is wrongly classified as ymail_mobile_new

- RTC#15463 - **[iqiyi] Missing Classification**

Bug Info	Description
Reported against	ProtocolBundle-1.72.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Missing classification

- RTC#15533 - **[windowslive] missing classification**

Bug Info	Description
Reported against	ProtocolBundle-1.71.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification Anomaly.

- RTC#15537 - **[yahoo] add classification**

Bug Info	Description
Reported against	ProtocolBundle-1.71.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification Anomaly.

- RTC#15654 - **[spotify] add amazon_aws in the path**

Bug Info	Description
Reported against	ProtocolBundle-1.72.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification Anomaly.

8.4.2. Known Issues

There are no new Known Issues to report in this version.

9. Protocol Bundle 1.80.0

9.1. What's new in the Protocol Bundle 1.80.0

9.1.1. Major enhancements in this release

- New *PDB Swap* Feature and associated Code Sample (see Section 9.1.3, “Installation procedure” and attached TechNote),
- DNS: PDATA HTTP hostname resolution (IPv4 responses),
- 2 new Protocols Signature Plug-ins added (doodle_jump, telegram), 1 deprecated (youtube_hd), see Section 9.2, “Protocol Updates”,
- 8 new Event Attributes added, 1 updated (apple_update), see Section 9.3, “Attribute Updates”.

Ticket ID	Description
RTC#7118	**[doodle_jump] new protocol Doodle Jump (Game)**
RTC#11098	**[radius] 3 new attributes**
RTC#11115	**[ymsg] new metadata conference_id**
RTC#11270	**[telegram] added classification**
RTC#14485	**[youku] improved classification**
RTC#11967	**[youtube] Youtube/YoutubeHD classification unification + new video metadata extraction**
RTC#11970	**[dns] application detection using PDATA on reply hostname**
RTC#12532	**[tcp] new proto tune for TCP SYN timeout**
RTC#12608	**[ares] added classification over udp**
RTC#12635	**[chat_on] improved classification on Bada device**
RTC#12693	**[qq] added classification on tcp**
RTC#12801	**[tango] improved classification**
RTC#13413	**[VoIP Protocols] New metadata service stats_info**
RTC#13894	**[line] Landline Call detection**
RTC#14168	**[line] [tango] [facetime.] add proto tunes for service**
RTC#14287	**[steam] added classification over tcp**
RTC#14340	**[kapersky_update] improved classification over tcp**
RTC#14397	**[viber] improved classification over udp**
RTC#14461	**[baidu] improved classification over tcp**
RTC#14517	**[twitter] improved classification**

9.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.

- ixEngine 4.18.x versions 4.18.0-26 and higher.

9.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

9.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

9.2. Protocol Updates

9.2.1. New Protocols

The following new protocols have been added in this version:

ID	Name	Description
2252	doodle_jump	Mobile game developped by Lima Sky LLC
2240	telegram	Telegram is an instant messaging protocol like Whatsapp.

9.2.2. Deprecated Protocols

The following protocols have been deprecated in this version:

ID	Name	Description
558	youtube_hd	Youtube HD classification ensures that the user is watching a High Definition video (at least 720 lines).

9.3. Attribute Updates

9.3.1. New Event Attributes added in this version

9.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

9.3.1.2. Event Attributes added in this version

Protocol	Attribute	Description
dns	web_application_info	Structure containing metadata for classification of known HTTP-based web applications. These metadata are based on Type A (IPv4) DNS responses returned from the server. The ul3l4_addr_t structure contains the web application protocol path, classified using the requested host name, and the IPv4 address resolved by the server. The hostname lookup is performed on Q_HTTP_SERVER registered PDATA signatures only.
radius	delegated_ipv6_prefix	Provides the ipv6 prefix to be delegated to the user.
radius	framed_ip_netmask	IP netmask.
radius	framed_ipv6_prefix	Provides the ipv6 prefix to be configured for the user.
stun	magic_cookie	The magic cookie used to deobfuscate the XOR port and XOR mapped address
ymsg	conference_id	room identifier for a given conference
youtube	video_avgdatarate	Average video bitrate in kilobits per second.
youtube	video_type	File format.

9.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

9.3.3. Event Attributes modified in this version

The following Event Attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Protocol	Attribute	Updates (Before/After)
apple_update	pkg_name	session_fix, client, string, no_parent
		session_mod, both, string, no_parent

9.4. Bug Fixes and Known Issues

9.4.1. Bug Fixes

- RTC#10056 - **[hotspot_shield] Classification issue (2nd part: OpenSSL issue)**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	In some cases, Hotspot Shield isn't detected as it should be

- RTC#10833 - **[rtmp] extraction issue (page_url, etc.)**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Metadata extraction issues on rtmp.

- RTC#13279 - **[ppfilm] Video streams not classified**

Bug Info	Description
Reported against	ProtocolBundle-1.70.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[ppfilm] Video streams not classified

- RTC#13496 - **[irc] misclassified as ftp**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	IRC misclassified as FTP.

- RTC#13932 - **[imap] attach filename extraction fix**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	[imap] Content-Type "name=" value is set if no "filename=" value is found in Content-Disposition header

- RTC#14165 - **[thepiratebay] thepiratebay over ssl is not detected**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	thepiratebay over ssl is not detected

- RTC#14413 - **[SIP] extraction issue with CRLF in header value**

Bug Info	Description
Reported against	ProtocolBundle-1.70.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	\r\n in SIP header values are not supported and cause extraction issues with the subsequent headers

- RTC#15663 - **SPID disabled on cOS platform**

Bug Info	Description
Reported against	ProtocolBundle-1.72.0-20
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	SPID disabled on cOS platform

9.4.2. Known Issues

- RTC#12402 - **[SF 8041] Callback for Q_HTTP_FORWARD_ADDR does not handle IPv6 addresses**

Bug Info	Description
Reported against	ProtocolBundle-1.30.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Callback for Q_HTTP_FORWARD_ADDR does not handle IPv6 addresses
Workaround	No workaround

- RTC#13491 - **[viber] bad service detection**

Bug Info	Description
Reported against	ProtocolBundle-1.70.0-20
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Viber: bad service detection
Workaround	No workaround

10. Protocol Bundle 1.72.0

10.1. What's new in the Protocol Bundle 1.72.0

10.1.1. Major enhancements in this release

28 new Protocols added. See Section 10.2, “Protocol Updates”

Summary of major enhancements :

Ticket ID	Description
RTC#6048	**[kakaostory] Added new protocol KakaoStory (Web)**
RTC#6069	**[aol_on] Added new protocol Aol On (Web)**
RTC#7098	**[bitstrips] Added new protocol Bitstrips (Application Service)**
RTC#7096	**[plants_vs_zombies] Added new protocol Plants vs. Zombies (Game)**
RTC#7113	**[free_music_download] Improved classification**
RTC#7114	**[empire_four_kingdoms] Added new protocol Empire: Four Kingdoms (Game)**
RTC#7116	**[pou] Added new protocol Pou (Game)**
RTC#7121	**[skee_ball_arcade] Added new protocol Skee Ball Arcade (Game)**
RTC#7122	**[quizup] Added new protocol QuizUp: The biggest trivia game in the world! (Game)**
RTC#11862	**[tower_of_saviors] Added classification**
RTC#13822	**[livemail_mobile] Updated description**
RTC#13909	**[fsecure] new protocol**
RTC#14007	**[symantec] new protocol**
RTC#14225	**[oracle] new protocol**
RTC#14511	**[spotify] Improved classification**
RTC#14662	**[nba] Improved classification on android**
RTC#14830	**[google_analytics] Improved classification**
RTC#14862	**[mypeople_messenger] Improved classification over http**
RTC#14871	**[tumblr] Improved classification over https**
RTC#14874	**[facebook_mail] Updated description**
RTC#14877	**[tv4play] Improved classification**
RTC#14886	**[viber] Improved classification over http**
RTC#14926	**[flickr] Updated description**
RTC#14939	**[gmail] Improved classification**
RTC#14942	**[gmail_basic] Updated description**
RTC#14945	**[grooveshark] Improved classification**
RTC#14965	**[kik]Improved classification**
RTC#15078	**[spotify] Added classification on scdn.co**
RTC#15102	**[youtube] Improved classification**
RTC#15132	**[qq_games] Improved classification**

Ticket ID	Description
RTC#15135	**[qq_web] Improved classification**
RTC#15138	**[touch] Improved classification**
RTC#15280	**Added new protocols from the monthly list of top worldwide websites**

10.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

10.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don’t have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

10.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2

- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

10.2. Protocol Updates

10.2.1. New Protocols

The following new protocols have been added in this version:

Table 24. New protocols added in this version

Proto ID	Protocol	Description
2265	albawabhnews	Egyptian news portal.
2264	almasryalyoum	Egyptian news portal.
2272	amjilt	Mongolian news portal.
2269	ammonnews	Jordanian news portal.
2257	aol_on	AOL On is a video streaming web site.
2253	bitstrips	BitStrips allows to design cartoon versions of yourself and your friends.
2263	dba	Danish classified ads website.
2268	discuss	Hong Kongese forum about media and lifestyle.
2260	empire_four_kingdoms	Mobile game
2271	essahraa	Mauritanian news portal.
2262	expatriates	International Classified Ads website for expatriates.
2249	fsecure	F-Secure Corporation is a Finnish computer security company
2247	huffington_post	The Huffington Post is an American online news aggregator and blog.
2270	independent	Irish news portal.
2258	kakaostory	KakaoStory is a photo sharing social networking service for KakaoTalk users
2248	onelife	OneLife is a service of travelling photo sharing. Users can sort their Instagram photos by countries and follow other travelers.
2251	oracle	Oracle Corporation is multinational computer technology corporation. The company specializes in developing and marketing computer hardware systems and enterprise software products, particularly its own brands of database management systems.
2256	plants_vs_zombies	Plants vs Zombie is a mobile game.
2254	pou	Mobile game
2274	prensa	Panamanian news portal.
2267	prensalibre	Guatemalan news portal.
2255	quizup	Mobile game
2261	skee_ball_arcade	Mobile game
2250	symantec	Symantec Corporation makes security, storage, backup and availability software.
2266	tonaton	Ghanean classified ads website.
2259	tower_of_saviors	Mobile game
2275	trinidadexpress	Trinidadian news portal.
2273	wattan	Palestinian multimedia news website.

Proto ID	Protocol	Description
2276	webtretho	Vietnamese women lifestyle website.

10.2.2. Deprecated Protocols

No protocols have been deprecated in this version.

10.3. Attributes

This section describes the updates to Attributes.

10.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

10.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

10.3.1.2. Event Attributes added in this version

No Event Attributes have been added in this version.

10.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

10.3.3. Event Attributes modified in this version

No Event Attributes have been modified in this version.

10.4. Bug Fixes and Known Issues

10.4.1. Bug Fixes

There are no Bug Fixes in this version.

10.4.2. Known Issues

There are no new Known Issues in this version.

11. Protocol Bundle 1.71.0

11.1. What's new in the Protocol Bundle 1.71.0

11.1.1. Major enhancements in this release

Summary of major enhancements :

11 new Protocols added (angry_birds, burt, candy_crush_saga, king, nokia, quantcast, rovio, scorecardresearch, subway_surfers, turn, waze) and 6 deprecated. See Section 11.2, “Protocol Updates”

Improved classification for two dozen protocols.

Ticket ID	Description
RTC#13918	**[sina_weibo] improved classification**
RTC#13906	**[apple_update] improved classification**
RTC#13903	**[google_play] improved classification**
RTC#13891	**[cnet] improved classification over rtmp**
RTC#13885	**[babycenter] improved classification**
RTC#12562	**[ppstream] improved classification**
RTC#14378	**[flashplugin_update] improved classification**
RTC#14196	**[kaspersky_update] added classification**
RTC#14098	**[4shared] improved classification**
RTC#14018	**[google_maps] improved classification**
RTC#13994	**[aim] improved classification**
RTC#13983	**[steam] improved classification**
RTC#13953	**[twitpic] improved classification**
RTC#13944	**[wordpress] improved classification**
RTC#14610	**[flashplugin_update] improved classification on windows8**
RTC#14469	**[nba] improved classification**
RTC#14428	**[flickr] improved classification**
RTC#14357	**[nba] improved classification**
RTC#14322	**[java_update] improved classification**
RTC#14316	**[norton_update] improved classification**
RTC#14313	**[kaspersky] improved classification**
RTC#14275	**[windows_update] improved classification over ssl**
RTC#14265	**[cnn] improved classification**
RTC#14250	**[blogger] improved classification**

11.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.

- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

11.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

11.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

11.2. Protocol Updates

11.2.1. New Protocols

The following new protocols have been added in this version:

Table 25. New protocols added in this version

ID	Name	Description
2242	angry_birds	Angry Birds is a mobile game edited by Rovio.
2239	burt	Burt is a web analytics platform.
2244	candy_crush_saga	Candy Crush Saga is a mobile puzzle game edited by King Entertainment
2245	king	King is a mobile game editor. This plug-in handles King games content delivery traffic and King.com website access.
2235	nokia	Nokia is a leader in the fields of network infrastructure, location-based technologies and advanced technologies.
2238	quantcast	Quantcast provides audience and advertisement services for web sites.
2243	rovio	Rovio is a mobile game editor. This plug-in handles Rovio games content delivery traffic and Rovio website access.
2237	scorecardresearch	Scorecard Research provides a web data collection service.
2241	subway_surfers	Mobile game
2236	turn	Turn provides audience, campaign and analytics services.
2246	waze	Waze is a community based mapping, traffic & navigation app.

11.2.2. Deprecated Protocols

The following protocols have been deprecated in this version:

Table 26. Deprecated protocols in this version

ID	Name	Description	
1836	aprod	Hungarian free classifieds website	
2039	dealfish	Thai classified ads	
2191	mercador	Romanian classified ads portal	
2061	prodavalnik	Bulgarian classified ads	
1786	slando	Belarusian free classified ads	
1944	sulit	Filipino online classified ads.	

11.3. Attributes

This section describes the updates to Attributes.

11.3.1. Generic Events added in this version

No Generic Events have been added in this version.

11.3.2. Event Attributes added in this version

No Event Attributes have been added in this version.

11.3.3. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

11.3.4. Event Attributes modified in this version

No Event Attributes have been modified in this version.

11.4. Bug Fixes and Known Issues

11.4.1. Bug Fixes

There are no Bug Fixes in this version.

11.4.2. Known Issues

There are no new Known Issues in this version.

12. Protocol Bundle 1.70.0

12.1. What's new in the Protocol Bundle 1.70.0

12.1.1. Major enhancements in this release

Deprecated 2 Protocols. See Section 12.2, “Protocols”

Added 69 new Event Attributes, modified 21 existing Event Attributes. See Section 12.3, “Attributes”

Resolved 14 issues, see Section 12.4.1, “Bug Fixes”

Summary of major enhancements :

Ticket ID	Description
RTC#9790	**[stun] Added metadata extraction**
RTC#9691	**[rtcp] extracted metadata regarding the Sender Report (SR) and Receiver Report (RR)**
SF#5783 - RTC#8799	**[rtp] added support for h.264 codec name**
SF#7581 - RTC#8781	**[Normalization]: added Unicode normalization for URLs**
RTC#11105	**[h248_text] [h248_binary] Megaco/H248: new metadata**
RTC#10811	**[ldap] attribute restructuration**
RTC#10631	**[imap] extract attributes from compressed traffic (deflate)**
RTC#11173	**[mypeople_messenger] proto_evolution**
RTC#12148	**[spotify] Added classification (run2)**
RTC#12734	**[wechat] improved classification over udp**
RTC#13460	**[spdy] implemented spdy/2**
RTC#13868	**[windowslive] improved classification**
RTC#13862	**[dailymail] improved classification over rtmp**
RTC#13828	**[sina] improved classification**
RTC#13819	**[odnoklassniki] improved classification**
RTC#13534	**[letscrate] New signature over HTTP and HTTPS**
RTC#13523	**[hushmail] New signature over HTTP and HTTPS**

12.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

12.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

12.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

12.2. Protocols

12.2.1. New Protocols

No new protocols have been added in this version.

12.2.2. Deprecated Protocols

The following protocols have been deprecated in this version:

ID	Name	Description
121	msn_groups	MSN Groups was a website part of the MSN network which hosted online communities, and which contained Web pages, hosted images, and contained a message board. MSN Groups was shut down on February 2009 as part of a migration of online applications and services to the Windows Live brand, and later renovated as Windows Live Groups.
122	msn_search	This protocol is used for sending user queries to the MSN Live search engine.

12.3. Attributes

This section describes the updates to Attributes.

12.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

12.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

12.3.1.2. Event Attributes added in this version

Protocol	Attribute	Description
h248_binary	action	The action designates the command that is executed during the transaction. The command name is postfixed by Req if the transaction is a request, by Reply if the transaction is a reply
h248_binary	call_id	Call id, extracted for each call.
h248_binary	dst_audio_connection	Destination audio connection type
h248_binary	dst_audio_port	Destination audio connection port
h248_binary	dst_video_connection	Destination video connection type
h248_binary	dst_video_port	Destination video connection port
h248_binary	end	Indicates the end of a top level event.
h248_binary	from_ip	Source IPv4 address
h248_binary	from_ipv6	Source IPv6 address
h248_binary	response_code	Return code, extracted from the reply
h248_binary	src_audio_connection	Source audio connection type
h248_binary	src_audio_port	Source audio connection port
h248_binary	src_video_connection	Source video connection type
h248_binary	src_video_port	Source video connection port
h248_binary	to_ip	Destination IPv4 address
h248_binary	to_ipv6	Destination IPv6 address
h248_binary	transaction	Parent attribute including transaction elements
h248_text	action	The action designates the command that is executed during the transaction. The command name is postfixed by Req if the transaction is a request, by Reply if the transaction is a reply

Protocol	Attribute	Description
h248_text	call_id	Call id, extracted for each call.
h248_text	dst_audio_connection	Destination audio connection type
h248_text	dst_audio_port	Destination audio connection port
h248_text	dst_video_connection	Destination video connection type
h248_text	dst_video_port	Destination video connection port
h248_text	end	Indicates the end of a top level event.
h248_text	from_ip	Source IPv4 address
h248_text	from_ipv6	Source IPv6 address
h248_text	response_code	Return code, extracted from the reply
h248_text	src_audio_connection	Source audio connection type
h248_text	src_audio_port	Source audio connection port
h248_text	src_video_connection	Source video connection type
h248_text	src_video_port	Source video connection port
h248_text	to_ip	Destination IPv4 address
h248_text	to_ipv6	Destination IPv6 address
h248_text	transaction	Parent attribute including transaction elements
http	uri_unicode_normalized	Unicode normalized URL (after decoding).
ldap	level	Depth level in LDAP tree.
ldap	message	A LDAP message.
rtcp	end	Indicates the end of a top level event.
rtcp	receiver_report	Reception report that contains all fields concerning quality and metrics
rtcp	rr_dlsr	The delay between receiving the last RR packet from source n and sending reception report block.
rtcp	rr_fcnlost	The fraction of RTP data packets from source lost since the previous RR packet
rtcp	rr_highestseqnum	highest sequence number received in an RTP data packet from source SSRC_n
rtcp	rr_lsr	The middle 32 bits out of 64 in the NTP timestamp
rtcp	rr_pkt_sender_ssrc	The synchronization source identifier for the originator of this Receiver Report packet.

Protocol	Attribute	Description
rtcp	rr_rptblock	Receiver report block that contains all reception related fields
rtcp	sender_report	The report concerning the sending side
rtcp	sr_cumlost	Contains the cumulative number of lost packets (in sender reports).
rtcp	sr_dlsr	The delay between receiving the last SR packet from source n and sending reception report block.
rtcp	sr_fcnlost	The fraction of RTP data packets from source lost since the previous SR packet
rtcp	sr_highestseqnum	highest sequence number received in an RTP data packet from source SSRC_n
rtcp	sr_jitter	Jitter value (in Sender report).
rtcp	sr_lsr	The middle 32 bits out of 64 in the NTP timestamp
rtcp	sr_ntp_ts_lsw	NTP timestamp, least significant word
rtcp	sr_ntp_ts_msw	NTP timestamp, most significant word
rtcp	sr_octet_count	The total number of payload octets transmitted in RTP
rtcp	sr_pkt_count	The total number of RTP data packets transmitted by the sender
rtcp	sr_pkt_sender_ssrc	The synchronization source identifier for the originator of this Sender Report packet.
rtcp	sr_rptblock	The record containing fields about the sending side quality and metrics
rtcp	sr_rtp_ts	RTP timestamp
rtcp	sr_sender_info	The record that contains all information about a given sender
rtcp	sr_ssrc_id	The SSRC identifier of the source
stun	end	Indicates the end of a top level event.
stun	mapped_address_ipv4	IP v4 address to be mapped.
stun	mapped_address_ipv6	IP v6 address to be mapped.
stun	message	set of attributes for a given stun message
stun	port	port to be mapped.

Protocol	Attribute	Description
stun	xor_mapped_address_ipv4	IP v4 address to be mapped (deobfuscated version).
stun	xor_mapped_address_ipv6	IP v6 address to be mapped (deobfuscated version).
stun	xor_port	port to be mapped (deobfuscated version).

12.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

12.3.3. Event Attributes modified in this version

The following Event Attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Protocol	Attribute	Updates (Before/After)
facetime	service	session_mod, both, string, service_info
		session_prt, both, string, service_info
facetime	service_duration	session_mod, both, uint32, service_info
		session_prt, both, uint32, service_info
facetime	service_duration_tv	session_mod, both, timeval, service_info
		session_prt, both, timeval, service_info
facetime	service_id	session_mod, both, uint32, service_info
		session_prt, both, uint32, service_info
h248_binary	context_id	session_mod, both, uint32, no_parent

Protocol	Attribute	Updates (Before/After)
		session_mod, both, uint32, transaction
h248_text	context_id	session_mod, both, string, no_parent
		session_mod, both, string, transaction
http	video	session_mod, server, parent, no_parent
		session_mod, server, parent, request
ldap	contains_sasl	session_mod, both, uint32, no_parent
		session_mod, both, uint32, message
ldap	element	session_mod, both, parent, element
		session_mod, both, parent, message
ldap	filter_expression	session_mod, both, parent, no_parent
		session_mod, both, parent, message
ldap	hostname	session_mod, both, string, no_parent
		session_mod, both, string, message
ldap	message_id	session_mod, both, uint32, element
		session_mod, both, uint32, message
ldap	message_type	session_mod, both, string, element
		session_mod, both, string, message
rtcp	rr_cumlost	session_mod, both, uint32, no_parent
		session_mod, both, uint32, rr_rptblock
rtcp	rr_jitter	session_mod, both, uint32, no_parent
		session_mod, both, uint32, rr_rptblock
rtcp	rr_ssrc_id	session_mod, both, uint32, no_parent
		session_mod, both, uint32, rr_rptblock
tango	attach	session_mod, both, parent, service_info
		session_prt, both, parent, service_info

Protocol	Attribute	Updates (Before/After)
tango	service	session_mod, both, string, service_info session_prt, both, string, service_info
tango	service_duration	session_mod, both, uint32, service_info session_prt, both, uint32, service_info
tango	service_duration_tv	session_mod, both, timeval, service_info session_prt, both, timeval, service_info
tango	service_id	session_mod, both, uint32, service_info session_prt, both, uint32, service_info

12.4. Bug Fixes and Known Issues

12.4.1. Bug Fixes

- RTC#12937 - **[SF8055] [http] uri extraction truncated**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	uri extraction truncated

- RTC#11375 - **[SF7951] mygazines not classified**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	the host has changed

- RTC#11288 - **[http] not classified SEARCH method**

Bug Info	Description
Reported against	PB 1.50.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	http not classified

- RTC#12225 - **[SF8035] UDP session wrongly classified as GTP**

Bug Info	Description
Reported against	PB 1.60.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	fix some bad gtp classification when over ipv6

- RTC#12186 - **[DNS] dns:name sometimes extracted as empty string**

Bug Info	Description
Reported against	PB 1.30.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	dns:name sometimes extracted as empty string

- RTC#12035 - **Call to ctl_security_get changes classification**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	pdata fails to pass multiple init.

- RTC#12565 - **[qq_lady] fashion.qq.com to be added to qq_lady http hosts**

Bug Info	Description
Reported against	PB 1.60.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[qq_lady] fashion.qq.com to be added to qq_lady http hosts

- RTC#12544 - **[yihaodian] yihaodianimg.com added to hosts**

Bug Info	Description
Reported against	PB 1.60.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[yihaodian] yihaodianimg.com added to hosts

- RTC#12389 - **[HTTP] Allow NOTIFY request to end with LF in addition to CR LF**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Improve HTTP classification.

- RTC#12882 - **[SF8091][AIM] filename and filesize not extracted**

Bug Info	Description
Reported against	PB 1.50.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	AIM: filesize and filename not always extracted

- RTC#12844 - **[conversion tools] ipaddrtoi allows incomplete IP address**

Bug Info	Description
Reported against	PB 1.60.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	fix IPv4 detection

- RTC#12700 - **[msn_groups] [msn_search] protocol is now deprecated**

Bug Info	Description
Reported against	ProtocolBundle-1.70.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	

- RTC#13020 - **[ppfilm] Video streams not classified**

Bug Info	Description
Reported against	PB 1.60.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[ppfilm] Video streams not classified

- RTC#13013 - **[qq_web] Video stream not detected**

Bug Info	Description
Reported against	PB 1.60.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[qq_web] Video stream not detected

12.4.2. Known Issues

- RTC#10083 - **[stun] STUN over TCP without framing not classified**

Bug Info	Description
Reported against	PB 1.50.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[stun] STUN classification improved
Workaround	No workaround

- SF#7565 - RTC#8572 - **[SF7565][sip] support RFC5626 Keepalives**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	
Workaround	No workaround

- RTC#10874 - **[http] method is not correct when we have unlucky segmentation**

Bug Info	Description
Reported against	PB 1.50.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Method is not correct when we have unlucky segmentation.
Workaround	No workaround

- RTC#11898 - **[FTP/jabber] - Classification issue caused by proxy + L3L4 cache**

Bug Info	Description
Reported against	PB 1.60.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Don't use l3l4 cache over proxy
Workaround	No workaround

- RTC#12708 - **[SF 8039] Possible memory leak in the appsdk module**

Bug Info	Description
Reported against	PB 1.31.0
Platform	All
Effect of bug	Memory Leak
Expected versus actual behavior	Possible memory leak in the appsdk module
Workaround	No workaround

- RTC#13215 - **[skype] wrong/missing service duration**

Bug Info	Description
Reported against	ProtocolBundle-1.70.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Service duration attribute has been improved for SKYPE.
Workaround	No workaround

- RTC#13307 - **[teamspeak_v3] potential jamming on regexp evaluation**

Bug Info	Description
Reported against	PB 1.31.0
Platform	All
Effect of bug	Performance Anomaly
Expected versus actual behavior	Potential jamming on regexp evaluation
Workaround	None

- RTC#13491 - **[viber] bad service detection**

Bug Info	Description
Reported against	ProtocolBundle-1.70.0-2x
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Viber: bad service detection
Workaround	No workaround

13. Protocol Bundle 1.62.0

13.1. What's new in the Protocol Bundle 1.62.0

13.1.1. Major enhancements in this release

5 new protocols added. See Section 13.2, “Protocol Updates”

Summary of major enhancements :

Ticket ID	Description
RTC#12864	**[google_play] Classification enhancement**
RTC#12798	**[nba] Classification enhancement**
RTC#12697	**[adobe_update] Classification enhancement**
RTC#12668	**[youku] Classification enhancement**
RTC#12652	**[orangemail] Classification enhancement**
RTC#12625	**[dailymotion] Classification enhancement**
RTC#12602	**[itunes] Classification enhancement**
RTC#12578	**[viber] Classification enhancement**
RTC#12552	**[silverlight]Classification enhancement**
RTC#12486	**[viber] Classification improved on web browser**
RTC#13345	**[tv4play] Classification enhancement**
RTC#13296	**[addthis] Added new protocol: social bookmarking service**
RTC#13290	**[yadro] Added new protocol: advertising company**
RTC#13269	**[gmail] Classification enhancement**
RTC#13255	**[utorrent] Added new protocol: bittorrent client**
RTC#13252	**[bitlord] Added new protocol: bittorrent client**
RTC#13152	**[instagram] Classification improved over amazon_aws**
RTC#13149	**[farmville] Added new protocol: network game**
RTC#13137	**[appstore] Classification enhancement**
RTC#12940	**[java_update] Classification enhancement**
RTC#12892	**[steam] Classification improved over http**
RTC#13587	**[flickr] Classification enhancement**
RTC#13543	**[dailymail] Classification enhancement**
RTC#13427	**[vkontakte] Classification enhancement**
RTC#13424	**[tu] Classification enhancement**
RTC#13387	**[yahoo_search] Classification enhancement**

13.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.

- ixEngine 4.18.x versions 4.18.0-26 and higher.

13.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

13.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

13.2. Protocol Updates

13.2.1. New Protocols

The following new protocols have been added in this version:

Table 27. New protocols added in this version

Proto ID	Protocol	Description
2231	addthis	AddThis is a social bookmarking service that can be integrated into a website with the use of a web widget.
2234	bitlord	BitLord is a free BitTorrent client. This plugin classifies traffic to the software company website. The generated traffic by this client is classified as bittorrent.
2218	farmville	FarmVille is a farming simulation social network game developed by Zynga.
2233	utorrent	uTorrent is a closed source BitTorrent client. This plugin classifies traffic to the software company website. The generated traffic by this client is classified as bittorrent.
2232	yadro	Yadro is an advertising company that is part of a network of sites and other technologies.

13.2.2. Deprecated Protocols

No protocols have been deprecated in this version.

13.3. Attributes

This section describes the updates to Attributes.

13.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

13.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

13.3.1.2. Event Attributes added in this version

No Event Attributes have been added in this version.

13.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

13.3.3. Event Attributes modified in this version

No Event Attributes have been modified in this version.

13.4. Bug Fixes and Known Issues

13.4.1. Bug Fixes

There are no Bug Fixes in this version.

13.4.2. Known Issues

There are no Known Issues in this version.

14. Protocol Bundle 1.61.0

14.1. What's new in the Protocol Bundle 1.61.0

14.1.1. Major enhancements in this release

14 new Protocols added. See Section 14.2, “Protocol Updates”

Summary of major enhancements :

Ticket ID	Description
RTC#12717	**[flashplugin_update] improve classification**
RTC#12575	**[yahoo_search] improve classification**
RTC#12504	**[google_maps] add classification on symbian OS and WindowsPhone**
RTC#12070	**[amazon-adsystem] new protocol**
RTC#10262	**[thunder] check proto_evolution**
RTC#13097	**[qq] improve classification over http**
RTC#12905	**[tv4play] improve classification on video workflow**
RTC#12871	**[blogger] [blogspot] improve classification**
RTC#12793	**[norton_update] improve classification**
RTC#12769	**[blackberry] improve classification**
RTC#12752	**[debian_update] improve classification**
RTC#12737	**[gstatic] improve classification**
RTC#13191	**New protocols the top worldwide web sites list of 2014-04-08**

14.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

14.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don’t have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

14.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

14.2. Protocol Updates

14.2.1. New Protocols

The following new protocols have been added in this version:

Table 28. New protocols added in this version

Proto ID	Protocol	Description
2225	aastocks	Chinese financial services and stock market website
2207	amazon_adsystem	This protocol plug-in classifies the trafic related to Amazon adsystem services.
2209	aol	This protocol plug-in classifies the trafic related to the AOL portal.
2226	aparat	Iranian multimedia website
2219	cameroon_info	Cameroonian news portal
2221	crhoy	Coasta rican news portal
2227	digikala	Iranian electronics and tech review website
2222	ecuavisa	Ecuadorian TV channel website
2223	lapagina	El salvadorian news portal
2224	mozzi	International Mobile services provider
2229	naver_mobile	Mobile application for Naver (Korean Search Engine).
2230	stick_cricket	Mobile game
2228	xendan	Iranian news portal
2220	yapo	Chilian classified ads website

14.2.2. Deprecated Protocols

The following protocols have been deprecated in this version:

Table 29. Deprecated protocols in this version

Proto ID	Protocol	Description	
975	blogspot	This protocol plug-in classifies the http traffic to the host blogspot.com.	
1040	pps	This protocol plug-in classifies the http traffic to the host pps.tv. This traffic is now classified as PPstream.	

14.3. Attributes

This section describes the updates to Attributes.

14.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

14.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

14.3.1.2. Event Attributes added in this version

No Event Attributes have been added in this version.

14.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

14.3.3. Event Attributes modified in this version

No Event Attributes have been modified in this version.

14.4. Bug Fixes and Known Issues

14.4.1. Bug Fixes

- RTC#13167 - **[iqiyi] Inaccurate iqiyi classification**

Bug Info	Description
Reported against	PB 1.60.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[iqiyi] Inaccurate iqiyi classification

14.4.2. Known Issues

There are no Known Issues in this version.

15. Protocol Bundle 1.60.0

15.1. What's new in the Protocol Bundle 1.60.0

15.1.1. Major enhancements in this release

- 28 Event Attributes added concerning 14 protocols (base, bittorrent, http, imap, ip6, mplus_messenger, nntp, pop3, sip, smtp, ssl, tcp, wechat, whatsapp). See Section 15.3.1.2, “Event Attributes added in this version”.
- 10 Event Attributes modified concerning 4 protocols (line, mplus_messenger, wechat, whatsapp). See Section 15.3.3, “Event Attributes modified in this version”.
- Various Bug Fixes, see Section 15.4.1, “Bug Fixes”.
- Extraction of « header_raw » attribute in SMTP, POP3, IMAP, NNTP.
- Major extension of the mapi plug-in on the advanced workflows of Microsoft Exchange/Outlook, classification and extraction.
- Advanced support of offloading in the bittorrent plug-in.
- New metrics implemented in TCP for de-sequencing analysis (unseq_ack, retransmission_bytes, dup_ack).
- New detection of file types for files transmitted over HTTP, IMAP, POP3, SMTP (about 40 file types) by binary prefix-matching

Summary of major enhancements :

Ticket ID	Description
SF#6541 - RTC#7524	**[tcp] add attribute for retransmission counters and duplicates ack**
SF#7384 - RTC#7028	**[sip] add new attribute authorization username**
SF#6541 - RTC#5886	**[tcp] add attribute unack_sequence**
SF#7077 - RTC#5757	**[SF7077] [ssl] add new attributes (index and request_size)**
RTC#5230	**[rtsp] add URI attribute beginning and end offsets**
RTC#5221	**[ftp] add attributes data port beginning and end offsets**
RTC#5218	**[smb] add attribute service_data**
SF#3963 - RTC#7818	**[bittorrent] add "signalization" and "declassification" feature override when the flow can be offloaded**
RTC#10492	**[POP3] New metadata header_raw**
RTC#10468	**[SMTP] new metadata header_raw**
RTC#10357	**[tftp] Add feature nocaching**
RTC#10277	**[bittorrent/somud] Improved Classification**
RTC#10241	**[ssl] add new attribute organization_name**
RTC#9884	**[ymsg_conf] ymsg_conf over UDP**
RTC#10751	**[NNTP] New metadata header_raw**
RTC#10495	**[IMAP] New metadata header_raw**
RTC#11425	**[kakaotalk] classification on tcp (blackberry workflow)**

Ticket ID	Description
RTC#11321	**[badoo] Classification over TCP (Android/Blackberry/Windowsphone)**
RTC#11847	**[tango] Classification on header_name=TangoMe-TaskId**
RTC#12094	**[ustream] Improved Classification**
RTC#12433	**[badoo] Improved Classification**
RTC#12307	**[here]: add https case for 'here' classification**

15.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

15.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don’t have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

15.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

15.2. Protocol Updates

15.2.1. New Protocols

No new protocols have been added in this version.

15.2.2. Deprecated Protocols

No protocols have been deprecated in this version.

15.3. Attributes

This section describes the updates to Attributes.

15.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

15.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

15.3.1.2. Event Attributes added in this version

15.3.1.2.1. Added Event Attributes

Protocol	Attribute	Description
base	create_time	This attribute gives the timestamp of the first packet in the flow fed in the ixEngine. It is restricted to INT FLOW VERSION ONLY of ixEngine.
bittorrent	declassify_override	Attribute used to specify whether the current session path maybe be declassified or not. This value overrides the proto_feature flag defined in the layer raising this event.
bittorrent	signalization_override	Attribute used to specify whether the current session may provide incoming flows information or not. This value overrides the proto_feature flag defined in the layer raising this event.
http	file_type	Received or sent file content type (prefix-based pattern recognition) exchanged using this protocol.
http	uri_raw	Complete name (scheme/authority + path + request) of a web resource.
http	uri_raw_path	Complete name (scheme/authority + path) of a web resource without query parameters.
imap	file_type	Received or sent file content type (prefix-based pattern recognition) exchanged using this protocol.
imap	header_raw	One HTTP header line (field and value).

Protocol	Attribute	Description
mplus_messenger	end	Indicates the end of a top level event.
mplus_messenger	service_info	Parent attribute for service information.
nntp	header_raw	One NNTP header line (field and value).
pop3	file_type	Received or sent file content type (prefix-based pattern recognition) exchanged using this protocol.
pop3	header_raw	One POP3 header line (field and value).
sip	authorization_username	User's name as specified in the Authorization SIP header.
smtp	file_type	Received or sent file content type (prefix-based pattern recognition) exchanged using this protocol.
smtp	header_raw	One SMTP header line (field and value).
ssl	index	Identifier of the request and response in a SSL flow.
ssl	organization_name	Organisation name mentioned in the certificate.
ssl	request	An SSL request.
ssl	request_size	Contains the total length in bytes of the request or the response (including SSL headers). This attribute is computed at the end of the request or response.
tcp	dup_ack	Extracted when the current packet has the ACK flag and validates a data segment that was already acknowledged.
tcp	retransmission_bytes	Current packet overlapping bytes count, extracted when out-of-order TCP sequence occurs.
tcp	unack_sequence	Provides the difference between the maximum sequence number seen in payload packets minus the maximum ack seq number seen on the other way.
wechat	end	Indicates the end of a top level event.
wechat	service_info	Parent attribute for service information.
whatsapp	end	Indicates the end of a top level event.

Protocol	Attribute	Description
whatsapp	service_info	Parent attribute for service information.

15.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

15.3.3. Event Attributes modified in this version

The following Event Attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 30. Modified Event Attributes

Protocol	Event attribute	Changes
line	service	session_mod, both, string, service_info
		session_prt, both, string, service_info
line	service_duration	session_mod, both, uint32, service_info
		session_prt, both, uint32, service_info
line	service_duration_tv	session_mod, both, timeval, service_info
		session_prt, both, timeval, service_info
line	service_id	session_mod, both, uint32, service_info
		session_prt, both, uint32, service_info
mplus_messenger	service	session_mod, both, string, no_parent
		session_prt, both, string, service_info
mplus_messenger	service_id	session_mod, both, uint32, no_parent
		session_prt, both, uint32, service_info
wechat	service	session_mod, both, string, no_parent
		session_prt, both, string, service_info
wechat	service_id	session_mod, both, uint32, no_parent
		session_prt, both, uint32, service_info
whatsapp	service	session_mod, both, string, no_parent

Protocol	Event attribute	Changes
		session_prt, both, string, service_info
whatsapp	service_id	session_mod, both, uint32, no_parent
		session_prt, both, uint32, service_info

15.4. Bug Fixes and Known Issues

15.4.1. Bug Fixes

- RTC#9640 - **optimization of the facebook protocol for the extraction with unidirectional traffic**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification issue with the server way for unidirectional traffic

- RTC#9637 - **optimize the extraction of attribute for ymail_mobile_new with unidir traffic**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	issue to extract some email attributes in case of unidirection traffic

- RTC#8959 - **[offloading] http abusive declassification**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Bug corrceted in HTTP decalssification mechanism to not find the same path again after a declassification has been performed.

- RTC#8956 - **[offloading] we must classifiy websocket on first packet**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Classification bug corrected on Websocket protocol plugin.

- SF#7548 - RTC#8340 - **[imap] newline preceeding boundary should not be part of attach content**

Bug Info	Description
Reported against	PB 1.31.0
Platform	All
Effect of bug	Extraction Anomaly

Bug Info	Description
Expected versus actual behavior	[imap] Multipart attachment extraction updated

- RTC#10250 - **[SF7787] Classification issue of yahoo_buy**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	classification

- RTC#10247 - **[SF7786] taku_file_bin not detected**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	taku_file_bin not detected

- RTC#10244 - **[SF7785] classification of foxmovies.com**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	add the support foxmovies.com

- RTC#9856 - **[SF7424] Crash in AIM - due to alignment**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	alignment issue

- RTC#10783 - **[google] query_type not correctly extracted with mobile**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	google:query_type not extracted correctly on mobile

- RTC#10548 - **[msn_video] DNS classified as msn_video**

Bug Info	Description
Reported against	PB 1.50.0

Bug Info	Description
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[msn_video] DNS classified as msn_video

- RTC#10505 - **[gmail_basic] gmail_basic improvement (GET param ui=html is gmail_basic)**

Bug Info	Description
Reported against	PB 1.50.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[gmail_basic] Classification improved

- RTC#11192 - **[line] missing classification**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Classification bug corrected on Line protocol plugin.

- RTC#11138 - **[SF7873] [ibibo] Classification issue**

Bug Info	Description
Reported against	PB 1.50.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Not all traffic related to Ibibo is detected as ibibo

- RTC#11135 - **[hyves] Classification issues**

Bug Info	Description
Reported against	PB 1.50.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Not all traffic related to Hyves Games is detected as hyves

- RTC#11012 - **[maktoob] classification lost**

Bug Info	Description
Reported against	PB 1.50.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification bug corrected on Maktoob protocol plugin.

- RTC#11378 - **[SF7954] BEEMP3 not classified**

Bug Info	Description
Reported against	ProtocolBundle-1.60.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Update of protocol BEEMP3 to handle new hosts.

- RTC#11372 - **[kakaotalk] classification over tcp can be improved**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	enhance classification

- RTC#11832 - **[apple_airplay] Classification prediction of event, audio and video sessions + AppleCoreMedia http sessions**

Bug Info	Description
Reported against	PB 1.50.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[apple_airplay] Classification prediction of event, audio and video sessions + AppleCoreMedia http sessions

- RTC#12064 - **[bbm] classified is not raised**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Performance Anomaly
Expected versus actual behavior	Sessions were never flagged as classified.

15.4.2. Known Issues

- RTC#9548 - **Issue to extract the ymail2 contact information in case of server way only**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	issue to extraction information from the server way in case of unidirectional traffic
Workaround	No workaround

- RTC#11349 - **[tcp] utcp_layer_completion is called several times at timeout**

Bug Info	Description
Reported against	PB 1.50.0

Bug Info	Description
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	TCP time based metrics are duplicated on session_timeout
Workaround	No workaround

16. Protocol Bundle 1.53.0

16.1. What's new in the Protocol Bundle 1.53.0

16.1.1. Major enhancements in this release

Ticket ID	Description
RTC#12364	**[conviva]: add http case for 'conviva' classification**
RTC#7099	**[snapchat] Add new protocol Snapchat (Application Service)**
RTC#7105	**[gt_racing_2] Add new protocol GT Racing 2 (Game)**
RTC#7944	**[SF6678][champion_football] Add new protocol Champion Football (Game)**
RTC#7953	**[SF6678][akinator] Add new protocol akinator (Game)**
RTC#7959	**[SF6678][puzzle_and_dragon] Add new protocol puzzle and dragon (Game)**
RTC#7962	**[SF6678][infinity_blade_ii] Add new protocol Infinity Blade II (Game)**
RTC#7965	**[SF6678][despicable_me_2] Add new protocol despicable me 2 (Game)**
RTC#12373	**[google_earth] add classification on browser**
RTC#12376	**[kaspersky_update] add classification**
RTC#12411	**[badoo] add classification over SSL**
RTC#7983	**[SF6678][tapatalk] Add new protocol tapatalk (Application Service)**
RTC#12058	**[qq] improve classification**
RTC#11979	**[sina_weibo] update protocol classification**
RTC#12061	**[vimeo] improve video workflow classification**

8 new protocols have been added in this version, see Section 16.2, “Protocol Updates”

No Event Attributes have been added or modified in this version.

There are no Bug Fixes or Known Issues to report in this version.

16.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

16.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

16.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

16.2. Protocol Updates

16.2.1. New Protocols

The following new protocols have been added in this version:

Table 31.

Proto ID	Protocol	Description
2214	akinator	Mobile game.
2211	champion_football	Mobile game.
2213	gameloft	Games for mobile devices, by Gameloft.
2212	gt_racing_2	Mobile game, edited by Gameloft. Most of the traffic should be classified as gameloft.
2217	infinity_blade_ii	Mobile game.
2216	puzzle_and_dragon	Japanese Mobile game.
2210	snapchat	Snapchat is a photo/video sharing service.
2215	tapatalk	Mobile app which allows to browse forums.

16.3. Attributes

No Event Attributes have been added or updated in this version.

16.4. Bug Fixes and Known Issues

There are no Bug Fixes or Known Issues in this version.

17. Protocol Bundle 1.52.0

17.1. What's new in the Protocol Bundle 1.52.0

17.1.1. Major enhancements in this release

14 Protocol signatures have been added (air_video, femina, foxbusiness, free, free_music_download...). See Section 17.2, “Protocol Updates”

14 Protocol signatures have been updated to enhance the classification or support protocol evolutions.

Summary of major enhancements :

Ticket ID	Description
RTC#6063	**[air_video] Add new protocol Air video (Audio/Video)**
RTC#11339	**[pinterest] Protocol Evolution**
RTC#11409	**[grooveshark] Classification enhancement**
RTC#11506	**[plurk] Classification enhancement**
RTC#11540	**[dailymotion] Classification enhancementt**
RTC#11546	**[icloud] Classification enhancement**
RTC#11582	**[cnn] Protocol Evolution**
RTC#11591	**[redtube] Update protocol Classification**
RTC#11759	**[dailymail] Update Protocol Classification**
RTC#11775	**[odnoklassniki] Update classification**
RTC#11851	**[yahoo_search] Update classification**
RTC#11868	**[flickr] SSL classification enhancement on Android**
RTC#11874	**[foxnews] update classification**
RTC#11894	**[tube8] update protocol classification**
RTC#11931	**[dailymail] update classification on Web Browser**
RTC#11957	**[foxbusiness] New protocol Classification**
RTC#12103	**New web sites classification added from worldwide top list**

17.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

17.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don’t have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

17.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

17.2. Protocol Updates

17.2.1. New Protocols

The following new protocols have been added in this version:

Table 32. New protocols added in this version

Proto ID	Protocol	Description
2208	a_dakar	Senegalese news portal
2196	air_video	Air Video can stream videos to your iPhone, iPad and iPod touch.
2203	eluniverso	Ecuadorian news portal
2206	femina	Macedonian website specialised in women news, trends, gears, etc
2195	foxbusiness	Fox Business Network (FBN) is an American cable and satellite business news television channel that is owned by the Fox Entertainment Group division of 21st Century Fox. The network discusses business and financial news.
1811	free	French ISP and mobile operator website.
2197	free_music_download	Download, play, sort, organize media files.
2200	kohsantepheapdaily	Cambodian news portal
2204	myjoyonline	Ghanaian news portal
2199	news_au	Australian news portal
2202	sigmalive	Cypriot news portal
2205	tayyar	Lebaneese news portal
2198	telegrafi	Albanian news and media portal
2201	vecernji	Crotaian news portal

17.2.2. Deprecated Protocols

No protocols have been deprecated in this version.

17.3. Attributes

This section describes the updates to Attributes.

17.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

17.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

17.3.1.2. Event Attributes added in this version

No Event Attributes have been added in this version.

17.3.2. Event Attributes removed in this version

No Event Attributes have been removed in this version.

17.3.3. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

17.3.4. Event Attributes modified in this version

No Event Attributes have been modified in this version.

17.4. Bug Fixes and Known Issues

17.4.1. Bug Fixes

There are no Bug Fixes in this version.

17.4.2. Known Issues

There are no Known Issues in this version.

18. Protocol Bundle 1.51.0

18.1. What's new in the Protocol Bundle 1.51.0

18.1.1. Major enhancements in this release

20 new Protocols added, 5 deprecated. See Section 18.2, “Protocol Updates”

4 issues resolved. See Section 18.4.1, “Bug Fixes”

Summary of major enhancements :

Ticket ID	Description
RTC#10645	**[badoo] protocol signature udpate**
RTC#10284	**[instagram] classify traffic to amazon_aws**
RTC#10290	**[line] classification update**
RTC#10304	**[qq_games] classification update**
RTC#10323	**[shoutcast] classification update**
RTC#11176	**[mitalk] protocol signature udpate**
RTC#11223	**[steam] classification update**
RTC#11226	**[wordpress] classification update**
RTC#11246	**[twitpic] protocol signature update**
RTC#11256	**[babycenter] classification update**
RTC#10354	**[youku] classification update**
RTC#10428	**[baidu] classification on windows_phone**
RTC#10502	**[baidu] classification on Android/Windows7**
RTC#10508	**[google] classification update**
RTC#11264	**[svtplay] protocol signature update**
RTC#11291	**[cnet] classification update**
RTC#10978	**[sendspace] protocol signature update**
RTC#11069	**[photobucket] protocol signature update**
RTC#11157	**[sina] classification update**
RTC#11164	**[tango] classification update**

18.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

18.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

18.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

18.2. Protocol Updates

18.2.1. New Protocols

The following new protocols have been added in this version:

Table 33. New protocols added in this version

ID	Name	Description
2185	aib	Irish banking website
2187	arabiaweather	Jordanian meteorological portal
2178	clumsy_ninja	Mobile game.
2180	deer_hunter_2014	Mobile game.
2183	eltiempo	Colombian news portal
2176	fruit_ninja	Mobile game.
2181	gazetaexpress	Albanian news portal
2184	gazzetta	Greek news portal
2192	globalpublishers	Tanzanian news portal
2182	khmer_news	Cambodian news portal
2189	kwejk	Polish multimedia website
2191	mercador	Romanian classified ads portal
2193	mover	Uzbek vide streaming website
2177	my_talking_tom	My Talking Tom is a mobile game.
2194	noticias24	Venezuelian news portal
2175	oneworld_org	OneWorld is a NGO with a mission to provide internet and mobile phone applications to third-world countries inhabitants
2188	palweather	Palestinian meteorological portal
2186	sarayanews	Jordanian news portal
2179	the_simpsons_tapped_out	Mobile game (EA Games).
2190	xl	Portugese multisites and portal

18.2.2. Deprecated Protocols

The following protocols have been deprecated in this version:

Table 34. Deprecated protocols in this version

ID	Name	Description
463	oneclimate	This protocol plug-in is deprecated.
464	oneworldtv	This protocol plug-in is deprecated.
488	socialvibe	This protocol plug-in used to classify the http traffic to the host socialvibe.com.
362	the_auteurs	This protocol plug-in used to classify the http traffic to the host theauteurs.com.
746	ytimg	This protocol plug-in classified the http traffic to the host .ytimg.com. This traffic is now classified as youtube.

18.3. Attributes

This section describes the updates to Attributes.

18.3.1. New Event Attributes added in this version

No Event Attributes have been added in this version.

18.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

18.3.1.2. Event Attributes added in this version

No Event Attributes have been added in this version.

18.3.2. Event Attributes removed in this version

No Event Attributes have been removed in this version.

18.3.3. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

18.3.4. Event Attributes modified in this version

No Event Attributes have been modified in this version.

18.4. Bug Fixes and Known Issues

18.4.1. Bug Fixes

- RTC#10253 - **[SF7791] Classification overlap between ytimg and youtube**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	overlap on ytimg.com

- RTC#10623 - **[oneclimate] [oneworldtv] Merge plug-ins**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	oneworldtv and oneworldclimate both redirect to the same website and should be merged in a new plug-in

- RTC#10626 - **[poker_stars] classification issues**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification issues with poker_stars

- RTC#11262 - **Duplicated file "forum.html" found in the Protobook archive**

Bug Info	Description
Reported against	PB 1.50.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	During extraction on Windows, a warning is raised for a duplicated file Forum.html and forum.html.

18.4.2. Known Issues

There are no Known Issues in this version.

19. Protocol Bundle 1.50.0

19.1. What's new in the Protocol Bundle 1.50.0

19.1.1. Major enhancements in this release

Added 24 new Protocols and deprecated 14 Protocols, see Section 19.2, “Protocol Updates”.

Added 20 new Event Attributes concerning 12 protocols (facetime, ftp, http, imp, line, rtsp, sip, skype, smb, socks5, tango, viber).

Modified Attributes service_id and service_duration for 2 protocols (line and tango), see Section 19.3, “Attributes”.

Summary of major enhancements :

Ticket ID	Description
SF#6915 - RTC#5233	**[octoshape] add classification (p2p)**
RTC#5230	**[rtsp] add URI attribute beginning and end offsets**
RTC#5224	**[sip] add attributes media address beginning and end offsets**
RTC#5221	**[ftp] add attributes data port beginning and end offsets**
RTC#5218	**[smb] add attribute service_data**
SF#7224 - RTC#5103	**[pdata] add support: ipv4 protocol and ipv6 next header**
RTC#4004	**[perfect_dark] add classification (p2p)**
RTC#2073	**[socks5] login/password extraction**
SF#7330 - RTC#6693	**[http] support mpeg_ts container for http video metadata extraction**
RTC#5853	**[PB] Ability to disable any protocol plug-in (C/hybrid/pdd)**
RTC#8401	**[retroshare] add classification (C/PDL)**
RTC#9369	**[SF7650] add the support of GYGAN-NNTP signature**
RTC#9478	**[kakaotalk] unknown packets over tcp**
RTC#9381	**[facetime][line][skype][tango][viber] service_duration to be raised in microseconds**
RTC#9372	**[SF7651]add the support of OZYMAN-DNS-TUNNELsignature**
RTC#9815	**15 new protocols from the list of top worldwide web sites**
RTC#9958	**[aim] update classification**
RTC#9853	**[qq] add qq classification over udp**
RTC#10016	**[linkedin] Missing classification - protocol update**
RTC#9992	**[skype] Update protocol**
RTC#9982	**[ymail_mobile_new] protocol update**
RTC#10226	**[Baidu] Protoevolution : Missing classification**
RTC#10417	**[norton_update] missing classification on Mac platform**

19.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

19.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

19.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1

- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

19.2. Protocol Updates

19.2.1. New Protocols

The following new protocols have been added in this version:

Table 35. New protocols added in this version

Proto ID	Protocol	Description
2156	armorgames_play	This signature detects requests to play games on ArmorGames.com, an on-line, flash-based video game site. Users can play simple video games for free.
2152	bittorrent_application	This signature detects the access to the BitTorrent Apps web ressources from the BitTorrent application.
2161	educarriere	Ivory Coast Job portal
2165	elhourriya	Mauritanian news portal
2168	fnb	South African banking website
2150	google_accounts	Detects SSL access to the Google Accounts server.
2170	haber7	Turkish tv streaming website
2163	jamaicaobserver	Jamaican news portal
2172	lapatilla	Venezuelian news portal
2158	livemail_attach	This signature detects Windows Live Mail File attachment uploads.
2162	mihanwebads	Iranian Internet AD company website
2151	mikogo	Mikogo is a free desktop sharing and web conferencing service.
2166	moe_gov	Omanian Ministry of Education portal
2169	mosaiquefm	Tunisian radio streaming website
2171	newvision	Ugandan news portal
2154	octoshape	Octoshape is a video streaming solution provider for web streaming platforms which uses P2P technology.
2164	over_blog	French and American blog administration website
2148	perfect_dark	Perfect Dark is a peer-to-peer file-sharing (P2P) protocol from Japan.
1908	retroshare	Retroshare is a communication and file-sharing Open Source platform which is secured and decentralized.
2173	sahafah	Yemeni news portal
2014	scheduled_tp	STP is a connection-oriented data transfer protocol. It is found over the IP layer (IANA protocol number: 118).
2160	top_channel	Albanina tv streaming website
2167	ultimahora	Honduran news portal
2174	yemen_net	Yemeni service provider portal

19.2.2. Deprecated Protocols

The following protocols have been deprecated in this version:

Table 36. Deprecated protocols in this version

Proto ID	Protocol	Description
372	books_iread	This protocol plug-in classified the http traffic to the host weread.com. Moved to flipkart.com/books service.
1202	emaps	This protocol plug-in classifies the http traffic to the host empas.com.
789	files_to	This protocol plug-in classifies the http traffic to the host files.to.
816	kino	This protocol plug-in classifies the http traffic to the host kino.to.
823	meevee	Closed on-line video aggregator website.
824	megavideo	This protocol plug-in classifies the http traffic to the host megavideo.com.
827	mobile_me	On-line web application suite (me.com) created by Apple and remplaced by iCloud in 2011.
1219	paran	This protocol plug-in classifies the http traffic to the host praran.com.
472	playahead	This protocol plug-in classifies the http traffic to the host playahead.se.
476	qapacity	This protocol plug-in classifies the http traffic to the host qapacity.com.
203	synflood	This plug-in is no longer supported.
514	wiserearth	This protocol plug-in classifies the http traffic to the host wiserearth.org.
295	yahoo_biz	This protocol plug-in classifies the http traffic to the hosts fr.biz.yahoo.com and finance.yahoo.com.
328	ymail_mobile	(Deprecated) Yahoo Mail Mobile is the yahoo.com webmail adapted to mobiles.

19.3. Attributes

This section describes the updates to Attributes.

19.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

19.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

19.3.1.2. Event Attributes added in this version

Table 37. Added Event Attributes

Proto ID	Protocol	Description
facetime	service_duration_tv	Timeval structure indicating, when the service is ended, the length of it in second and microseconds.
ftp	data_port_end_offset	Offset to the first byte which is not part of the TCP port value, given in the PORT command.
ftp	data_port_start_offset	Offset to the first FTP port byte given in the PORT command.
http	video_mangled	The video stream is mangled (probably encrypted).
imp	msglist_sender_email	Address of email sender.
line	service_duration_tv	Timeval structure indicating, when the service is ended, the length of it in seconds and microseconds.
rtsp	uri_end_offset	Offset to the first byte which is not part of the URI in the stream.
rtsp	uri_start_offset	Offset to the first URI byte in the stream.
sip	media_attr_addr_end_offset	Offset to the first byte which is not part of the IP address field given in the media attribute.
sip	media_attr_addr_start_offset	Offset to the first IP address field byte given in the media attribute.
sip	media_attr_port_end_offset	Offset to the first byte which is not part of the PORT field given in the media attribute.
sip	media_attr_port_start_offset	Offset to the first PORT field byte given in the media attribute.
skype	service_duration_tv	Timeval structure indicating, when the service is ended, the length of it in second and microseconds.
smb	service_data	Data associated with the resource that the client intends to access.
socks5	login	User's login string.
socks5	password	User's password string.
tango	attach	Parent attribute containing metadata related to an attached file exchanged between two users.
tango	attach_filename	Transferred file name.

Proto ID	Protocol	Description
tango	service_duration_tv	Timeval structure indicating, when the service is ended, the length of it in second and microseconds.
viber	service_duration_tv	Timeval structure indicating, when the service is ended, the length of it in second and microseconds.

19.3.2. Event Attributes removed in this version

The following Event Attributes have been removed:

Table 38. Removed Event Attributes

Protocol	Removed event attributes	Comments
ymail_mobile	end	Indicates the end of a top level event.
ymail_mobile	msglist_sender	Full address of email sender (alias and email address).
ymail_mobile	msglist_sender_alias	Name of email sender.
ymail_mobile	msglist_sender_entry	Parent entry for a sender in a message list.
ymail_mobile	msglist_receiver	Full address of email receiver in a message list.
ymail_mobile	msglist_receiver_alias	Name of email receiver.
ymail_mobile	msglist_receiver_entry	Parent entry for a receiver in a message list.
ymail_mobile	msglist_subject	Message subject in a message list.
ymail_mobile	msglist_msgid	Message identifier.
ymail_mobile	msglist_entry	Parent entry, for different elements belonging to the same message of a message list.
ymail_mobile	draft	Indicates if the email is a draft or has really been posted
ymail_mobile	attach_content	Attached files' content.
ymail_mobile	attach_id	Attachment identifier.
ymail_mobile	attach_filename	Attachment name.
ymail_mobile	attach	Parent entry, for attach fields in a message.
ymail_mobile	content	Message content.
ymail_mobile	receiver_type	Type of the email receiver.
ymail_mobile	receiver_alias	Name of email receiver (included cc and bcc receivers).
ymail_mobile	receiver_email	Email address of message receiver (included cc and bcc receivers).
ymail_mobile	receiver	Full address of email receiver (including cc and bcc receivers).

Protocol	Removed event attributes	Comments
ymail_mobile	receiver_entry	Parent entry, for different elements belonging to the email receiver.
ymail_mobile	date	Message date.
ymail_mobile	sender_alias	Name of the email sender.
ymail_mobile	sender_email	Email address of the email sender.
ymail_mobile	sender	Full address of email sender (alias followed by email address).
ymail_mobile	sender_entry	Parent entry, for different elements belonging to the sender.
ymail_mobile	subject	Message subject.
ymail_mobile	msg_id	Identifier of the message.
ymail_mobile	action	Indicates if the message is read (Read) or composed (Compose).
ymail_mobile	email	Parent entry, for fields belonging to the same email.
ymail_mobile	folder	Indicates the directory from where messages are read.
ymail_mobile	contact_email	Email address of a contact.
ymail_mobile	contact_alias	Alias of a contact.
ymail_mobile	contact_entry	This attribute groups information about a contact.
ymail_mobile	password	User's password string.
ymail_mobile	login	User's login string.
ymail_mobile	contact	Complete contact.
ymail_mobile	attach_type	Content type of the sent attached file.
ymail_mobile	session_id	Uniquely identifies the current user session.

19.3.3. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

19.3.4. Event Attributes modified in this version

The following Event Attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 39. Modified Event Attributes

Protocol	Event attribute	Changes (before/after)
line	service_duration	session_mod, both, int32, service_info
		session_mod, both, uint32, service_info
line	service_id	session_mod, both, int32, service_info
		session_mod, both, uint32, service_info
tango	service_duration	session_mod, both, int32, service_info
		session_mod, both, uint32, service_info
tango	service_id	session_mod, both, int32, service_info
		session_mod, both, uint32, service_info

19.4. Bug Fixes and Known Issues

19.4.1. Bug Fixes

- RTC#3581 - **[funshion] classification issue (smart client)**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Update of the protocol Funshion for classification over Tcp layer.

- SF#6862 - RTC#5440 - **[ftp_data] does not support FTP connection reset.**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	FTP_DATA does not support connection reset.

- SF#7183 - RTC#8302 - **[skype] classification improvement**

Bug Info	Description
Reported against	PB 1.31.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Improve skype classification for some rare occurences of traffic over TCP.

- SF#7423 - RTC#7068 - **[SF 7423] [http] normalization cases not supported (duplicated slashes, empty query, dot-segtments)**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	duplicated slashes, empty query and dot-segtments cases are not supported

- SF#7512 - RTC#8614 - **[SF7512][skype][SPID] misclassified as bittorrent**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	bittorrent classification issue

- RTC#8910 - **[netflix/ubmff] classification_match is different beween AMP/SMP**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	diff classification_match between amp/smp

- SF#7369 - RTC#8814 - **[SF7369] [NTP] sessions are not identified - classify on invalid poll**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Fix ntp classification when using ntp extension

- SF#7584 - RTC#8691 - **[SF7584] [tango] filename not extracted on server side**

Bug Info	Description
Reported against	PB 1.30.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	http:filename not extracted on server side

- RTC#8996 - **[tor] classification issues with last implementation**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Some TOR sessions aren't detected as such

- RTC#8973 - **[Ultrasurf] - Classification behind proxy**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Unable to classify Ultrasurf over proxy

- RTC#8976 - **[kakaotalk] image transfer over tcp to classify**

Bug Info	Description
Reported against	PB 1.30.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	improved kakaotalk classification over tcp

- RTC#9277 - **[sip] timeout is set to small value (60 s) after ACK command**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	[sip] timeout after ACK command increased

- RTC#9499 - **[facebook_apps] Classification issue**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification issue of facebook_apps over HTTPS

- RTC#9493 - **[SF7665] integration GOOGLE-ACCOUNTS-SSL signature**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	google-accounts not supported

- RTC#9460 - **[spotify] unknown packets over TCP**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Improvement of the classification of protocol Spotify over the Tcp layer.

- RTC#9572 - **[msn] unitary extraction issue on chat attributes**

Bug Info	Description
Reported against	PB 1.31.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	bug on msn:receiver, this attribute is not raised at least on some cases.

- RTC#9566 - **[wow] Classification improvement**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[wow] Classification improvement

- RTC#9554 - **[windowslive] Classification issue**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification issue with windowslive when using Skype

- RTC#9518 - **[thunder] metadata must be added**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification of Thunder (Xunlei) improved.

- RTC#9804 - **[SF7726] yahoo_finance vs yahoo_biz**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	yahoo_finance conflicts with yahoo_biz

- RTC#9770 - **[apple_airplay] apple_airplay over RTSP/RTP**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	[apple_airplay] apple_airplay over RTSP/RTP now supported

- RTC#9700 - **[pplive] Classification issue for the video stream**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	The video stream of PPLive application is only detected as HTTP

- RTC#9675 - **[SF7707] lastpass classification over HTTP**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification issue with lastpass over HTTP

- RTC#9949 - **[4shared] Missing SSL classification**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Updatethe classification of 4Shared protocol over the SSL layer.

19.4.2. Known Issues

There are no Known Issues in this version.

20. Protocol Bundle 1.42.0

20.1. What's new in the Protocol Bundle 1.42.0

20.1.1. Major enhancements in this release

65 new Protocols added, see Section 20.2, “Protocol Updates”

Protocol updates and enhancements:

- Deprecated the Jajah protocol (Jajah was a VoIP provider owned by Telefonica Europe; Telefonica shut down Jajah on January 31, 2014)
- Deprecated the Hudong protocol (hudong.com, a major chinese online encyclopedia, is now baike.com)
- Added referer functionality to enhance the qq_games classification.
- Updated audio/video formats list to classify youtube_hd in all conditions.
- Supported protocol evolutions for vimeo, livemail_mobile, chrome_update, live_hotmail, wechat, window_marketplace, qq_web, dailymotion and java_update.
- Added domain extension for regional URLs for sapo, orange, gumtree, laprensa, elpais, mercadolibre, delfi, olx.
- Resolved ssl issue with dropbox and classification issue with 9game.

20.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

20.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don’t have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

20.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

20.2. Protocol Updates

20.2.1. New Protocols

The following new protocols have been added in this version:

Table 40. New protocols added in this version

Proto ID	Protocol	Description
2096	hln	Belgian news portal
2122	origo	Hungarian news portal
2133	sana	Syrian news portal
2125	postimees	Estonian news portal
2090	filelist	Romanian torrent indexing website
2092	forum	Coratian forum
2138	tawary	Mauritanian news portal
2131	sabay	Cambodian news and information portal
2116	news_mn	Mongolian news portal
2097	hs	Finnish news portal
2084	elnashra	Lebanese news portal
2126	pressan	Icelandic news portal
2095	gossiplankanews	SriLankan news portal
2112	milliyet	Turkish news portal
2109	maybank2u	Malay banking website
2130	rtvslo	Slovenian news portal
2105	lrytas	Lithuanian news portal
2135	skroutz	Greek price comparator
2146	zaluu	Mongolian news portal
2124	pazar3	Macedonian classifed ads
2137	stuff	New zealander news portal
2143	vijesti	Serbian nwes portal
2111	merrjep	Kosovan classified ads
2128	reklama5	Macedonian classifed ads
2091	flipkart	Indian ecommerce website
2088	ethiojobs	Ethiopian job ads
2103	lanacion	Argentinian news portal
2120	onet	Polish news portal
2100	jutarnji	Croatian news portal
2129	rimnow	Mauritanian news portal
2115	nacion	Costa Rican news portal
2093	gerasanews	Jordanian news portal
2089	ethiotube	Ethiopian video hosting website
2142	vanguardngr	Nigerian news portal
2118	novinky	Czech news portal
2085	elsalvador	EL Salvadorian news portal
2106	maannews	Palestinian news portal
2104	lexpress	Mauritian news portal

Proto ID	Protocol	Description
2141	tvnet	Latvian news and content portal
2102	klix	Bosinian news portal
2145	yle	Finnish news portal
2134	shekulli	Albanian news portal
2108	maltatoday	Maltese news portal
2147	zing	Vietnamese classified ads.
2121	onliner	Belarussian ecommerce website
2101	kajgana	Macedonian news portal
2136	souq	Saudi Arabian ecommerce website
2114	monitor	Ugandan news portal
2132	saharamedias	Mauritanian news portal
2144	vnexpress	Vietnamese news portal
2087	essirage	Mauritanian news portal
2117	news24	South African news portal
2119	nu	Dutch news portal
2094	gob	Bolivian government portal
2110	mbl	Icelandic news portal
2113	mistreci	Albanian movie streaming website
2082	apollo_lv	Latvian news portal
2139	topky	Slovak news portal
2099	investigator	Ugandan news portal
2086	emol	Chilean news portal
2107	mako	Israeli news portal
2140	trend	Azerbaijani news portal
2081	999_md	Moldavian classified ads
2123	paraguay	Paraguayan news portal
2083	ask_fm	International Social network

20.2.2. Updated Protocols

The following protocols have evolved in this version:

- dailymotion
- laprensa
- sapo
- elpais
- gumtree
- orange
- olx
- delfi
- mercadolibre
- qq_web

- livemail_mobile
- live_hotmail
- youtube_hd
- windows_marketplace
- wechat
- java_update
- vimeo
- chrome_update
- dropbox

20.2.3. Deprecated Protocols

The following protocols have been deprecated in this version:

Table 41. Deprecated protocols in this version

Proto ID	Protocol	Description	Comments
1281	jajah	Jajah was a VoIP provider owned by Telefonica Europe.	Telefonica has shut down Jajah on January 31, 2014.
1272	hudong	This protocol plug-in classified the http traffic to the host hudong.com.	hudong.com, a major chinese online encyclopedia, is now baike.com.

20.3. Attributes

There are no updates to Attributes in this version.

20.4. Bug Fixes and Known Issues

20.4.1. Bug Fixes

- RTC#9230 - **[9game] Classification issue**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	9game.com isn't detected as 9game

20.4.2. Known Issues

There are no Known Issues in this version.

21. Protocol Bundle 1.41.0

21.1. What's new in the Protocol Bundle 1.41.0

21.1.1. Major enhancements in this release

65 new protocols added, including several popular web portals (see Section 21.2, “Protocol Updates”).

Updated protocol signatures and supported versions for appstore, nba, facebook_apps. See Section 21.4.1, “Bug Fixes”.

Summary of major enhancements :

Ticket ID	Description
RTC#9287	**New protocols to add to cover the top worldwide web sites list**

21.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

21.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don’t have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

21.1.4. Supported platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit User mode LSB 3.x and 4.x, AMP and SMP
- x86 64-bit User mode LSB 3.x and 4.x, AMP and SMP
- x86 32-bit FreeBSD 9, AMP and SMP, with an External Flow Manager
- x86 64-bit FreeBSD 9, AMP and SMP, with an External Flow Manager
- x86 64-bit FreeBSD 8, SMP, with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- Continuous Computing / Radisys PP50 based on dual XLR Processor Family - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium Networks OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium Networks OCTEON II CN68XX - SDK version 2.3
- Tilera TilePro 64
- Tilera TileGx avec MDE version 4.0.0

21.2. Protocol Updates

21.2.1. New Protocols

The following new protocols have been added in this version:

Table 42. New protocols added in this version

Proto ID	Protocol	Description
2043	dr	Danish news and content portal
2021	alwakeelnews	Jordanian news portal
2030	caak	Mongolian news portal
2017	20min	Swiss news portal
2026	bidorbuy	South African auction and shopping website
2061	prodavalnik	Bulgarian classified ads
2018	abola	Portugese sports news portal
2039	dealfish	Thai classified ads
2066	sabq	Saudi Arabian news portal
2049	nation	Kenyan news portal
2071	standardmedia	Kenyan news portal
2020	aliexpress	Chinese ecommerce website
2064	rt	Worldwide Russian news channel in Russian, Arabic, Spanish and English.
2028	bild	German news portal
2048	nagariknews	Nepali news portal
2051	net	Croatian news portal
2054	nzherald	New zealander news portal
2062	puls24	Macedonian news portal
2041	diretube	Ethiopian media website
2077	visir	Icelandic news portal
2074	torg	Uzbek classified ads
2060	press24	Macedonian news portal
2058	partis	Slovenian news portal
2029	blick	Swiss news portal
2065	ruv	Icelandic news portal
2070	sme	Slovak news portal
2025	bankmellat	Iranian Banking website
2034	clarin	Argentinian news portal
2063	repubblica	Italian news portal
2044	elcomercio	Ecuadorian news portal
2080	zamunda	Bulgarian Torrent tracker
2059	philenews	Cypriot news portal
2022	apa	Azerbaijani news portal
2037	dakaractu	Senegalese news portal
2016	edgecast	Edgecast is a file streaming solution provider for audio/video content web services.

Proto ID	Protocol	Description
2015	conviva	Conviva is a video streaming solution provider for audio/video content web services.
2038	day	Azerbaijani news portal
2078	wp	Polish news portal
2052	newsit	Greek news portal
2019	alakhbar	Mauritanian news portal
2040	derstandard	Austrian news portal
2050	nationnews	Barbadian news portal
2073	timesofmalta	Maltese news portal
2024	avaz	Croatian news portal
2047	elmundo	El Salvadorian news portal
2055	onlinekhabar	Nepali news portal
2056	orf	Austrian news portal
2035	coccoc	Vietnamese search engine
2042	doisongphapluat	Vietnamese news portal
2068	seneweb	Senegalese news portal
2036	cyberctm	Chinese news portal
2069	siol	Slovenian news portal
2027	bikhir	Moroccan classified ads
2057	pantip	Thai information and entertainment portal
2072	tasweernews	Jordanian news portal
2046	elheraldo	Honduran news portral
2023	atlasinfo	Mauritanian news portal
2031	cas	Slovak news portal
2075	uol	Brazalian news portal
2079	ynet	Israeli news portal
2076	vg	Norwegian news portal
2032	cdm	Montenegrin news portal
2067	sameerbook	Jordanian news portal
2053	nrk	Norwegian news portal
2045	eldeber	Bolivian news portal

21.2.2. Deprecated Protocols

No protocols have been deprecated in this version.

21.3. Attributes

This section describes the updates to Attributes.

21.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

21.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

21.3.1.2. Event Attributes added in this version

No Event Attributes have been added in this version.

21.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

21.3.3. Event Attributes modified in this version

No Event Attributes have been modified in this version.

21.4. Bug Fixes and Known Issues

21.4.1. Bug Fixes

- RTC#9011 - **[facebook_apps] check proto_evolution**

Bug Info	Description
Reported against	ProtocolBundle-1.41.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	update protocol + supported version : v4.0.0 (Android);v6.8 (iOS)

- RTC#9005 - **[appstore] check proto_evolution**

Bug Info	Description
Reported against	ProtocolBundle-1.41.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Update protocol + supported version : iOS 7.0.4

- RTC#9002 - **[nba] check proto_evolution**

Bug Info	Description
Reported against	ProtocolBundle-1.41.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Update protocol + supported version : 5.1.4 (iOS), 4.1106 (Android)

- RTC#8584 - **[vkontakte] support mobile versions**

Bug Info	Description
Reported against	ProtocolBundle-1.41.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Update protocol : supported version :3.3.2 (Android), 2.0 (iOS), 3.0.3 (WinPhone)

- RTC#8581 - **[cnn] support version 2.01**

Bug Info	Description
Reported against	ProtocolBundle-1.41.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Update protocol + supported version : 2.0 (iOS)

- RTC#8578 - **[google_maps] support last versions of mobile application**

Bug Info	Description
Reported against	ProtocolBundle-1.41.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Update protocol on windowsphone platform. Software version : 8.0.9.1

- RTC#8575 - **[baidu] support version 5.0 + web update**

Bug Info	Description
Reported against	ProtocolBundle-1.41.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Update protocol + supported versions : 5.0.1 (iOS), 5.0 (Android).

- RTC#9344 - **[vimeo] add support for Vimeo android mobile application**

Bug Info	Description
Reported against	ProtocolBundle-1.41.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Update protocol + supported version : 1.1.41 (Android)

- RTC#9329 - **[linkedIn] Classification problem over the HTTPS layer**

Bug Info	Description
Reported against	PB 1.40.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Correction of the protocol plugin LinkedIn for classification over the HTTPS layer.

- RTC#9314 - **[chat_on] update signatures to maximize classification**

Bug Info	Description
Reported against	ProtocolBundle-1.41.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Update. Supported versions : 3.2.137 (Android) 2.7.7 (iOS)

- RTC#9311 - **[qq_games] update signatures to support localized application (China)**

Bug Info	Description
Reported against	ProtocolBundle-1.41.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Update protocol

21.4.2. Known Issues

There are no Known Issues in this version.

22. Protocol Bundle 1.40.0

22.1. What's new in the Protocol Bundle 1.40.0

22.1.1. Major enhancements in this release

19 new Protocols added (see Section 22.2, “Protocol Updates”), including

- blackberry_messenger BBM 10 (audio/video)
- several P2P protocols (e.g. filesharepro, allmusic ...)

18 new Event Attributes added (see Section 22.3, “Attributes”), including

- metadata on radius (3GPP IMSI)
- new http attributes for host offsets
- facetime : support for new service_info attributes

Summary of major enhancements :

Ticket ID	Description
SF#6915 - RTC#5242	**[peerguardian] add classification (p2p)**
SF#6915 - RTC#5239	**[mp3_rocket] add classification (p2p)**
SF#6915 - RTC#5236	**[allmusic] add classification (p2p)**
SF#6897 - RTC#3117	**[ftp] attributes structuration**
RTC#322	**[SF6236] [blackberry_messenger] BBM 10 support (audio/video)**
SF#7283 - RTC#6093	**[SF7283] [opengw] Add new protocol (Tunneling)**
SF#7282 - RTC#6090	**[SF7282][gbridge] Add new protocol Gbridge (Tunneling)**
SF#7383 - RTC#6853	**[nfs] extraction improvement**
SF#7368 - RTC#6665	**[facetime] add extraction service_info structure**
SF#7296 - RTC#6645	**[http] Add http host offsets (start and end)**
SF#7280 - RTC#6635	**[vtunnel] support classification of protocols over vtunnel proxy**
SF#7166 - RTC#6371	**[radius] add metadata (3GPP IMSI)**
SF#7285 - RTC#6099	**[SF7285][hamachi] Add new protocol Hamachi (Tunneling)**
SF#7284 - RTC#6096	**[SF7284][asproxy] Add new protocol Asproxy (Tunneling)**
RTC#7061	**[pdata] reduce allocation of protocol data at initialization**
SF#7468 - RTC#7640	**[SF7468] [http] Add LAST_MODIFIED attribute**
SF#7481 - RTC#7821	**[krb5] Extendable krb5 buffer**
SF#7434 - RTC#7784	**[SCTP] SCTP over IPv6**
RTC#8125	**[http] add new 'application' attribute**
RTC#8262	**[pdata] buff_alloc versus stack allocation**
RTC#8479	**[bittorrent] support specific BitTorrent clients**
RTC#8477	**[ares] classification with spid**
RTC#8472	**[thunder] Classification must be enhanced**

22.1.2. ixEngine compatibility

This Protocol Bundle is fully compatible with:

- ixEngine 4.15.x versions 4.15.0-26 and higher.
- ixEngine 4.16.x versions 4.16.2-20 and higher.
- ixEngine 4.17.x versions 4.17.0-20 and higher.
- ixEngine 4.18.x versions 4.18.0-26 and higher.

22.1.3. Installation procedure

This Protocol Bundle can be directly included in your ixEngine or loaded via the hot swap API.

To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

```
gcc user_application.c -L. -lqmengine -lqmprotocols -o application
```

If you plan to use the hot swap API, you don't have to link your application with the libqmprotocols. For example:

```
gcc user_application.c -L. -lqmengine -o application
```

Note:

Do not forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

22.1.4. Supported Platforms

This version has been validated on the following hardware platforms:

x86 platforms

- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) Monothread
- x86 32-bit and 64-bit User-Mode LSB (Linux Standard Base 3.x) SMP
- x86 32-bit Solaris 10 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 AMP with an External Flow Manager
- x86 32-bit and 64-bit FreeBSD 9 SMP with an External Flow Manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6

- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

22.2. Protocol Updates

22.2.1. New Protocols

The following new protocols have been added in this version:

Table 43. New protocols added in this version

Proto ID	Protocol	Description
1557	bbm	BBM is the messenger/voip/Video protocol for blackberry. This plug-in classifies the audio and video data flows of BlackBerry Messenger.
1558	bbm_audio	bbm_audio is the voip layer of the blackberry's messenger.
1559	bbm_video	BBM_video is the video layer of the blackberry's messenger.
2009	gbridge	Gbridge is a free software that lets you remotely control PCs, sync folders, share files, and chat securely.
2002	hotspot_shield	The Hotspot Shield application secures internet connections made from public access points using a VPN network.
2011	path	It is a free social instant messenger for private messaging and sharing photos, videos, music, etc.
1695	softros_messenger	Softros Messenger is a LAN messaging and file transfer application.
2005	hamachi	Hamachi is a VPN service provided by LogMeIn. This signature classifies traffic to the LogMeIn servers used by Hamachi. The P2P VPN streams between users are using IPSEC, and won't be classified as hamachi, but ipsec instead.
2001	frostwire	FrostWire is a BitTorrent client. This signature classifies flows to the official software website
2010	asproxy	ASProxy is a free and open-source web proxy which allows the user to surf the net anonymously. This plug-in classifies the usage of this proxy for web browsing, as a fallback to other recognized applications/protocols.
1560	blackberry_locate	This protocol refers to all Blackberry mobile device communications about localization over wifi.
2003	allmusic	Allmusic is an online music guide service website. This plug-in classifies navigation on the AllMusic web service, and MP3 music playback. Video clip streaming is handled by youtube.
2006	peerguardian	PeerGuardian is capable of blocking incoming and outgoing connections based on IP blacklists. This plug-in classifies the firewall attempts to update its blacklist from PeerGuardian servers.
1907	filesharepro	File transfer application, allowing file sharing on a LAN network, or on the Internet.

Proto ID	Protocol	Description
2004	mp3_rocket	MP3 Rocket is a music file downloader application. It uses the Youtube (aka Google Video) service to search and download video clips, and then transforms them into MP3 files on the host machine using a MP3 converter. This plug-in only classifies secondary flows of the application, like client updates. Video clip downloads are classified as youtube.
2007	freeproxies	Proxy hosting service (redirector and anonymizer) that uses the CGI Proxy script. Main features are SSL support and Youtube.com video streaming proxying. It hosts several proxy websites, like Vtunnel.com.
2013	xl_nonton	XL Nonton offers access streaming contents via PC and Smartphone.
2012	xl_webportal	Indonesian mobile telecommunications services operator web portal.
2008	opengw	OpenGW (aka VPN Gate) is a Public VPN Relay Servers service, used in several VPN solutions (example: PacketiX. This service uses the SoftEther VPN technology).

22.2.2. Deprecated Protocols

No protocols have been deprecated in this version.

22.3. Attributes

This section describes the updates to Attributes.

22.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

22.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

22.3.1.2. Event Attributes added in this version

Table 44. Added Event Attributes

Protocol	New event attributes
facetime	end
facetime	service
facetime	service_duration
facetime	service_id
facetime	service_info
ftp	method_content
ftp	request
http	host_end_offset
http	host_start_offset
http	last_modified
kaskus	end
kaskus	query
kaskus	query_raw
kaskus	query_text
kaskus	title
owa	msglist_receiver
radius	3gpp_imsi
ymail_mobile_new	msglist_content

22.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

22.3.3. Event Attributes modified in this version

The following Event Attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 45. Modified Event Attributes

Protocol	Event attribute	Changes
ftp	method	in PB 1.31.0 [string,client,session_mod,command] in PB 1.40.0 [string,client,session_mod,request]
yahoo_search	encoding	in PB 1.31.0 [string,client,session_fix,no_parent] in PB 1.40.0 [string,both,session_mod,no_parent]
yahoo_search	query	in PB 1.31.0 [parent,client,session_mod,no_parent] in PB 1.40.0 [parent,both,session_mod,no_parent]
yahoo_search	query_raw	in PB 1.31.0 [string,client,session_prt,query] in PB 1.40.0 [string,both,session_mod,query]
yahoo_search	query_text	in PB 1.31.0 [string,client,session_prt,query] in PB 1.40.0 [string,both,session_mod,query]
yahoo_search	query_type	in PB 1.31.0 [string,client,session_prt,query] in PB 1.40.0 [string,both,session_mod,query]

22.4. Bug Fixes and Known Issues

22.4.1. Bug Fixes

- SF#7012 - RTC#5614 - **[rtp] codec_name is missing**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	[rtp] codec_name is missing

- SF#7241 - RTC#2950 - **[pdata] updata_layer.c generation fails if no "category" tag is present in pdd file**

Bug Info	Description
Reported against	PB 1.17.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	PDB compilation fails if there's no category tag in PDD file.

- SF#6617 - RTC#1822 - **[funshion] classification issue**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification issues concerning Funshion smart client usage.

- SF#7183 - RTC#5336 - **[skype] improved service type extraction with skype client 6.9**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Improve service type extraction on low bitrate workflows with latest skype clients.

- SF#7337 - RTC#6353 - **[SF7337][ip6][defrag issue**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	TBD

- SF#7427 - RTC#7257 - **[SF7427][google_play] application_name not extracted**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Fix application_name extraction

- SF#7357 - RTC#7043 - **[SF7357] [smtp] BDAT chunks extraction anomaly**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	SMTP: BDAT chunks extraction fix

- SF#7447 - RTC#7360 - **[SF7447] [yahoo_search] classified after http:uri extraction so yahoo_search:query is not extracted**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Yahoo search protocol update

- SF#7469 - RTC#7591 - **[SF7469] [youtube] video_duration extraction code seems to be missing**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Fix youtube:video_duration extraction

- SF#7470 - RTC#7585 - **[SF7470] [baidu] query not extracted**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Fix query & query_raw extraction

- SF#7462 - RTC#7547 - **[http] new supported methods seems to be not fully supported**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Extraction Anomaly

Bug Info	Description
Expected versus actual behavior	N/A

- SF#7395 - RTC#7443 - **[ssl] [extflow] losing classification with NPN and missing peer**

Bug Info	Description
Reported against	ProtocolBundle-1.30.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	In External flow flavour, a SSL session using NPN may be declassified then reclassified with less precision.

- SF#7491 - RTC#8025 - **[SF7491][line] missing host**

Bug Info	Description
Reported against	PB 1.31.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	a line host not supported

- SF#7524 - RTC#8237 - **[pdata] ctl_pdata_load abort on double free when a dynamic layer has been already created.**

Bug Info	Description
Reported against	ProtocolBundle-1.30.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	issue on ctl_pdata_load

- SF#7530 - RTC#8287 - **[youtube] not any metadata extracted from cutstomer trace**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	attributes correctly extracted with mobile apps

- RTC#8475 - **[wechat] add classification for file transfer workflow**

Bug Info	Description
Reported against	ProtocolBundle-1.30.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	

- RTC#8474 - **[windows_azure] improve classification over http**

Bug Info	Description
Reported against	ProtocolBundle-1.31.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	

- RTC#8473 - **[ares] Ares Protocol over multiple ports classification issue**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	

- RTC#8790 - **[SF7588] Application ID mismatch (centrum, flycell, index,hr, jobs.af)**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	

22.4.2. Known Issues

- RTC#7058 - **[SF7376][gtpv2] add message_type strings**

Bug Info	Description
Reported against	PB 1.31.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	improve gtpv2 message_type extraction
Workaround	No workaround

- SF#6862 - RTC#5440 - **[ftp_data] does not support FTP connection reset.**

Bug Info	Description
Reported against	ProtocolBundle-1.40.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	FTP_DATA does not support connection reset.
Workaround	No workaround

23. Protocol Bundle 1.31.0

23.1. What's new in the Protocol Bundle 1.31.0

23.1.1. Note about the major enhancements of the release

- 22 new Protocols added. See Section 23.2, “Protocol updates”; the directdownloadlinks signature has been split into multiple protocol signatures, one for each type of link provided by directdownloadlinks.
- The following protocol signatures have been updated :
  - [wechat] protocol update detected (udp.unknown)
  - [ymail_classic] protocol update
  - [ymail_mobile_new] protocol update
  - [vkontakte] protocol update
  - [chrome_update] protocol update
  - [spotify] protocol update detected version 0.9.4.169
  - [google_plus] protocol update

23.1.2. ixEngine compatibility

This protocol bundle is fully compatible with

- ixe 4.15.x versions 4.15.0-26 and higher
- ixe 4.16.x versions 4.16.2-20 and higher
- ixe 4.17.x versions 4.17.0-20 and higher
- ixe 4.18.x versions 4.18.0-26 and higher

23.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

  ```
  gcc user_application.c -L. -lqmengine -lqmprotocols -o application
  ```

- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example:

  ```
  gcc user_application.c -L. -lqmengine -o application
  ```

Note:

Don’t forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

23.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager
- This version has been validated on FreeBSD 9 for x86 32-bit and 64-bit AMP and SMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

23.2. Protocol updates

23.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 46. New protocols added in this version

Proto ID	Protocol	Description
1955	data_hu	Classifies web browsing on the data.hu Direct DownLoad links service.
1957	filepost_ru	Classifies web browsing on the filepost.ru Direct DownLoad links service.
1958	ifolder_ru	Classifies web browsing on the ifolder.ru Direct DownLoad links service.
1961	load_to	Classifies web browsing on the load.to Direct DownLoad links service.
1963	uploaded_net	Classifies web browsing on the uploaded.net Direct DownLoad links service.
1964	leteckaposta_cz	Classifies web browsing on the leteckaposta.cz Direct DownLoad links service.
1965	yourfiles_biz	Classifies web browsing on the yourfiles.biz Direct DownLoad links service.
1967	ultrashare_net	Classifies web browsing on the ultrashare.net Direct DownLoad links service.
1970	upload_com	Classifies web browsing on the CNET upload.com Direct DownLoad links service.
1971	rapidupload_com	Classifies web browsing on the rapidupload.com Direct DownLoad links service.
1972	transferbigfiles_com	Classifies web browsing on the transferbigfiles.com Direct DownLoad links service.
1974	bestsharing_com	Classifies web browsing on the bestsharing.com Direct DownLoad links service.
1978	savefile_com	Classifies web browsing on the savefile.com Direct DownLoad links service.
1987	gigasize_com	Classifies web browsing on the gigasize.com Direct DownLoad links service.
1988	sharebee_com	Classifies web browsing on the sharebee.com Direct DownLoad links service.
1989	megashares_com	Classifies web browsing on the megashares.com Direct DownLoad links service.
1991	filefactory_com	Classifies web browsing on the filefactory.com Direct DownLoad links service.
1993	uploadingit_com	Classifies web browsing on the uploadingit.com Direct DownLoad links service.
1995	simpleupload_net	Classifies web browsing on the simpleupload.net Direct DownLoad links service.
1997	filesend_net	Classifies web browsing on the filesend.net Direct DownLoad links service.
1998	filer_net	Classifies web browsing on the filer.net Direct DownLoad links service.

Proto ID	Protocol	Description
2000	odsiebie_najlepsze_net	Classifies web browsing on the odsiebie.najlepsze.net Direct DownLoad links service.

23.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

23.3. Attributes

This section describes the attribute updates.

23.3.1. New event attributes added in this version

There are no event attributes added in this version.

23.3.2. Deprecated event attributes in this version

There are no deprecated event attributes in this version.

23.3.3. Event attributes modified in this version

There are no event attributes modified in this version.

23.4. Bugs fixed and Known Issues

23.4.1. Bugs fixed in this version

- SF#7407 - RTC#7319 - **[protobook] remove the "deprecated" qualification on protocol which can still be classified**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Remove the "deprecated" qualification on protocol which can still be classified

- SF#7395 - RTC#6884 - **[ssl][google_maps] classification over spdy.google_gen lost when dropping tcp syn packets**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Classification anomaly.
Expected versus actual behavior	Poor google_maps classification when using the option drop-syn.

23.4.2. Known issues

There are no known issues raised in this version.

24. Protocol Bundle 1.30.0

24.1. What's new in the Protocol Bundle 1.30.0

24.1.1. Note about the major enhancements of the release

- 46 new Protocols added. See Section 24.2, “Protocol updates”
- 10 new Event Attributes added. See Section 24.3, “Attributes”
- New `service_info` parent attribute for `service`, `service_id` and `service_duration` attributes. This attribute is available for `skype`, `viber`, `line` and `tango`.
- New payload types and EVRC codec support for `rtp`.

24.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-26 and higher (for ixe 4.15.x versions), ixEngine 4.16.2-20 and higher (for ixe 4.16.x versions) and 4.17.0-20 and higher versions of ixEngine.

24.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

  ```
  gcc user_application.c -L. -lqmengine -lqmprotocols -o application
  ```

- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example:

  ```
  gcc user_application.c -L. -lqmengine -o application
  ```

Note:

Don’t forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

24.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread

- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager
- This version has been validated on FreeBSD 9 for x86 32-bit and 64-bit AMP and SMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

24.2. Protocol updates

24.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 47. New protocols added in this version

Proto ID	Protocol	Description
1906	iscsi	Internet Small Computer Systems Interface (iSCSI), as described in RFC3720.
1917	ndmp	NDMP (Network Data Management Protocol) is an open protocol for enterprise-wide network based backup over TCP.
1916	quantum_dxi_ost	Classifies the Symantec NetBackup streams that use the Quantum DXi replication solution. This implements the OpenStorage API (OST).
1914	worksite	WorkSite is a Document Management System (DMS) application. It is primarily used by law firms and corporate legal departments.
1915	ypbind	The ypbind utility is the process that maintains NIS binding information. At startup, it searches for an NIS server responsible for serving the system's default domain (as set by the domainname(1) command) using net-work broadcasts
1912	imessage_file_download	Apple Web Service used to retrieve video messages sent between two iOS devices via the iMessage application. This signature only classifies video download from the message receiver device. The video upload from the sender will be classified as apns (Apple Push Notification)
1913	bits	Background Intelligent Transfer Service (BITS) transfers files (downloads or uploads) between a client and server and provides progress information related to the transfers.
1910	somud	SoMud is a BitTorrent client. This signature classifies BitTorrent tracker streams over http specific to the SoMud client. Data streams will be classified as bittorrent only.
1918	maltapark	Maltapark is the most popular trading website in Malta.
1919	mana	French Polynesian internet service provider website
1920	marktplaats	Dutch advertising site where you can sell, new and second-hand goods.
1921	mihanblog	Persian blogging platform
1922	moov	Malagasy internet web portal
1923	motika	Macedonian video posting website.
1924	mudah	Malaisian free classified ads.
1925	nairaland	Nigerian forum hosting site
1926	namba	Kyrgyzstani forum and social networking site.
1927	njuskalo	Croatian online classified ads

Proto ID	Protocol	Description
1928	ouedkniss	Algerian internet portal
1929	persianblog	Persian blogging platform
1930	petitesannonces	French Polinesian online classified ads
1931	peyvandha	Persian internet portal.
1932	pik	Bosnian online trading website.
1933	plius	Lithuanian online classified ads.
1934	qatarliving	Qatari online classified ads.
1935	radio1	French Polinesian radio broadcast website.
1936	ricardo	Swiss online trading website.
1937	sahibinden	Turkish online classified ads and e-commerce platform.
1938	saitebi	Georgian internet catalog.
1909	sccm	System Center Configuration Manager, is a systems management software product by Microsoft for managing large groups of computers running Windows, Mac OS X, Linux or UNIX, as well as various mobile operating systems.
1939	seznam	Czech internet web protal.
1940	shobiddak	Palestinian online classified ads.
1941	skelbiu	Lithuanian online classified ads and trading website.
1942	s_oman	Omani forum hosting website.
1943	ss	Latvian online classified ads.
1944	sulit	Filipino online classified ads.
1945	super	Prague based agency represents models from Czech and Slovak Republic.
1947	trademe	New Zealander online trading site.
1948	tunisia_sat	Tunisian forum hosting platform.
1949	tut	Belarusian internet portal.
1911	tvking	TvKing is an application which is able to get video stream lists from its own web site and from other ones. Classifies HTTP web browsing only.
1950	varzesh3	Persian online sports new portal.
1951	vbox7	Bulgarian video streaming website.
1952	walla	Israelian internet portal.
1953	willhaben	Austrian online classified ads.
1954	zoznam	Slovakian internet portal.

24.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

24.3. Attributes

This section describes the attribute updates.

24.3.1. New event attributes added in this version

The following event attributes have been added in this version.

24.3.1.1. Generic events added in this version

There are no generic events added in this version.

24.3.1.2. Events added in this version

Table 48. Added event attributes

Protocol	New event attributes
line	service_duration
line	service_info
sip	expires
skype	end
skype	service_info
smb	security_blob
smb	security_blob_len
ssl	certificate_raw
tango	service_info
viber	service_info

24.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 49. Deprecated event attributes

Protocol	Deprecated event attributes	Comments
rsh	remote_login	This attribute is now deprecated.

24.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 50. Event attributes modified

Protocol	Event attribute	Changes
line	service	in PB 1.23 [string,both,session_mod,no_parent] in PB 1.30 [string,both,session_mod,service_info]
line	service_id	in PB 1.23 [int32,both,session_mod,no_parent] in PB 1.30 [int32,both,session_mod,service_info]
rsh	login	in PB 1.23 [string,client,session_mod,no_parent] in PB 1.30 [string,client,session_fix,no_parent]
sip	method	in PB 1.23 [string,client,session_prt,request] in PB 1.30 [string,both,session_prt,request]
skyblog	account	in PB 1.23 [parent,client,session_fix,no_parent] in PB 1.30 [parent,both,session_mod,no_parent]
skyblog	login	in PB 1.23 [string,client,session_prt,account] in PB 1.30 [string,both,session_mod,account]
skyblog	password	in PB 1.23 [string,client,session_prt,account] in PB 1.30 [string,both,session_mod,account]
skype	service	in PB 1.23 [string,both,session_mod,no_parent] in PB 1.30 [string,both,session_prt,service_info]
skype	service_duration	in PB 1.23 [uint32,both,session_mod,no_parent] in PB 1.30 [uint32,both,session_prt,service_info]
skype	service_id	in PB 1.23 [uint32,both,session_mod,no_parent] in PB 1.30 [uint32,both,session_prt,service_info]
smpp	content	in PB 1.23 [binary,both,session_prt,message] in PB 1.30 [buffer,both,session_prt,message]

Protocol	Event attribute	Changes
tango	service	in PB 1.23 [string,both,session_mod,no_parent] in PB 1.30 [string,both,session_mod,service_info]
tango	service_duration	in PB 1.23 [int32,both,session_mod,no_parent] in PB 1.30 [int32,both,session_mod,service_info]
tango	service_id	in PB 1.23 [int32,both,session_mod,no_parent] in PB 1.30 [int32,both,session_mod,service_info]
viber	service	in PB 1.23 [string,both,session_mod,no_parent] in PB 1.30 [string,both,session_prt,service_info]
viber	service_duration	in PB 1.23 [uint32,both,session_mod,no_parent] in PB 1.30 [uint32,both,session_prt,service_info]
viber	service_id	in PB 1.23 [uint32,both,session_mod,no_parent] in PB 1.30 [uint32,both,session_prt,service_info]

24.4. Bug fixed and known issues

24.4.1. Bugs fixed in this version

- SF#6546 - RTC#1844 - **[udp] Invalid checksum errors reported by udp.wrong_crc**

Bug Info	Description
Reported against	ProtocolBundle-1.15.0
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	Checksum verification is invalid in case of udp over gtp with fragmented ip packets, and UDP wrong_crc attribute is incorrectly reported.

- RTC#2097 - **[orangemail] attach_content extraction bug**

Bug Info	Description
Reported against	ProtocolBundle-1.9.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	When attached content is in http multipart, bounds aren't sought properly.

- RTC#3523 - **[Jabber] False classification**

Bug Info	Description
Reported against	PB 1.5.1
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	don't update l3l4 cache for jabber over proxy

- RTC#3611 - **[base] fix time attributes**

Bug Info	Description
Reported against	ProtocolBundle-1.13.0 / 1.15.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	

- SF#7123 - RTC#4415 - **[SF7123][HTTP] base:classified=1 not raised**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	The event attribute base:classified=1 is not extracted for an HTTP session

- SF#5737 - RTC#4498 - **[SF5737] [ppstream/pps] Protocol update**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Missing HTTP hosts in pps plugin

- SF#7175 - RTC#4642 - **[imesh]: PR-924579:NgAppid:Some IMESH UDP Probes are reporting as UNKNOWN**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	enhance imesh classification

- SF#7179 - RTC#4704 - **[SF7179][sip] extraction issue of the attributes media_attr_addr and media_attr_addr_v6**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	The attributes media_attr_addr and media_attr_addr_v6 are not extracted from traffic including SDP information.

- SF#7299 - RTC#5992 - **[RSH] rsh sessions not classified**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Some RSH sessions are not classified as the protocol processes them as separate packets

- SF#7198 - RTC#4962 - **[Sohu]: classification improvement**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	sohu videostream classification update

- SF#7129 - RTC#4965 - **msn:encoding extraction bug**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Not Applicable

Bug Info	Description
Expected versus actual behavior	MSN module does not extract text encoding well if the last header in a message is a content-type header

- RTC#4979 - **[ocsp] Classification overlapping on next http request**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	

- SF#7206 - RTC#4998 - **[SF7206] [netflix] support extraction of metadata for Netflix/ HLS**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	add support for some meta data extraction of NETFLIX.

- SF#7201 - RTC#5121 - **mgcp: extraction of call_id for short values fail**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	MGCP call_id should be a string of hexadecimal digits of length 1-32. Current ixE does not extract call_id of length 1 or 2.

- SF#7139 - RTC#5357 - **[SF 7139] HTTP CONNECT: do not extract 2 values for request_size**

Bug Info	Description
Reported against	PB 1.17 for DF
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	In case of HTTP CONNECT method, the attribute request_size is extracted 2 times (at the end of headers and at the end of the session)

- SF#7252 - RTC#5478 - **[SF7252][pdata] allow empty pdd files**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	allow empty pdd files when merging pdata.

- RTC#5482 - **[skype] service duration wrong value on x86_32**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	

- RTC#5672 - **[http] fix memory leak in priv struct.**

Bug Info	Description
Reported against	ProtocolBundle-1.23.0
Platform	All
Effect of bug	Memory Leak
Expected versus actual behavior	The probelm occurs during a merge of two different sessions already classified as HTTP. [fuzzing] [http] : 360 bytes in 1 blocks are definitely lost in loss record 1 of 1

- RTC#5880 - **[fuzzing] [udp] [PDATA] Conditional jump or move depends on uninitialised value(s)**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Conditional jump or move depends on uninitialised value(s)

- RTC#5938 - **ip4 defrag can concatenate packet from different ip addr two-tuple**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	ip4 defrag reassembles packets from different ip addr two-tuple since only src_addr and id are checked.

- SF#7003 - RTC#5959 - **[http] wrong and request_size value**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	The http request_size value is incorrect

- SF#7277 - RTC#6203 - **ssl: common_name extraction improvement**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly

Bug Info	Description
Expected versus actual behavior	The ssl module does not extract common_name/issuer when a common name item is the second item in a setssl

- SF#7325 - RTC#6320 - **[SF7325][shoutcast] classification regression**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Improve shoutcast classification on ICY server responses

- RTC#6342 - **[SF7310][youtube] improving classification**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	

- SF#7338 - RTC#6380 - **[silverlight] classification regression**

Bug Info	Description
Reported against	PB 1.23.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	The classification of Silverlight over Akamai is not supported

- SF#7358 - RTC#6540 - **[SF7358]: detect SSH session inside http_tunnel**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	SSH sessions are not identified inside http_tunnel

- SF#7363 - RTC#6574 - **[nntp] sessions not identified**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	enhance NNTP classification

- SF#7370 - RTC#6648 - **[SF7370] [Netflow] sessions are not identified**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0

Bug Info	Description
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Netflow sessions are not identified

- SF#7387 - RTC#6828 - **[ftp_data] classification improvement**

Bug Info	Description
Reported against	ProtocolBundle-1.23.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Ftp_data classification improvement.

24.4.2. Known issues

- SF#7279 - RTC#5782 - **[SF7279] fix inner defrag6**

Bug Info	Description
Reported against	ProtocolBundle-1.30.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Activating inner IP defragmentation on IPv4 and IPv6 packets.
Workaround	No workaround

- RTC#6583 - **[APPSDK] Public PB header uhttp.h must split in two parts: public and private features**

Bug Info	Description
Reported against	ProtocolBundle-1.30.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	
Workaround	No workaround

25. Protocol Bundle 1.23.0

25.1. What's new in the Protocol Bundle 1.23.0

25.1.1. Note about the major enhancements of the release

- 105 new Protocols added, including:
  - dubizzle: Dubizzle is a free classifieds website covering Arabian Peninsula and Maghreb.
  - craigslist: Online classified ads mostly used in the US and Canada.
  - gulfup: Online file sharing website popular in Saudi Arabia and countries around the Gulf.
  - inbox: Latvian webmail and wep portal.
  - lotterypost: Provides information about winning lottery numbers in the US.
  - bluewin: Swiss news portal.

  See Section 25.2, “Protocol updates”.

25.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-26 and higher (for ixe 4.15.x versions), ixEngine 4.16.2-20 and higher (for ixe 4.16.x versions) and 4.17.0-20 and higher versions of ixEngine.

25.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

  ```
  gcc user_application.c -L. -lqmengine -lqmprotocols -o application
  ```

- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example:

  ```
  gcc user_application.c -L. -lqmengine -o application
  ```

Note:

Don’t forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

25.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

25.2. Protocol updates

25.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 51. New protocols added in this version

Proto ID	Protocol	Description
1819	15min	Lithuanian news portal
1820	24h	Vietnamese news portal
1821	24ora	Aruban news portal
1822	24sata	Croatian news portal
1823	24ur	Slovenian news portal
1824	abc_news	Paraguayan news portal
1825	abidjan	Cote d Ivoire news portal
1826	abv	Bulgarian webmail
1827	aftonbladet	Swedish news portal
1828	aktuality	Slovak news portal
1829	alfajertv	Palestinian news portal
1830	allegro	Polish shopping web portal
1831	almanar	Lebanese news portal
1832	alnilin	Sudanese news portal
1833	alrakoba	Sudanese news portal
1834	alwatanvoice	Palestinian news portal
1835	ambebi	Georgian news portal
1836	aprod	Hungarian free classifieds website
1800	avito_ma	Free Moroccan classified ads
1801	avito_ru	Free russian classified ads
1837	avto	Slovenian vehicle related classifieds
1838	azet	Slovak web portal
1839	b92	Serbian news portal
1840	balkanweb	Albanian news portal
1841	banglanews24	Bangladeshi news portal
1842	bdnews24	Bangladeshi news portal
1806	blic	Serbian news portal
1843	blocket	Swedish local classified ads
1844	blog	Hungarian blog hosting website
1845	bluewin	Swiss news portal
1846	bolha	Slovenian local classified ads
1802	bt_bt	Bhutan Telecom Limited (BTL) is the leading provider of telecommunications and Internet services in the Kingdom of Bhutan.
1803	bt_dk	Danish news portal
1805	caf	French National Fund for Family Allowances (Caisse d Allocation familiale)
1807	centrum_cz	SMS alerts service based in Ecuador

Proto ID	Protocol	Description
1808	centrum_sk	Slovakian web portal
1847	clasificadosonline	Puerto Rican classified ads
1848	craigslist	Online classified ads mostly used in the US and Canada
1849	crnobelo	Macedonian news portal
1850	dagbladet	Norwegian news portal
1851	dantri	Vietnamese news portal
1852	dap_news	Cambodian news portal
1853	dbs	Singaporian online banking website
1854	defimedia	Mauritian news portal
1855	dir	Bulgarian news portal
1856	donedeal	Irish classified ads website
1857	dorgio	Mongolian news portal
1858	draugas	Lithuanian web portal
1859	druknet	Buthan Telecom website
1860	dstv	Program synopsis and channel information for South Africa satellite network.
1817	dubizzle	Dubizzle is your free classifieds website to buy, sell and find anything in your local community. It is covering Arabian Peninsula and Maghreb.
1861	dv	Icelandic news portal
1862	echoroukonline	Algerian news portal
1863	ekantipur	Nepalese news portal
1864	ekstrabladet	Danish news portal
1865	elcat	Kyrgyzstanese internet service provider
1866	elheddaf	Algerian sports new portal
1867	elnuevodia	Puerto Rican news portal
1868	elnuevodiario	Nicaraguan news portal
1869	facenama	Iranian social network
1870	farsnews	Iranian news portal
1871	fatakat	Egyptian portal targeted to arab wowen lifestyle
1872	fijitimes	Fijian news portal
1873	finn	Norwegian web portal
1809	flycell_ec	Croatian web portal
1810	flycell_pe	Peruvian ringtone, wallpaper and mobile game portal
1874	foreningssparbanken	Swedish web portal
1875	freemail	Hungarian webmail
1876	garaanews	Jordanian news portal
1877	gazeta	Polish news portal
1878	ghanaweb	Ghanaian news portal
1879	globo	Brazilian news portal
1880	gogo	Mongolian search engine and web portal
1881	grid	Macedonian news portal
1882	guampdn	Guamanian news portal
1816	gulfup	Online file sharing website popular in Saudi Arabia and countries around the Gulf

Proto ID	Protocol	Description
1883	haveeru	Maldivian news portal
1884	hespress	Moroccan news portal
1804	hkgolden	Game and electonics news portal based in Hong Kong
1885	hurriyet	Turkish news portal
1886	ibay	Maldivian online classified ads
1887	idnes	Czech news portal
1888	igihe	Rwandan news website
1889	ikman	Sri Lankan free online classified ads
1890	ikub	Albanian web portal
1891	iltalehti	Finnish news portal
1892	iltasanomat	Finnish news portal
1893	inbox	Latvian webmail and wep portal
1812	index_hr	Online job search in Afghanistan
1813	index_hu	Hungarian web portal
1894	indiatimes	Indian news portal
1895	ing	ING online banking website
1896	interia	Polish news portal
1898	jamiiforums	Tanzanian forum and blog hosting site
1897	ja	Icelandic web portal
1814	jobs_af	Czech web portal
1815	jobs_bg	Bulgarian online job search
1899	khmerload	Cambodian web portal
1900	kigalitoday	Rwandese news portal
1901	kijiji	Canadian free local classifieds
1902	kuenselonline	Bhutanese news portal
1818	kurir_info	Serbian news portal
1903	laprensa	Nicaraguan news portal
1904	leral	Senegalese news portal
1905	lotterypost	Provides information about winning lottery numbers in the US

25.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

25.3. Attributes

This section describes the attribute updates.

25.3.1. New event attributes added in this version

25.3.1.1. Generic events added in this version

There are no generic events added in this version.

25.3.1.2. Events added in this version

There are no events added in this version.

25.3.2. Deprecated event attributes in this version

No event attributes have been deprecated in this version.

25.3.3. Event attributes modified in this version

No event attributes have been modified in this version.

25.4. Bug fixed and known issues

25.4.1. Bugs fixed in this version

There are no bugs fixed in this version.

25.4.2. Known issues

There are no known issues raised in this version.

26. Protocol Bundle 1.22.0

26.1. What's new in the Protocol Bundle 1.22.0

26.1.1. Note about the major enhancements of the release

- 127 new Protocols added. See Section 26.2, “Protocol updates”.
- 15 new Event Attributes added. See Section 26.3, “Attributes”.
- Added support on `wikipedia` mobile applications.
- Enhanced support on `dropbox` for the Dropbox Desktop application.
- Enhanced support on `windows_marketplace`.
- Added service duration per type on `skype`, `tango` and `viber`.
- New organization of the `ftp` attributes.
- Enhanced structure of the `protocols.xml` file included in the Protobook archive (protocol `hr` tag structure updates).

26.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-26 and higher (for ixe 4.15.x versions), ixEngine 4.16.2-20 and higher (for ixe 4.16.x versions) and 4.17.0-20 and higher versions of ixEngine.

26.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

  ```
  gcc user_application.c -L. -lqmengine -lqmprotocols -o application
  ```

- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example:

  ```
  gcc user_application.c -L. -lqmengine -o application
  ```

Note:

Don’t forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

26.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

26.2. Protocol updates

26.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 52. New protocols added in this version

Proto ID	Protocol	Description
1688	apple_airplay	Apple airplay is a protocol for display picture and video to a connected tv from a device connected to the same private network
1689	apple_airprint	Apple Airprint is a network printing feature for Apple systems. It's based on the Dns Service Discovery protocol and IPP(needs URF format support).
1686	ip_exp_1	The IP_EXP_1 protocol (IANA Internet Protocol Number 253) is found over the IP layer (IANA protocol number: 253).
1687	ip_exp_2	The IP_EXP_2 protocol (IANA Internet Protocol Number 254) is found over the IP layer (IANA protocol number: 254).
1576	unassigned_ip_prot_143	The UNASSIGNED_IP_PROT_143 protocol (IANA Unassigned Internet Protocol Number 143) is found over the IP layer (IANA protocol number: 143).
1577	unassigned_ip_prot_144	The UNASSIGNED_IP_PROT_144 protocol (IANA Unassigned Internet Protocol Number 144) is found over the IP layer (IANA protocol number: 144).
1578	unassigned_ip_prot_145	The UNASSIGNED_IP_PROT_145 protocol (IANA Unassigned Internet Protocol Number 145) is found over the IP layer (IANA protocol number: 145).
1579	unassigned_ip_prot_146	The UNASSIGNED_IP_PROT_146 protocol (IANA Unassigned Internet Protocol Number 146) is found over the IP layer (IANA protocol number: 146).
1580	unassigned_ip_prot_147	The UNASSIGNED_IP_PROT_147 protocol (IANA Unassigned Internet Protocol Number 147) is found over the IP layer (IANA protocol number: 147).
1581	unassigned_ip_prot_148	The UNASSIGNED_IP_PROT_148 protocol (IANA Unassigned Internet Protocol Number 148) is found over the IP layer (IANA protocol number: 148).
1582	unassigned_ip_prot_149	The UNASSIGNED_IP_PROT_149 protocol (IANA Unassigned Internet Protocol Number 149) is found over the IP layer (IANA protocol number: 149).
1583	unassigned_ip_prot_150	The UNASSIGNED_IP_PROT_150 protocol (IANA Unassigned Internet Protocol Number 150) is found over the IP layer (IANA protocol number: 150).
1584	unassigned_ip_prot_151	The UNASSIGNED_IP_PROT_151 protocol (IANA Unassigned Internet Protocol Number 151) is found over the IP layer (IANA protocol number: 151).
1585	unassigned_ip_prot_152	The UNASSIGNED_IP_PROT_152 protocol (IANA Unassigned Internet Protocol Number 152) is found over the IP layer (IANA protocol number: 152).

Proto ID	Protocol	Description
1586	unassigned_ip_prot_153	The UNASSIGNED_IP_PROT_153 protocol (IANA Unassigned Internet Protocol Number 153) is found over the IP layer (IANA protocol number: 153).
1587	unassigned_ip_prot_154	The UNASSIGNED_IP_PROT_154 protocol (IANA Unassigned Internet Protocol Number 154) is found over the IP layer (IANA protocol number: 154).
1588	unassigned_ip_prot_155	The UNASSIGNED_IP_PROT_155 protocol (IANA Unassigned Internet Protocol Number 155) is found over the IP layer (IANA protocol number: 155).
1589	unassigned_ip_prot_156	The UNASSIGNED_IP_PROT_156 protocol (IANA Unassigned Internet Protocol Number 156) is found over the IP layer (IANA protocol number: 156).
1590	unassigned_ip_prot_157	The UNASSIGNED_IP_PROT_157 protocol (IANA Unassigned Internet Protocol Number 157) is found over the IP layer (IANA protocol number: 157).
1591	unassigned_ip_prot_158	The UNASSIGNED_IP_PROT_158 protocol (IANA Unassigned Internet Protocol Number 158) is found over the IP layer (IANA protocol number: 158).
1592	unassigned_ip_prot_159	The UNASSIGNED_IP_PROT_159 protocol (IANA Unassigned Internet Protocol Number 159) is found over the IP layer (IANA protocol number: 159).
1593	unassigned_ip_prot_160	The UNASSIGNED_IP_PROT_160 protocol (IANA Unassigned Internet Protocol Number 160) is found over the IP layer (IANA protocol number: 160).
1594	unassigned_ip_prot_161	The UNASSIGNED_IP_PROT_161 protocol (IANA Unassigned Internet Protocol Number 161) is found over the IP layer (IANA protocol number: 161).
1595	unassigned_ip_prot_162	The UNASSIGNED_IP_PROT_162 protocol (IANA Unassigned Internet Protocol Number 162) is found over the IP layer (IANA protocol number: 162).
1596	unassigned_ip_prot_163	The UNASSIGNED_IP_PROT_163 protocol (IANA Unassigned Internet Protocol Number 163) is found over the IP layer (IANA protocol number: 163).
1597	unassigned_ip_prot_164	The UNASSIGNED_IP_PROT_164 protocol (IANA Unassigned Internet Protocol Number 164) is found over the IP layer (IANA protocol number: 164).
1598	unassigned_ip_prot_165	The UNASSIGNED_IP_PROT_165 protocol (IANA Unassigned Internet Protocol Number 165) is found over the IP layer (IANA protocol number: 165).
1599	unassigned_ip_prot_166	The UNASSIGNED_IP_PROT_166 protocol (IANA Unassigned Internet Protocol Number 166) is found over the IP layer (IANA protocol number: 166).
1600	unassigned_ip_prot_167	The UNASSIGNED_IP_PROT_167 protocol (IANA Unassigned Internet Protocol Number 167) is found over the IP layer (IANA protocol number: 167).
1601	unassigned_ip_prot_168	The UNASSIGNED_IP_PROT_168 protocol (IANA Unassigned Internet Protocol Number 168) is found over the IP layer (IANA protocol number: 168).
1602	unassigned_ip_prot_169	The UNASSIGNED_IP_PROT_169 protocol (IANA Unassigned Internet Protocol Number 169) is found over the IP layer (IANA protocol number: 169).

Proto ID	Protocol	Description
1603	unassigned_ip_prot_170	The UNASSIGNED_IP_PROT_170 protocol (IANA Unassigned Internet Protocol Number 170) is found over the IP layer (IANA protocol number: 170).
1604	unassigned_ip_prot_171	The UNASSIGNED_IP_PROT_171 protocol (IANA Unassigned Internet Protocol Number 171) is found over the IP layer (IANA protocol number: 171).
1605	unassigned_ip_prot_172	The UNASSIGNED_IP_PROT_172 protocol (IANA Unassigned Internet Protocol Number 172) is found over the IP layer (IANA protocol number: 172).
1606	unassigned_ip_prot_173	The UNASSIGNED_IP_PROT_173 protocol (IANA Unassigned Internet Protocol Number 173) is found over the IP layer (IANA protocol number: 173).
1607	unassigned_ip_prot_174	The UNASSIGNED_IP_PROT_174 protocol (IANA Unassigned Internet Protocol Number 174) is found over the IP layer (IANA protocol number: 174).
1608	unassigned_ip_prot_175	The UNASSIGNED_IP_PROT_175 protocol (IANA Unassigned Internet Protocol Number 175) is found over the IP layer (IANA protocol number: 175).
1609	unassigned_ip_prot_176	The UNASSIGNED_IP_PROT_176 protocol (IANA Unassigned Internet Protocol Number 176) is found over the IP layer (IANA protocol number: 176).
1610	unassigned_ip_prot_177	The UNASSIGNED_IP_PROT_177 protocol (IANA Unassigned Internet Protocol Number 177) is found over the IP layer (IANA protocol number: 177).
1611	unassigned_ip_prot_178	The UNASSIGNED_IP_PROT_178 protocol (IANA Unassigned Internet Protocol Number 178) is found over the IP layer (IANA protocol number: 178).
1612	unassigned_ip_prot_179	The UNASSIGNED_IP_PROT_179 protocol (IANA Unassigned Internet Protocol Number 179) is found over the IP layer (IANA protocol number: 179).
1613	unassigned_ip_prot_180	The UNASSIGNED_IP_PROT_180 protocol (IANA Unassigned Internet Protocol Number 180) is found over the IP layer (IANA protocol number: 180).
1614	unassigned_ip_prot_181	The UNASSIGNED_IP_PROT_181 protocol (IANA Unassigned Internet Protocol Number 181) is found over the IP layer (IANA protocol number: 181).
1615	unassigned_ip_prot_182	The UNASSIGNED_IP_PROT_182 protocol (IANA Unassigned Internet Protocol Number 182) is found over the IP layer (IANA protocol number: 182).
1616	unassigned_ip_prot_183	The UNASSIGNED_IP_PROT_183 protocol (IANA Unassigned Internet Protocol Number 183) is found over the IP layer (IANA protocol number: 183).
1617	unassigned_ip_prot_184	The UNASSIGNED_IP_PROT_184 protocol (IANA Unassigned Internet Protocol Number 184) is found over the IP layer (IANA protocol number: 184).
1618	unassigned_ip_prot_185	The UNASSIGNED_IP_PROT_185 protocol (IANA Unassigned Internet Protocol Number 185) is found over the IP layer (IANA protocol number: 185).
1619	unassigned_ip_prot_186	The UNASSIGNED_IP_PROT_186 protocol (IANA Unassigned Internet Protocol Number 186) is found over the IP layer (IANA protocol number: 186).

Proto ID	Protocol	Description
1620	unassigned_ip_prot_187	The UNASSIGNED_IP_PROT_187 protocol (IANA Unassigned Internet Protocol Number 187) is found over the IP layer (IANA protocol number: 187).
1621	unassigned_ip_prot_188	The UNASSIGNED_IP_PROT_188 protocol (IANA Unassigned Internet Protocol Number 188) is found over the IP layer (IANA protocol number: 188).
1622	unassigned_ip_prot_189	The UNASSIGNED_IP_PROT_189 protocol (IANA Unassigned Internet Protocol Number 189) is found over the IP layer (IANA protocol number: 189).
1623	unassigned_ip_prot_190	The UNASSIGNED_IP_PROT_190 protocol (IANA Unassigned Internet Protocol Number 190) is found over the IP layer (IANA protocol number: 190).
1624	unassigned_ip_prot_191	The UNASSIGNED_IP_PROT_191 protocol (IANA Unassigned Internet Protocol Number 191) is found over the IP layer (IANA protocol number: 191).
1625	unassigned_ip_prot_192	The UNASSIGNED_IP_PROT_192 protocol (IANA Unassigned Internet Protocol Number 192) is found over the IP layer (IANA protocol number: 192).
1626	unassigned_ip_prot_193	The UNASSIGNED_IP_PROT_193 protocol (IANA Unassigned Internet Protocol Number 193) is found over the IP layer (IANA protocol number: 193).
1627	unassigned_ip_prot_194	The UNASSIGNED_IP_PROT_194 protocol (IANA Unassigned Internet Protocol Number 194) is found over the IP layer (IANA protocol number: 194).
1628	unassigned_ip_prot_195	The UNASSIGNED_IP_PROT_195 protocol (IANA Unassigned Internet Protocol Number 195) is found over the IP layer (IANA protocol number: 195).
1629	unassigned_ip_prot_196	The UNASSIGNED_IP_PROT_196 protocol (IANA Unassigned Internet Protocol Number 196) is found over the IP layer (IANA protocol number: 196).
1630	unassigned_ip_prot_197	The UNASSIGNED_IP_PROT_197 protocol (IANA Unassigned Internet Protocol Number 197) is found over the IP layer (IANA protocol number: 197).
1631	unassigned_ip_prot_198	The UNASSIGNED_IP_PROT_198 protocol (IANA Unassigned Internet Protocol Number 198) is found over the IP layer (IANA protocol number: 198).
1632	unassigned_ip_prot_199	The UNASSIGNED_IP_PROT_199 protocol (IANA Unassigned Internet Protocol Number 199) is found over the IP layer (IANA protocol number: 199).
1633	unassigned_ip_prot_200	The UNASSIGNED_IP_PROT_200 protocol (IANA Unassigned Internet Protocol Number 200) is found over the IP layer (IANA protocol number: 200).
1634	unassigned_ip_prot_201	The UNASSIGNED_IP_PROT_201 protocol (IANA Unassigned Internet Protocol Number 201) is found over the IP layer (IANA protocol number: 201).
1635	unassigned_ip_prot_202	The UNASSIGNED_IP_PROT_202 protocol (IANA Unassigned Internet Protocol Number 202) is found over the IP layer (IANA protocol number: 202).
1636	unassigned_ip_prot_203	The UNASSIGNED_IP_PROT_203 protocol (IANA Unassigned Internet Protocol Number 203) is found over the IP layer (IANA protocol number: 203).

Proto ID	Protocol	Description
1637	unassigned_ip_prot_204	The UNASSIGNED_IP_PROT_204 protocol (IANA Unassigned Internet Protocol Number 204) is found over the IP layer (IANA protocol number: 204).
1638	unassigned_ip_prot_205	The UNASSIGNED_IP_PROT_205 protocol (IANA Unassigned Internet Protocol Number 205) is found over the IP layer (IANA protocol number: 205).
1639	unassigned_ip_prot_206	The UNASSIGNED_IP_PROT_206 protocol (IANA Unassigned Internet Protocol Number 206) is found over the IP layer (IANA protocol number: 206).
1640	unassigned_ip_prot_207	The UNASSIGNED_IP_PROT_207 protocol (IANA Unassigned Internet Protocol Number 207) is found over the IP layer (IANA protocol number: 207).
1641	unassigned_ip_prot_208	The UNASSIGNED_IP_PROT_208 protocol (IANA Unassigned Internet Protocol Number 208) is found over the IP layer (IANA protocol number: 208).
1642	unassigned_ip_prot_209	The UNASSIGNED_IP_PROT_209 protocol (IANA Unassigned Internet Protocol Number 209) is found over the IP layer (IANA protocol number: 209).
1643	unassigned_ip_prot_210	The UNASSIGNED_IP_PROT_210 protocol (IANA Unassigned Internet Protocol Number 210) is found over the IP layer (IANA protocol number: 210).
1644	unassigned_ip_prot_211	The UNASSIGNED_IP_PROT_211 protocol (IANA Unassigned Internet Protocol Number 211) is found over the IP layer (IANA protocol number: 211).
1645	unassigned_ip_prot_212	The UNASSIGNED_IP_PROT_212 protocol (IANA Unassigned Internet Protocol Number 212) is found over the IP layer (IANA protocol number: 212).
1646	unassigned_ip_prot_213	The UNASSIGNED_IP_PROT_213 protocol (IANA Unassigned Internet Protocol Number 213) is found over the IP layer (IANA protocol number: 213).
1647	unassigned_ip_prot_214	The UNASSIGNED_IP_PROT_214 protocol (IANA Unassigned Internet Protocol Number 214) is found over the IP layer (IANA protocol number: 214).
1648	unassigned_ip_prot_215	The UNASSIGNED_IP_PROT_215 protocol (IANA Unassigned Internet Protocol Number 215) is found over the IP layer (IANA protocol number: 215).
1649	unassigned_ip_prot_216	The UNASSIGNED_IP_PROT_216 protocol (IANA Unassigned Internet Protocol Number 216) is found over the IP layer (IANA protocol number: 216).
1650	unassigned_ip_prot_217	The UNASSIGNED_IP_PROT_217 protocol (IANA Unassigned Internet Protocol Number 217) is found over the IP layer (IANA protocol number: 217).
1651	unassigned_ip_prot_218	The UNASSIGNED_IP_PROT_218 protocol (IANA Unassigned Internet Protocol Number 218) is found over the IP layer (IANA protocol number: 218).
1652	unassigned_ip_prot_219	The UNASSIGNED_IP_PROT_219 protocol (IANA Unassigned Internet Protocol Number 219) is found over the IP layer (IANA protocol number: 219).
1653	unassigned_ip_prot_220	The UNASSIGNED_IP_PROT_220 protocol (IANA Unassigned Internet Protocol Number 220) is found over the IP layer (IANA protocol number: 220).

Proto ID	Protocol	Description
1654	unassigned_ip_prot_221	The UNASSIGNED_IP_PROT_221 protocol (IANA Unassigned Internet Protocol Number 221) is found over the IP layer (IANA protocol number: 221).
1655	unassigned_ip_prot_222	The UNASSIGNED_IP_PROT_222 protocol (IANA Unassigned Internet Protocol Number 222) is found over the IP layer (IANA protocol number: 222).
1656	unassigned_ip_prot_223	The UNASSIGNED_IP_PROT_223 protocol (IANA Unassigned Internet Protocol Number 223) is found over the IP layer (IANA protocol number: 223).
1657	unassigned_ip_prot_224	The UNASSIGNED_IP_PROT_224 protocol (IANA Unassigned Internet Protocol Number 224) is found over the IP layer (IANA protocol number: 224).
1658	unassigned_ip_prot_225	The UNASSIGNED_IP_PROT_225 protocol (IANA Unassigned Internet Protocol Number 225) is found over the IP layer (IANA protocol number: 225).
1659	unassigned_ip_prot_226	The UNASSIGNED_IP_PROT_226 protocol (IANA Unassigned Internet Protocol Number 226) is found over the IP layer (IANA protocol number: 226).
1660	unassigned_ip_prot_227	The UNASSIGNED_IP_PROT_227 protocol (IANA Unassigned Internet Protocol Number 227) is found over the IP layer (IANA protocol number: 227).
1661	unassigned_ip_prot_228	The UNASSIGNED_IP_PROT_228 protocol (IANA Unassigned Internet Protocol Number 228) is found over the IP layer (IANA protocol number: 228).
1662	unassigned_ip_prot_229	The UNASSIGNED_IP_PROT_229 protocol (IANA Unassigned Internet Protocol Number 229) is found over the IP layer (IANA protocol number: 229).
1663	unassigned_ip_prot_230	The UNASSIGNED_IP_PROT_230 protocol (IANA Unassigned Internet Protocol Number 230) is found over the IP layer (IANA protocol number: 230).
1664	unassigned_ip_prot_231	The UNASSIGNED_IP_PROT_231 protocol (IANA Unassigned Internet Protocol Number 231) is found over the IP layer (IANA protocol number: 231).
1665	unassigned_ip_prot_232	The UNASSIGNED_IP_PROT_232 protocol (IANA Unassigned Internet Protocol Number 232) is found over the IP layer (IANA protocol number: 232).
1666	unassigned_ip_prot_233	The UNASSIGNED_IP_PROT_233 protocol (IANA Unassigned Internet Protocol Number 233) is found over the IP layer (IANA protocol number: 233).
1667	unassigned_ip_prot_234	The UNASSIGNED_IP_PROT_234 protocol (IANA Unassigned Internet Protocol Number 234) is found over the IP layer (IANA protocol number: 234).
1668	unassigned_ip_prot_235	The UNASSIGNED_IP_PROT_235 protocol (IANA Unassigned Internet Protocol Number 235) is found over the IP layer (IANA protocol number: 235).
1669	unassigned_ip_prot_236	The UNASSIGNED_IP_PROT_236 protocol (IANA Unassigned Internet Protocol Number 236) is found over the IP layer (IANA protocol number: 236).
1670	unassigned_ip_prot_237	The UNASSIGNED_IP_PROT_237 protocol (IANA Unassigned Internet Protocol Number 237) is found over the IP layer (IANA protocol number: 237).

Proto ID	Protocol	Description
1671	unassigned_ip_prot_238	The UNASSIGNED_IP_PROT_238 protocol (IANA Unassigned Internet Protocol Number 238) is found over the IP layer (IANA protocol number: 238).
1672	unassigned_ip_prot_239	The UNASSIGNED_IP_PROT_239 protocol (IANA Unassigned Internet Protocol Number 239) is found over the IP layer (IANA protocol number: 239).
1673	unassigned_ip_prot_240	The UNASSIGNED_IP_PROT_240 protocol (IANA Unassigned Internet Protocol Number 240) is found over the IP layer (IANA protocol number: 240).
1674	unassigned_ip_prot_241	The UNASSIGNED_IP_PROT_241 protocol (IANA Unassigned Internet Protocol Number 241) is found over the IP layer (IANA protocol number: 241).
1675	unassigned_ip_prot_242	The UNASSIGNED_IP_PROT_242 protocol (IANA Unassigned Internet Protocol Number 242) is found over the IP layer (IANA protocol number: 242).
1676	unassigned_ip_prot_243	The UNASSIGNED_IP_PROT_243 protocol (IANA Unassigned Internet Protocol Number 243) is found over the IP layer (IANA protocol number: 243).
1677	unassigned_ip_prot_244	The UNASSIGNED_IP_PROT_244 protocol (IANA Unassigned Internet Protocol Number 244) is found over the IP layer (IANA protocol number: 244).
1678	unassigned_ip_prot_245	The UNASSIGNED_IP_PROT_245 protocol (IANA Unassigned Internet Protocol Number 245) is found over the IP layer (IANA protocol number: 245).
1679	unassigned_ip_prot_246	The UNASSIGNED_IP_PROT_246 protocol (IANA Unassigned Internet Protocol Number 246) is found over the IP layer (IANA protocol number: 246).
1680	unassigned_ip_prot_247	The UNASSIGNED_IP_PROT_247 protocol (IANA Unassigned Internet Protocol Number 247) is found over the IP layer (IANA protocol number: 247).
1681	unassigned_ip_prot_248	The UNASSIGNED_IP_PROT_248 protocol (IANA Unassigned Internet Protocol Number 248) is found over the IP layer (IANA protocol number: 248).
1682	unassigned_ip_prot_249	The UNASSIGNED_IP_PROT_249 protocol (IANA Unassigned Internet Protocol Number 249) is found over the IP layer (IANA protocol number: 249).
1683	unassigned_ip_prot_250	The UNASSIGNED_IP_PROT_250 protocol (IANA Unassigned Internet Protocol Number 250) is found over the IP layer (IANA protocol number: 250).
1684	unassigned_ip_prot_251	The UNASSIGNED_IP_PROT_251 protocol (IANA Unassigned Internet Protocol Number 251) is found over the IP layer (IANA protocol number: 251).
1685	unassigned_ip_prot_252	The UNASSIGNED_IP_PROT_252 protocol (IANA Unassigned Internet Protocol Number 252) is found over the IP layer (IANA protocol number: 252).
1690	abc	ABC is a Bittorrent client based on BitTornado
1691	ants_p2p	Ants is a distributed P2P client.
1799	apple_hls	Apple implementation of the HTTP Live Streaming IETF draft. Used on Apple iOS devices.
1692	bitcoin	Bitcoint is a distributed payment system.
1573	vuze	Vuze is a BitTorrent client.

Proto ID	Protocol	Description
1693	filesovermiles	Filesovermiles is a p2p written in Flash which is meant to be executed from a browser page (blocking use case is supported but flow classification is limited to web).
1699	jxta	Open source peer-to-peer protocol launched by Sun Microsystems.
1694	lanshark	Lanshark is a p2p client for LAN.
1698	luke	Luke is a P2P portal and software.
1696	stealthnet	Stealthnet is a file sharing application between two or more hosts.
1697	vsee	Vsee is a videoconferencing software
1575	skydrive_login	On-line file storage service owned by Microsoft.
1574	xboxlive_marketplace	Xbox Live Marketplace is a service where users can purchase and download games and multimedia.

26.2.2. Deprecated protocols in this version

Table 53. Deprecated protocols in this version

Proto ID	Protocol	Description	Comments
248	doubleclick_ads	DoubleClick is a subsidiary of Google which develops and provides Internet ad serving services.	This protocol has been replaced by `google_ads`.
628	ip_exp	The IP_EXP protocols (IANA Internet Protocol) are found over the IP layer (IANA protocol).	It has been replaced by `ip_exp_1` and `ip_exp_2`.
693	unassigned_ip_prot	The UNASSIGNED_IP_PROT protocol (IANA Unassigned Internet Protocol) is found over the IP layer (IANA protocol).	It has been replaced by unassigned_ip_prot_xxxx protocols corresponding to IANA number 143 to 252.
278	pando	pando is a peer-to-peer protocol.	Pando servers have been definitely shut down in August 2013.

26.3. Attributes

This section describes the attribute updates.

26.3.1. New event attributes added in this version

The following event attributes have been added in this version.

26.3.1.1. Generic events added in this version

There are no generic events added in this version.

26.3.1.2. Events added in this version

Table 54. Added event attributes

Protocol	New event attributes
base	multi_match_proto_id
ftp	index
line	service
line	service_id
skype	service_duration
smb	end_of_file
smb	version
tango	service_duration
tcp	stream
tns	response
tns	response_size
tns	response_time
udp	stream
viber	service_duration
windows_marketplace	application_name

26.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 55. Deprecated event attributes

Protocol	Deprecated event attributes	Comments
doubleclick_ads	ad_client	doubleclick_ads is now deprecated.
doubleclick_ads	ad_page	doubleclick_ads is now deprecated.
doubleclick_ads	ad_url	doubleclick_ads is now deprecated.
doubleclick_ads	doubleclick_ad	doubleclick_ads is now deprecated.
doubleclick_ads	end	doubleclick_ads is now deprecated.

26.3.3. Event attributes modified in this version

There's no modified event in this version.

26.4. Bug fixed and known issues

26.4.1. Bugs fixed in this version

- RTC#286 - **[isup] Extraction issue on call_duration**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	x86 XLR
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Different values for call_duration are raised between 32 and 64 bits for X86 and XLR platforms.

- SF#6518 - RTC#387 - **[SF6518] [stun] performance issue**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Performance Anomaly
Expected versus actual behavior	Performance regression for STUN sessions.

- RTC#392 - **[ymail2] Regression on content extraction**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	ymail2:content is extracted in several parts.

- RTC#2557 - **[rtp] Extraction issue on header_len**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	On some specific traces with RTP traffic, the header_len of each RTP packet is 0.

- RTC#2934 - **[hot swap] dpi_bundle fails hotswapping**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Memory Leak
Expected versus actual behavior	Hot-swap usage error can cause memory leak.

- RTC#3006 - **[ymail2] classification issue**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Missing classification in "mail.yahoo.co.uk" and over ssl support.

- SF#6802 - RTC#3017 - **[Line] callee attribute not extracted**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Extraction fails for callee attribute based on json in LINE packets.

- RTC#3198 - **[http] classification must be improved with unidirectional traffic**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	In specific cases, we can enhance the classification of the traffic upper HTTP in unidirectional mode (example: netflix).

- RTC#3478 - **[H225] event(h225,caller) on root parent whereas 'end' attribute is already extracted**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	

- SF#6662 - RTC#3488 - **[sf6662][share] Classification must be improved**

Bug Info	Description
Reported against	PB 1.17.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Some flow classified as unknown should be classified as share.

- RTC#3707 - **[ymail_mobile_new] extraction issue for attach_content**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	attach_content events of a unique mail attachment are linked to several parent attributes "attach".

- RTC#3818 - **[sina_news] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	sina_news is sometimes classified as sina_video on specific traces.

- RTC#3827 - **[twitter] Classification issues**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	twitter is sometimes classified as twitter_update on specific traces.

- SF#7032 - RTC#4038 - **[SF7032][ipsec] classification must be enhanced**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Misclassification of the traffic as ipsec.

- RTC#4084 - **[smb] the attribute "information_level" is not extracted in smb:information_level**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	In some cases, the attribute smb:information_level is not extracted.

- SF#4507 - RTC#4099 - **[SF4507] [tcp] Duplicated RST packets not dropped by the reassembly**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	Duplicated RST packets should be dropped when TCP reassembly is enabled.

- SF#6994 - RTC#4179 - **[yahoo_maps] attributes not extracted**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All

Bug Info	Description
Effect of bug	Extraction Anomaly
Expected versus actual behavior	The extraction must be improved for specific data flow structure.

- SF#7047 - RTC#4363 - **[SMB] smb:content not always extracted**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	The attribute smb:content is not extracted for specific write smb commands.

- RTC#4559 - **[archive] fix login and password attributes**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	x86
Effect of bug	Extraction Anomaly
Expected versus actual behavior	On specific cases, the login and password are not extracted.

- SF#6998 - RTC#4629 - **[netbios]: Unexpected extraction of netbios:caller**

Bug Info	Description
Reported against	PB 1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Extraction anomaly: caller value should not be extracted on specific cases.

- RTC#4704 - **[sip] extraction issue of the attributes media_attr_addr and media_attr_addr_v6**

Bug Info	Description
Reported against	ProtocolBundle-1.22.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	The attributes media_attr_addr and media_attr_addr_v6 are not extracted from traffic including SDP information.

26.4.2. Known issues

There's no known issues raised in this version.

27. Protocol Bundle 1.21.0

27.1. What's new in the Protocol Bundle 1.21.0

27.1.1. Note about the major enhancements of the release

99 new protocols added: 45 Bittorrent tracker search engines, famous websites as HSBC, Paypal, BBC or AVG. See Section 27.2, “Protocol updates”

27.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-26 and higher (for ixe 4.15.x versions), ixEngine 4.16.2-20 and higher (for ixe 4.16.x versions) and 4.17.0-20 and higher versions of ixEngine.

27.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

  ```
  gcc user_application.c -L. -lqmengine -lqmprotocols -o application
  ```

- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example:

  ```
  gcc user_application.c -L. -lqmengine -o application
  ```

Note:

Don’t forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

27.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x

- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

27.2. Protocol updates

27.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 56. New protocols added in this version

Proto ID	Protocol	Description
1700	1337x	Bittorrent tracker search engine
1782	adcash	Adcash is an international Ad network providing Internet publishers
1794	adserverplus	Online advertisement
1702	animebw	Bittorrent tracker search engine
1751	anz	Offers home, car, and business loans, as well as internet banking, and insurance.
1703	asiandvdclub	Bittorrent tracker search engine
1755	avg	Antivirus and security software products for home and business users.
1766	babylon	Babylon is a leading global provider of language and search solutions
1754	bbc	The BBC Homepage providing News and Broadcast
1704	bemaniso	Bittorrent tracker search engine
1705	bitenova	Bittorrent tracker search engine
1706	bithq	Bittorrent tracker search engine
1707	bitme	Bittorrent tracker search engine
1708	bitmetv	Bittorrent tracker search engine
1709	bitseduce	Bittorrent tracker search engine
1710	bitshock	Bittorrent tracker search engine
1711	bitsoup	Bittorrent tracker search engine
1712	bitvaulttorrent	Bittorrent tracker search engine
1701	bitworld	Bittorrent tracker search engine
1796	blogfa	Persian Blog Hosting
1713	bootytape	Bittorrent tracker search engine
1714	browntracker	Bittorrent tracker search engine
1715	bt_chat	Bittorrent tracker search engine
1717	btjunkie	Bittorrent tracker search engine
1716	bt_wrzru	Bittorrent tracker search engine
1718	central_torrent	Bittorrent tracker search engine
1719	cinemageddon	Bittorrent tracker search engine
1757	commentcamarche	CommentCaMarche.net is a french website providing technical explanations as well as forums.
1720	crazysaloon	Bittorrent tracker search engine
1721	cuteyhoneyflash	Bittorrent tracker search engine
1722	cyber12	Bittorrent tracker search engine
1723	danishbits	Bittorrent tracker search engine
1724	deepseek	Bittorrent tracker search engine
1784	delfi	Estonian news portal

Proto ID	Protocol	Description
1765	delta_search	Browser toolbar search engine
1776	directrev	DirectREV Media Delivery Platform is a real-time digital ad marketplace that connects publishers with agencies, ad networks and third-party technology providers.
1725	dreamora	Bittorrent tracker search engine
1761	elpais	Spanish news web portal
1783	encuentra24	Official Panama Classifieds Portal. Publish ads for rent or sale real estate, or jobs, cars, pet
1726	energy_torrent	Bittorrent tracker search engine
1773	espncricinfo	International cricket news, live scores, photos, columns and player profiles.
1727	extremebits	Bittorrent tracker search engine
1728	extremenova	Bittorrent tracker search engine
1729	fenopy	Bittorrent tracker search engine
1730	freeloader	Bittorrent tracker search engine
1731	freetorrent	Bittorrent tracker search engine
1780	goal	New media company that provides soccer news and entertainment
1798	gumtree	Gumtree is the first site for free classifieds ads in the UK; for buying and selling items, cars, properties, and find or offer jobs.
1795	heureka	Czech e-commerce website
1750	hsbc	HSBC banking website
1781	ilivid	Browser toolbar search engine and video player
1744	iminent	Website providing add-ons for most messengers
1797	jfranews	New portal popular in Jordan and Palestinian Territory
1752	kapook	Thailandese web portal
1732	kingdomxxx	Bittorrent tracker search engine
1769	kooora	Arabic sports news portal
1746	labanquepostale	French bank offering insurance an banking services
1764	marca	Spanish sports news portal
1770	mercadolibre	MercadoLibre is a technology company that provides e-commerce solutions
1787	morefreecamsecrets	Adult live webcam site
1767	neobux	NeoBux excels in providing new business solutions as a Paid-to-Click service
1778	news_am	Armenian news portal
1779	nordea	Danish online banking and investment web portal
1772	olx	Free classified ads website
1789	opensooq	Market place framework aimed to Arab countries
1753	orange	French operators website providing internet and telephone servics as well as web and media portal services.
1775	panet	News and entertainment web portal
1747	paypal	Online payment services
1745	pole_emploi	French website for job seekers.

Proto ID	Protocol	Description
1733	qtrax	Bittorrent tracker search engine
1734	raulken	Bittorrent tracker search engine
1735	rayfile	Bittorrent tracker search engine
1736	rmvbusters	Bittorrent tracker search engine
1749	rutracker	Bittorrent tracker search engine
1762	sanook	Thailandese website providing lottery games, music. chat, news, jobs, shopping and entertainment.
1788	sapo	Mozambican web partal including mail, news, lifestyle
1737	scenehd	Bittorrent tracker search engine
1774	searchnu	Browser toolbar search engine
1738	sharebox	Bittorrent tracker search engine
1739	sharereactor	Bittorrent tracker search engine
1786	slando	Belarusian free classified ads
1756	softonic	Softonic.com is a software download portal based in Barcelona
1790	startimes	Arabic forum hosting site
1777	swedbank	Estonian online banking and investment web portal
1740	swepiracy	Bittorrent tracker search engine
1741	tamilthunder_com	Bittorrent tracker search engine
1760	telegraaf	Dutch news web portal
1785	telegraf	Serbian web portal
1791	to_mati	Greek web portal
1763	t_online	T-Online Deutch ISP web portal
1792	tv2	Danish news portal
1759	ucoz	uCoz is a free web hosting with a built-in content management system.
1742	usabit_com	Bittorrent tracker search engine
1743	vector	Bittorrent tracker search engine
1768	vube	Monthly video contest and video sharing website.
1793	weather2umbrella	World Weather Forecast
1748	westpac	Australia s First Bank with a range of innovative financial packages
1758	y8	Y8.com has Free Online Mini Games in both Flash and Shockwave
1771	yieldmanager	Yield Manager is an advertising delivery technology operated by Right Media. Since 2007, this has operated as a subsidiary of Yahoo.

27.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

27.3. Attributes

This section describes the attribute updates.

27.3.1. New event attributes added in this version

The following event attributes have been added in this version.

27.3.1.1. Generic events added in this version

There are no generic events added in this version.

27.3.1.2. Events added in this version

There's no new attribute in this release.

27.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this release.

27.3.3. Event attributes modified in this version

There's no modified attribute in this version.

27.4. Bug fixed and known issues

27.4.1. Bugs fixed in this version

There's no bug fixed in this release.

27.4.2. Known issues

There's no known issue raised in this release.

28. Protocol Bundle 1.20.0

28.1. What's new in the Protocol Bundle 1.20.0

28.1.1. Note about the major enhancements of the release

- 12 new Protocols added. See Section 28.2, “Protocol updates”
- 40 new Event Attributes added. See Section 28.3, “Attributes”
- Added decompression support in Jabber.
- Added new protocol high_entropy over Unknown. Unknown flows that are encrypted or compressed will be classified as high_entropy as a last resort. Requires ixEngine 4.18 or higher.
- Added the following popular Asian protocols: touch, mypeople_messenger, chat_on, saavn_music, magumagu, line_wind_runner, maaii. Also improved classification of Kakaotalk to include Kakaostory.
- Improved ICAP request extraction.
- New mechanism for handling service-type attributes for: skype, tango, viber, wechat, and whatsapp (previously extracted within SPID process; now extracted using packet metrics).
- Added google_drive in documentation, as a reference to google_docs.
- Added classification of SSL over SOCKS4/5.

28.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-26 and higher (for ixe 4.15.x versions), ixEngine 4.16.2-20 and higher (for ixe 4.16.x versions) and 4.17.0-20 and higher versions of ixEngine.

28.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. For example:

  ```
  gcc user_application.c -L. -lqmengine -lqmprotocols -o application
  ```

- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example:

  ```
  gcc user_application.c -L. -lqmengine -o application
  ```

Note:

Don’t forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries will not be found by the dynamic linker.

28.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.7.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

28.2. Protocol updates

28.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 57. New protocols added in this version

Proto ID	Protocol	Description
1563	blackberry_update	This protocol classifies the Blackberry 10 family OS software updates.
1567	chat_on	chatON is a global mobile communication service introduced by Samsung Electronics.
1561	high_entropy	High Entropy is a virtual protocol used to detect potentially encrypted payloads. Important note: the classification of this layer is effective since the 4.18.0 version of the ixEngine framework. The classification is based on two methods: entropy value computation, and printable strings detection.
1572	line_games	This protocol plug-in classifies the http traffic to the host linegame.com, the portal of various Line games.
1570	line_wind_runner	Line Wind Runner is a popular asian mobile device game accessible from the Line application.
1564	lync	Microsoft Lync IM, VoIP and desktop sharing services (corporate and on-line services).
1571	maaii	Maaii is a cross-platform messaging application which allows iPhone and Android users to send and receive text messages and phone calls for free.
1566	magumagu	2013 for Kakao (aka Magu-Magu) is Korean baseball game, developped by CJ E&M corp.
1569	mypeople_messenger	MyPeople Messenger is a cross-platform application providing free text, picture, and video messaging.
1565	saavn_music	Saavn is a streaming application providing free Indian and Bollywood music to listeners.
1568	touch	Touch is a cross-platform application providing free text, picture, and video messaging.
1504	websocket	The WebSocket Protocol, as described in IETF RFC6455.

28.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

28.3. Attributes

This section describes the attribute updates.

28.3.1. New event attributes added in this version

The following event attributes have been added in this version.

28.3.1.1. Generic events added in this version

There are no generic events added in this version.

28.3.1.2. Events added in this version

Table 58. Added event attributes

Protocol	New event attributes
ares	peer_info
bittorrent	peer_info
directconnect	peer_info
edonkey	peer_info
ftp	command
gnutella	peer_info
high_entropy	entropy
http	post_variable_decoded
http	upgrade_header
http	uri_decoded
http	uri_get_decoded
http	uri_path_decoded
http	uri_post_decoded
icap	code_respmod_req
icap	content_type_respmod_req
icap	end
icap	host_respmod_req
icap	method_respmod_req
icap	referer_respmod_req
icap	request_respmod_req
icap	uri_respmod_req
icap	user_agent_respmod_req
icap	x_client_ip_respmod_req
line	caller
mute	peer_info
qq	call_duration
skype	service_id
tango	service
tango	service_id
viber	service

Protocol	New event attributes
viber	service_id
websocket	end
websocket	msg
websocket	opcode
websocket	raw
websocket	wsframe
wechat	service
wechat	service_id
whatsapp	service
whatsapp	service_id

28.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 59. Deprecated event attributes

Protocol	Deprecated event attributes	Comments
icap	x_client_ip	This attribute has been renamed to x_client_ip_respmod_req.
skype	end	The attribute was extracted within SPID process. The mechanisms has been updated to use packet metrics.
skype	nearest_service	The attribute was extracted within SPID process. The mechanisms has been updated to use packet metrics.
skype	service_divergence	The attribute was extracted within SPID process. The mechanisms has been updated to use packet metrics.
skype	service_type	The attribute was extracted within SPID process. The mechanisms has been updated to use packet metrics.

28.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 60. Event attributes modified

Protocol	Event attribute	Changes
ftp	content_type	in PB 1.19.0 [string,server,session_mod,no_parent] in PB 1.20.0 [string,server,session_mod,command]
ftp	data_port	in PB 1.19.0 [uint16,both,session_mod,no_parent] in PB 1.20.0 [uint16,both,session_mod,command]
ftp	filename	in PB 1.19.0 [string,both,session_mod,no_parent] in PB 1.20.0 [string,both,session_mod,command]
ftp	filesize	in PB 1.19.0 [uint32,server,session_mod,no_parent] in PB 1.20.0 [uint32,server,session_mod,command]
ftp	greeting_message	in PB 1.19.0 [string,server,session_fix,no_parent] in PB 1.20.0 [string,server,session_fix,command]
ftp	loadway	in PB 1.19.0 [string,both,session_mod,no_parent] in PB 1.20.0 [string,both,session_mod,command]
ftp	login	in PB 1.19.0 [string,client,session_fix,no_parent] in PB 1.20.0 [string,client,session_fix,command]
ftp	method	in PB 1.19.0 [string,client,session_mod,no_parent] in PB 1.20.0 [string,client,session_mod,command]
ftp	offset	in PB 1.19.0 [uint32,server,session_mod,no_parent] in PB 1.20.0 [uint32,server,session_mod,command]
ftp	password	in PB 1.19.0 [string,client,session_fix,no_parent] in PB 1.20.0 [string,client,session_fix,command]

Protocol	Event attribute	Changes
ftp	return_msg	in PB 1.19.0 [parent,server,session_mod,no_parent] in PB 1.20.0 [parent,server,session_mod,command]
ftp	transfer_duration	in PB 1.19.0 [timeval,both,session_fix,no_parent] in PB 1.20.0 [timeval,both,session_fix,command]
skype	service	in PB 1.19.0 [parent,both,session_mod,no_parent] in PB 1.20.0 [string,both,session_mod,no_parent]

28.4. Bug fixed and known issues

28.4.1. Bugs fixed in this version

- SF#5622 - RTC#294 - **[mailru] upload attachment missing**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	Mailru upload attachment extract may be missing in some workflows.

- SF#5817 - RTC#305 - **[ymail2] attachment with unknown size not handled correctly**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	Extraction problem : attachments with unknown size [ymail2].

- RTC#363 - **[rlp] fix classification conflict**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	RLP may be incorrectly classified.

- RTC#372 - **[qq] [qq_transfer] call attributes extraction over tcp**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Issue with call attributes extraction of QQ over TCP.

- RTC#377 - **[qq] classification issue**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	

- RTC#388 - **[itunes] classification improvement**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	Improve classification of Itunes.

- RTC#2229 - **[aim] Improve classification**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Classification improvement : AIM v8 over RTMP.

- SF#6546 - RTC#1844 - **[udp] Invalid checksum errors reported by udp.wrong_crc**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Other Anomaly
Expected versus actual behavior	UDP wrong_crc was sometimes incorrectly reported.

- RTC#1804 - **[http] Documentation update on the HTTP methods**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	Documentation update on the HTTP methods.

- RTC#1927 - **[foxy] remove udp from bottom layer's list**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Foxy was incorrectly classified over UDP.

- SF#6619 - RTC#2005 - **[SF6619] [niconico_douga] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Sessions containing overlay comments are not classified

- SF#6591 - RTC#2016 - **[SF6591] [netflow] add netflow v9 classification**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Add Netflow version 9 classification.

- RTC#2116 - **[tango] support new version**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Support latest Tango client as of July 2013.

- RTC#2135 - **[SF6676][ymail2] classification regression because of pdd**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Fix classification of Ymail2.

- SF#6674 - RTC#2187 - **[SF6674][gmail] msglist_sender_email is extracted with some extra characters**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Extraction Anomaly
Expected versus actual behavior	Extraction fix: Gmail msglist_sender_email is extracted with some extra characters.

- SF#6881 - RTC#2190 - **[netflix] add classification for mobile applications**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Add Netflix classification for mobile applications.

- RTC#2293 - **[rtp] classif vs inheritance, backport from p_1_15**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable

Bug Info	Description
Expected versus actual behavior	Classification fix: rtp classified as gtalk when inherited from jabber.gtalk.

- SF#6768 - RTC#2528 - **[SF6768][ymail2] attach_content extracted when no download occurs**

Bug Info	Description
Reported against	PB 1.17.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Extraction fix: could not extract Ymail2 attachment in some particular scenario.

- SF#5815 - RTC#2534 - **[SF6768][ymail2] attach_content extracted with extra "\r\n" at the end**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	Extraction bug in upload workflow : ymail2[attach_content]has extra "\r\n" at the end.

- SF#6629 - RTC#2539 - **[SF6629] [pandora] no classification over ssl**

Bug Info	Description
Reported against	PB 1.17.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	

- SF#6605 - RTC#2614 - **[SF6605][gtalk] Classification can be improved**

Bug Info	Description
Reported against	PB 1.17.0
Platform	x86 XLP AMP
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification improvement : Google Talk over jabber.

- SF#6215 - RTC#2623 - **[wechat] improve classification**

Bug Info	Description
Reported against	PB 1.17.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Improving classification of wechat workflows generated by the latest wechat client version 4.5.

- SF#5302 - RTC#2629 - **[viber] improve classification**

Bug Info	Description
Reported against	PB 1.17.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Improve viber classification.

- RTC#2635 - **[tango] improve classification**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Improve classification of Tango over UDP.

- SF#6770 - RTC#2969 - **[SF6770][rtp] wrong classification thus extraction**

Bug Info	Description
Reported against	PB 1.17.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	RTP special case : for protocols that diverge from RTP's RFC, risk of signature calculation corruption causing overflow error.

28.4.2. Known issues

- RTC#319 - **[mmse, wtp] missing classification**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	Classification issue : MMSE, WTP missing classif.
Workaround	No workaround

- RTC#392 - **[ymail2] Regression on content extraction**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	Extraction fix : stop splitting attribute data such as ymail2[content].
Workaround	No workaround

- RTC#2934 - **[hot swap split] Memory leak**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Not Applicable
Expected versus actual behavior	hot-swap usage error can cause memory leak.
Workaround	No workaround

- SF#6954 - RTC#3469 - **[SF6954] [stun] [rtp] - rtp over lync**

Bug Info	Description
Reported against	ProtocolBundle-1.20.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	RTP in Lync, special case : unable to classify (possibly because of variations between the bytesize of STUN's MessageIntegrity attribute and MS's Lync implementation).
Workaround	No workaround

29. Protocol Bundle 1.19.0

29.1. What's new in the Protocol Bundle 1.19.0

29.1.1. Note about the major enhancements of the release

29.1.1.1. New protocols, new attributes and updates

The protocol `itv_player` has been added in this release. It classifies flows from the online video on demand service itv.com and the proprietary iOS application ITV Player.

The following protocols have been updated:

- `FogCreek`
- `Funshion`
- `Gtalk`
- `MapQuest`
- `Indonetwork`
- `Netflix`
- `Orange webmail`
- `YouSendIt`

29.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-26 and higher (for ixe 4.15.x versions), ixEngine 4.16.2-20 and higher (for ixe 4.16.x versions) and 4.17.0-20 and higher versions of ixEngine.

29.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don’t forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn’t be found by the dynamic linker when your starts.

29.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

29.2. Protocol updates

29.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 61. New protocols added in this version

Proto ID	Protocol	Description
1562	itv_player	Proprietary iOS application and website for VOD content (TV catch up) and live channels streaming.

29.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

29.3. Attributes

This section describes the attribute updates.

29.3.1. New event attributes added in this version

No new event attributes added in this version.

29.3.2. Deprecated event attributes in this version

No event attributes have been deprecated in this release.

29.3.3. Event attributes modified in this version

No event attributes have been modified in this version.

29.4. Bug fixed and known issues

29.4.1. Bugs fixed in this version

- SF#6617 - RTC#1822 - **[funshion] classification issue**

Bug Info	Description
Reported against	ProtocolBundle-1.19.0
Platform	All
Effect of bug	Classification Anomaly
Expected versus actual behavior	Classification issues for the Funshion web site and the dedicated client.

29.4.2. Known issues

There are no known issues raised in this release.

30. Protocol Bundle 1.18.0

30.1. What's new in the Protocol Bundle 1.18.0

30.1.1. Note about the major enhancements of the release

30.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release:

- `comm` : VoIP/IM mobile application.
- `cctv_vod` : Chinese VOD service.
- `spdy` : add classification of SPDY connections (over SSL or raw TCP).
- `iperf` : iperf is used by the self-titled tool for network performance measures.
- The following HTTP upper protocols have been added: `konaminet`, `mobage`, `monex`, `nend`, `radiko` and `softbank .`

The following protocols have been updated:

- `gmail` : corrections/enhancement
- `http` : multiple lines header extraction issue
- `http` : new metadata from « Authorization » header
- `http` : provide offsets attributes for "uri" and "user-agent", and offset attribute for "Request header end". Please refer to the protobook attribute documentation for details about these new metadata.
- `jabber` : Add socks4/5, https, ssl as bottom layers
- `line` : log metadata related to calls (timings, user info)
- `lotusnotes` : add attach_compress attribute
- `myspace` : login extraction improvement
- `myspace` : complete protocol update
- `paltalk` : extract channel fix
- `pop3, smtp, imap` : adding UTF-8 extraction
- `qq` : support of last versions (complete plug-in rewrite)
- `qvod` : update classification over TCP
- `shoutcast` : supporting last Winamp versions
- `squirrelmail` : missing attach_id, wrong email address.
- `ssl` : support the TLS NPN (next protocol) extension, required by SPDY/HTTP 2.0

- `viber` : support up to version 3.0
- `wechat` : protocol update.
- `whatsapp` : extracting customer's phone number
- `ymsg_conf` : adding call duration information

Important

Encoded strings (unicode, mime-encoding) of the protocols pop3, smtp and imap are now converted into UTF-8. All ixEngine string (CLEP_DATA_STRING) attributes must now be considered as UTF-8 strings. This functionality is available depends on the `iconv` library availability on the targeted OS.

30.1.1.2. Other features and enhancements

RT#	Description
17462	[rtmp] big allocation even in classification mode
17677	[PERF] [http] merge header_name and header_value in one attribute header_raw
18167	[HTTP] Provide attributes for pointers in payload for start of http header end
18168	[PERF][altiris]suppress smb from bottom layers (optimize smb)
18169	[SCCP] Add attributes device_type and device_name for SCCP

30.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-26 and higher (for ixe 4.15.x versions), ixEngine 4.16.2-20 and higher (for ixe 4.16.x versions) and 4.17.0-20 and higher versions of ixEngine.

30.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

30.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

30.2. Protocol updates

30.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 62. New protocols added in this version

Proto ID	Protocol	Description
1439	konaminet	This protocol plug-in classifies the http traffic to the host konaminet.jp. It also classifies the ssl traffic to the Common Name konaminet.jp.
1463	cctv_vod	VodCCTV provides a web on-line video and video on demand client for the CCTV Chinese television network.
1496	comm	COMM is a VoIP and Instant messaging application for mobile phones commonly used in Japan.
1461	iperf	The iperf protocol is used by the self-titled tool for network performance measures.
1456	mobage	Mobile games download portal and identification services.
1460	monex	Online broker.
1459	nend	Mobile in-apps ads integration service.
1458	radiko	Broadband broadcasts web retransmission services.
1457	softbank	Sorftbank network operator services.
1469	spdy	Experimental protocol initiated by Google to exchange web content and reduce the load time of the web pages.

30.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

30.3. Attributes

This section describes the attribute updates.

30.3.1. New event attributes added in this version

The following event attributes have been added in this version.

30.3.1.1. Generic events added in this version

There's no generic event added in this version.

30.3.1.2. Events added in this version

Table 63. Added event attributes

Protocol	New event attributes
http	auth_password
http	auth_username
http	header_end_offset
http	header_raw
http	uri_end_offset
http	uri_start_offset
http	user_agent_end_offset
http	user_agent_start_offset
line	call
line	call_byte_count
line	call_duration
line	call_id
line	call_pkt_count
line	callee
line	caller_addr
line	end
line	start_time
lotusnotes	attach_compress
qq	call_data
qvod	end
qvod	peer
qvod	peer_ip
qvod	peer_port
sccp	device_name
sccp	device_type
ssl	supported_next_protocol
whatsapp	phone_number
ymsg_conf	call_duration

30.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 64. Deprecated event attributes

Protocol	Deprecated event attributes	
base	date	
base	string	
base	uint16	
base	uint32	
base	uint64	
base	uint8	

30.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 65. Event attributes modified

Protocol	Event attribute	Changes
google_maps	east	in PB 1.14.0 [string,client,session_mod,space] in PB 1.15.0 [string,server,session_mod,space]
google_maps	north	in PB 1.14.0 [string,client,session_mod,space] in PB 1.15.0 [string,server,session_mod,space]
google_maps	south	in PB 1.14.0 [string,client,session_mod,space] in PB 1.15.0 [string,server,session_mod,space]
google_maps	space	in PB 1.14.0 [parent,client,session_mod,no_parent] in PB 1.15.0 [parent,server,session_mod,no_parent]
google_maps	west	in PB 1.14.0 [string,client,session_mod,space] in PB 1.15.0 [string,server,session_mod,space]

Protocol	Event attribute	Changes
google_maps	zoom	in PB 1.14.0 [string,client,session_mod,space] in PB 1.15.0 [string,server,session_mod,space]
qq	msg_type	in PB 1.14.0 [string_index,both,session_mod,no_parent] in PB 1.15.0 [uint32,both,session_mod,no_parent]

30.4. Bug fixed and known issues

30.4.1. Bugs fixed in this version

- 15645 - **[squirrelmail] missing attach_id, wrong email address.**

Bug Info	Description
Reported against	4.12.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 15924 - **[gmail] corrections/enhancement**

Bug Info	Description
Reported against	4.12.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16535 - **[SF5744] [ssl] issue with Session ID Length when it's 0**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Wrong Session ID extracted when the Session ID Length field of the SSL handshake is 0

- 16585 - **[IXP][XLR] [tns] packets extraction missing in coreplus IXP**

Bug Info	Description
Reported against	ProtocolBundle 1.6.0,ProtocolBundle 1.7.0
Platform	CorePlus-arm
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16680 - **[SF5829] [Skype] version extraction on ios version**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16806 - **SF5040: [ymail_classic] missing attach event**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.13.0,ProtocolBundle 1.5.0,ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Missing the last attachment summary after uploading several files.

- 16939 - **[SF5834] [ymsg_webmessenger] ymail2 classified as ymsg_webmessenger protocol**

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17522 - **[SF6192] [ip6] [udp] crc is wrongly computed**

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17571 - **[gre][ip][XLR/IXP] false wrong_crc value for gre and ip protocol**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17577 - **[ssl] incorrect bounds for encrypted payload**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17611 - **[SF6223] [icmp6] RTT not extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly

Bug Info	Description
Expected versus actual behavior	

- 17638 - **[http] multiple lines header extraction issue**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17710 - **[wtp] Bad classification between wtp and t38**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17711 - **[radius] Bad classification between wtp and radius**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17728 - **[http] [unmerge] rtt/request_size attributes are raised with no parent**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17764 - **[unit_test] gtpv2**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17824 - **[ftp] do not extract login twice**

Bug Info	Description
Reported against	ixm-4.13.1

Bug Info	Description
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	FTP LI probe partially export sessions

- 17828 - **[ftp] filename was kept between 2 up/downloads**

Bug Info	Description
Reported against	ixm-4.13.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17877 - **[BUG IXE] SCCP not classified**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	x86_64_USER
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17890 - **[PB] [extflow] bad pkt accessor used in multiple plug-ins**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	

- 17931 - **[SF6287] [gmail chat] missing classification over SSL**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.7.0
Platform	x86_64_USER
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17933 - **[mysql] Query not always extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17936 - **[tds] fix regression**

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17940 - **[SF6193] [spotify] Classification issue with fallback protocol**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	If Spotify is blocked using its default protocol, it will fallback to another protocol that fails to be detected by the ixEngine

- 17978 - **[SF6312] [gtpv2] gtpv2.s1u_sgw_gtpu_{teid,address} are not extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17993 - **[l2tp] Missing extraction**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17998 - **[teredo] missing attributes extraction**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 18025 - **[sf6310] [http] http:index is incremented when "100 CONTINUE" is received before "200 OK"**

Bug Info	Description
Reported against	ixm-4.14.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	http:index should not be incremented when "100 CONTINUE" is received before "200 OK"

- 18026 - **[SF6351] [smtp] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Classification issue if the session only contains the server error message

- 18080 - **[SF6356] [youtube] title extraction issue**

Bug Info	Description
Reported against	df-pb-1.12.0,ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	title of youtube videos isn't always extracted

- 18122 - **[sf5929][orangemail] login only extracted if logout operation is performed**

Bug Info	Description
Reported against	iol-2.2.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	login extraction expected before logout action.

- 18139 - **[bmff] duplicated source file name**

Bug Info	Description
Reported against	ProtocolBundle 1.10.0
Platform	All
Effect of bug	Other anomaly
Expected versus actual behavior	

- 18146 - **[SF6413] [GTP] TEID not extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 18150 - **[SF6395] [skype] spid.bittorrent is stealing some packets**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	The SPID-based bittorrent classification is stealing some packets classification to skype.

- 18162 - **[SF6816][http] uhttp_is_content_end only works if packet contains no less than 4 bytes**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 18201 - **[SF6242][ldap] Delete request not extracted**

Bug Info	Description
Reported against	ixm-4.14.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 18221 - **[SF6403] [google_maps] wrong way of attributes**

Bug Info	Description
Reported against	df-pb-1.12.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	If a tuple contains any of the following attributes: google_maps:zoom, google_maps:south, google_maps:east, google_maps:west, google_maps:north. Lines may never be created

30.4.2. Known issues

There's no known issue raised in this release.

31. Protocol Bundle 1.17.0

31.1. What's new in the Protocol Bundle 1.17.0

31.1.1. Note about the major enhancements of the release

31.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release:

- `baofeng` : New Dissector-based Protocol (PDL plug-ins) - mobile video player app
- `baidu_player` : New Dissector-based Protocol (PDL plug-ins) – mobile video player app
- `apple_maps` : New Signature-based Protocol (PDATA signatures) – maps mobile app from Apple
- `gomtv_vod` : New Signature-based Protocol (PDATA signatures) – mobile video player app
- `jingdong` : New Signature-based Protocol (PDATA signatures) – Chinese web store
- `lotus_live` : New Signature-based Protocol (PDATA signatures) – online collaborative office tools
- `qik_video` : New Signature-based Protocol (PDATA signatures) – video streaming web service
- `ubuntu_one` : New Signature-based Protocol (PDATA signatures) - file storage in the cloud

The following protocols have been updated:

- `icap` : embedded http request decoding and payload injection.
- `http` : file completed flag indicating whether file download is complete.
- `qq` : major update.
- `amazon_video` : classify RTMPe video stream.
- `skype` : extended 3G/SkypeOut classification.
- `winmx/gnutella` : classification update.
- `sccp` : attribute updates.

31.1.1.2. Others features and enhancements

- Protocol Data v2 – engine upgrade + SIP metadata integration.
- SPDY classification + extraction, classifying using PDATA engine.
- New offloading/cache-ability options.

Important

Important notice for source-customers: This bundle won't compile with existing frameworks (before the future ixE 4.18.x). Other frameworks need a patch adding the new "nocaching" proto_feature field. This patch will be provided with this delivery.

31.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-26 and higher (for ixe 4.15.x versions), ixEngine 4.16.2-20 and higher (for ixe 4.16.x versions) and 4.17.0-20 and higher versions of ixEngine.

31.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`

- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

31.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2

- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

31.2. Protocol updates

31.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 66. New protocols added in this version

Proto ID	Protocol	Description
1352	baofeng	Chinese video streaming portal.
1464	baidu_player	BaiduPlayer is a video player that can play local, online and OnDemand videos.
1498	jingdong	Popular chinese on-line hi-tech shop.
1499	lotus_live	Lotus live, maintenant IBM SmartCloud, est une suite d'applications web pour l'entreprise, fournissant des services de mail, de transfert de fichiers ou de meetings.
1500	apple_maps	Apple Maps is a proprietary map application for iOS 6 devices.
1501	ubuntu_one	Ubuntu One is a cloud file storage service available on PC and smartphones.
1502	qik_video	QIK is a PC/smartphone application allowing live and VOD streaming from the web. The video chat additional feature is not supported yet.
1503	gomtv_vod	Gom TV is a social video website designed for gamers.

31.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

31.3. Attributes

This section describes the attribute updates.

31.3.1. New event attributes added in this version

The following event attributes have been added in this version.

31.3.1.1. Generic events added in this version

There's no generic event added in this version.

31.3.1.2. Events added in this version

Table 67. Added event attributes

Protocol	New event attributes
gnutella	peer
gnutella	peer_addr
gnutella	peer_port
h225	version
hi5	uid
http	declassify_override
http	file_completed
http	nocaching_override
http	ntlm_domain
http	ntlm_user
http	ntlm_workstation
icap	x_client_ip
line	user_agent
mplus_messenger	service
mplus_messenger	service_id
nntp	login
nntp	password
postgres	authentification_type
postgres	password
spdy	associated_stream_id
spdy	content
spdy	control_frame
spdy	control_type
spdy	data_frame
spdy	end
spdy	flags
spdy	frame_type
spdy	header
spdy	header_count
spdy	header_name
spdy	header_value

Protocol	New event attributes
spdy	length
spdy	priority
spdy	rst_stream
spdy	slot
spdy	status_code
spdy	stream_id
spdy	syn_stream
spdy	version
ssl	declassify_override

31.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

31.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 68. Event attributes modified

Protocol	Event attribute	Changes
adobe_update	update_request	in PB 1.16.0 [parent,server,session_fix,no_parent] in PB 1.17.0 [parent,client,session_fix,no_parent]
aim	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
aim	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
aim_transfer	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]

Protocol	Event attribute	Changes
dhcp	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
ftp	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
ftp_data	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
gmail_chat	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
gmail_mobile	contact_uid	in PB 1.16.0 [string,both,session_mod,no_parent] in PB 1.17.0 [string,both,session_prt,contact_entry]
gmail_mobile	email_index	in PB 1.16.0 [string,both,session_mod,no_parent] in PB 1.17.0 [string,both,session_prt,email]
gtp	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
gtp	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
gtpv2	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
gtpv2	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
h225	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
h245	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
h245	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
http_tunnel	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
http_tunnel	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
ip	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
irc	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]

Protocol	Event attribute	Changes
irc_transfer	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
jabber	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
jabber_transfer	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
mgcp	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
msn	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
msn	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
msn_video	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
paltalk	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
paltalk	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
paltalk_audio	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
paltalk_transfer	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
paltalk_video	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
radius	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
rdt	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
rtcp	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
rtp	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
rtp	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]

Protocol	Event attribute	Changes
rtsp	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
sccp	call_way	in PB 1.16.0 [string_index,both,session_mod,call] in PB 1.17.0 [uint32,both,session_mod,call]
sccp	callstate	in PB 1.16.0 [string_index,both,session_mod,call] in PB 1.17.0 [uint32,both,session_mod,call]
sccp	codec	in PB 1.16.0 [string_index,both,session_mod,call] in PB 1.17.0 [uint32,both,session_mod,call]
sccp	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
sccp	message_type	in PB 1.16.0 [string_index,both,session_mod,no_parent] in PB 1.17.0 [uint32,both,session_mod,no_parent]
sccp	softkeyevent	in PB 1.16.0 [string_index,both,session_mod,no_parent] in PB 1.17.0 [uint32,both,session_mod,no_parent]
sip	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
sip	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
t38	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
ymsg	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
ymsg	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
ymsg_conf	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
ymsg_conf	inherit_parent	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
ymsg_transfer	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]
ymsg_video	inherit_key	in PB 1.16.0 [binary,both,session_fix,no_parent] in PB 1.17.0 [binary,both,session_mod,no_parent]

Protocol	Event attribute	Changes
youtube	video	in PB 1.16.0 [parent,client,session_fix,no_parent] in PB 1.17.0 [parent,both,session_fix,no_parent]

31.4. Bug fixed and known issues

31.4.1. Bugs fixed in this version

- 16611 - **[SF5738] [pplive] Classification issue over UDP**

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16888 - **[SF5926] [gmail_mobile] contact_uid not in contact_entry parent and email_index not in email parent**

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	contact_uid and email_index are not extracted in the parent they are identifying.

- 16981 - **[SF5884] [ymsg_webmessenger] message not extracted due to statemachine anomaly**

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Extraction incomplete due to statemachine anomaly

- 18368 - **[SF6476] [HTTP] - request_size is not extracted on the same packet when extracted with dechunk_size**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	request_size should be extracted on the same packet when extracted with dechunk_size

- 18377 - **[SF6518] [stun] classification issue**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	STUN isn't classified as it should be, preventing the classification of RTP

- 18384 - **[SF5635] [sina_video] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Classification issue of sina_video

- 18436 - **[SF6571] Improve google_docs classification**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 18584 - **[SF6619] [niconico_douga] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Some niconico_douga related traffic isn't clssified as such

- 18595 - **[SF6629] [pandora] Missing Classification**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Downloading album covers isn't classified as pandora

31.4.2. Known issues

- 16585 - **[IXP][XLR] [tns] packets extraction missing in coreplus IXP**

Bug Info	Description
Reported against	ProtocolBundle 1.6.0,ProtocolBundle 1.7.0
Platform	CorePlus-arm
Effect of bug	Classification anomaly
Expected versus actual behavior	
Workaround	No workaround

- 18607 - **[SF6624] [kakaotalk] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0

Bug Info	Description
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	
Workaround	No workaround

- 18613 - **issue with QQ protocol**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	
Workaround	No workaround

32. Protocol Bundle 1.16.0

32.1. What's new in the Protocol Bundle 1.16.0

32.1.1. Note about the major enhancements of the release

32.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release:

- `apple_maps` : Apple Maps is a proprietary map application for iOS 6 devices.
- `gomtv_vod` : Gom TV is a social video website designed for gamers.
- `lotus_live` : Lotus live, now IBM SmartCloud, is a web-based collaborative suite of applications for enterprises, including mail, file transfer, meetings and forms.
- `qik_video` : QIK is a PC/smartphone application allowing live and VOD streaming from the web. The video chat additional feature is not supported yet.
- `ubuntu_one` : Ubuntu One is a cloud file storage service available on PC and smartphones.

The following protocols have been updated: `apple`, `ask`, `buzzfeed`, `cam4`, `citrix_online`, `cloudme`, `conduit`, `evernote`, `fileflyer`, `hotfile`, `mixi`, `mobage`, `myspace`, `nend`, `nimbuzz_web`, `rambler_webmail`, `reddit`, `sky_player` and `xhamster`.

32.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-26 and higher (for ixe 4.15.x versions), ixEngine 4.16.2-20 and higher (for ixe 4.16.x versions) and 4.17.0-20 and higher versions of ixEngine.

32.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don’t forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn’t be found by the dynamic linker when your starts.

32.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

32.2. Protocol updates

32.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 69. New protocols added in this version

Proto ID	Protocol	Description
1500	apple_maps	Apple Maps is a proprietary map application for iOS 6 devices.
1503	gomtv_vod	Gom TV is a social video website designed for gamers.
1499	lotus_live	Lotus live, now IBM SmartCloud, is a web-based collaborative suite of applications for enterprises, including mail, file transfer, meetings and forms.
1502	qik_video	QIK is a PC/smartphone application allowing live and VOD streaming from the web. The video chat additional feature is not supported yet.
1501	ubuntu_one	Ubuntu One is a cloud file storage service available on PC and smartphones.

32.2.2. Deprecated protocols in this version

Table 70. Deprecated protocols in this version

Proto ID	Protocol	Description	Comments
363	avatars_united	This protocol plug-in classifies the http traffic to the host avatarsunited.com	On September 23, 2010 Linden Lab announced the closure of Avatars United.

32.3. Attributes

This section describes the attribute updates.

32.3.1. New event attributes added in this version

The following event attributes have been added in this version.

32.3.1.1. Generic events added in this version

There's no generic event added in this version.

32.3.1.2. Events added in this version

There's no added event in this version.

32.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

32.3.3. Event attributes modified in this version

There is no modified attributes in this version.

32.4. Bug fixed and known issues

32.4.1. Bugs fixed in this version

- 18384 - **[SF5635] [sina_video] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Classification issue of sina_video

32.4.2. Known issues

There's no known issue raised in this release.

33. Protocol Bundle 1.15.0

33.1. What's new in the Protocol Bundle 1.15.0

33.1.1. Note about the major enhancements of the release

33.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release:

- `comm` : VoIP/IM mobile application (HP).
- `cctv_vod` : Chinese VOD service (Clavister).
- `spdy` : add classification of SPDY connections (over SSL or raw TCP).
- `iperf` : iperf is used by the self-titled tool for network performance measures.
- The following HTTP upper protocols have been added: `konaminet`, `mobage`, `monex`, `nend`, `radiko` and `softbank .`

The following protocols have been updated:

- `gmail` : corrections/enhancement
- `http` : multiple lines header extraction issue
- `http` : new metadata from « Authorization » header
- `http` : provide offsets attributes for "uri" and "user-agent", and offset attribute for "Request header end". Please refer to the protobook attribute documentation for details about these new metadata.
- `jabber` : Add socks4/5, https, ssl as bottom layers
- `line` : log metadata related to calls (timings, user info)
- `lotusnotes` : add attach_compress attribute
- `myspace` : login extraction improvement
- `myspace` : complete protocol update
- `paltalk` : extract channel fix
- `pop3, smtp, imap` : adding UTF-8 extraction
- `qq` : support of last versions (complete plug-in rewrite)
- `qvod` : update classification over TCP
- `shoutcast` : supporting last Winamp versions
- `squirrelmail` : missing attach_id, wrong email address.
- `ssl` : support the TLS NPN (next protocol) extension, required by SPDY/HTTP 2.0

- `viber` : support up to version 3.0
- `wechat` : protocol update.
- `whatsapp` : extracting customer’s phone number
- `ymsg_conf` : adding call duration information

Important

Encoded strings (unicode, mime-encoding) of the protocols pop3, smtp and imap are now converted into UTF-8. All ixEngine string (CLEP_DATA_STRING) attributes must now be considered as UTF-8 strings. This functionality is available depends on the `iconv` library availability on the targeted OS.

33.1.1.2. Others features and enhancements

RT#	Description
17462	[rtmp] big allocation even in classification mode
17677	[PERF] [http] merge header_name and header_value in one attribute header_raw
18167	[HTTP] Provide attributes for pointers in payload for start of http header end
18168	[PERF][altiris]suppress smb from bottom layers (optimize smb)
18169	[SCCP] Add attributes device_type and device_name for SCCP

33.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-26 and higher (for ixe 4.15.x versions), ixEngine 4.16.2-20 and higher (for ixe 4.16.x versions) and 4.17.0-20 and higher versions of ixEngine.

33.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don’t forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn’t be found by the dynamic linker when your starts.

33.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

33.2. Protocol updates

33.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 71. New protocols added in this version

Proto ID	Protocol	Description
1439	konaminet	This protocol plug-in classifies the http traffic to the host konaminet.jp. It also classifies the ssl traffic to the Common Name konaminet.jp.
1463	cctv_vod	VodCCTV provides a web on-line video and video on demand client for the CCTV Chinese television network.
1496	comm	COMM is a VoIP and Instant messaging application for mobile phones commonly used in Japan.
1461	iperf	The iperf protocol is used by the self-titled tool for network performance measures.
1456	mobage	Mobile games download portal and identification services.
1460	monex	Online broker.
1459	nend	Mobile in-apps ads integration service.
1458	radiko	Broadband broadcasts web retransmission services.
1457	softbank	Sorftbank network operator services.
1469	spdy	Experimental protocol initiated by Google to exchange web content and reduce the load time of the web pages.

33.2.2. Deprecated protocols in this version

There's no deprecated protocols for this version.

33.3. Attributes

This section describes the attribute updates.

33.3.1. New event attributes added in this version

The following event attributes have been added in this version.

33.3.1.1. Generic events added in this version

There's no generic event added in this version.

33.3.1.2. Events added in this version

Table 72. Added event attributes

Protocol	New event attributes
http	auth_password
http	auth_username
http	header_end_offset
http	header_raw
http	uri_end_offset
http	uri_start_offset
http	user_agent_end_offset
http	user_agent_start_offset
line	call
line	call_byte_count
line	call_duration
line	call_id
line	call_pkt_count
line	callee
line	caller_addr
line	end
line	start_time
lotusnotes	attach_compress
qq	call_data
qvod	end
qvod	peer
qvod	peer_ip
qvod	peer_port
sccp	device_name
sccp	device_type
ssl	supported_next_protocol
whatsapp	phone_number
ymsg_conf	call_duration

33.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 73. Deprecated event attributes

Protocol	Deprecated event attributes	
base	date	
base	string	
base	uint16	
base	uint32	
base	uint64	
base	uint8	

33.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
    - pkt: the attribute changes in each packet
    - session_mod: the attribute value is set for the whole session but may change
    - session_fix: the attribute value is fixed for the whole session
    - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 74. Event attributes modified

Protocol	Event attribute	Changes
google_maps	east	in PB 1.14.0 [string,client,session_mod,space] in PB 1.15.0 [string,server,session_mod,space]
google_maps	north	in PB 1.14.0 [string,client,session_mod,space] in PB 1.15.0 [string,server,session_mod,space]
google_maps	south	in PB 1.14.0 [string,client,session_mod,space] in PB 1.15.0 [string,server,session_mod,space]
google_maps	space	in PB 1.14.0 [parent,client,session_mod,no_parent] in PB 1.15.0 [parent,server,session_mod,no_parent]
google_maps	west	in PB 1.14.0 [string,client,session_mod,space] in PB 1.15.0 [string,server,session_mod,space]

Protocol	Event attribute	Changes
google_maps	zoom	in PB 1.14.0 [string,client,session_mod,space] in PB 1.15.0 [string,server,session_mod,space]
qq	msg_type	in PB 1.14.0 [string_index,both,session_mod,no_parent] in PB 1.15.0 [uint32,both,session_mod,no_parent]

33.4. Bug fixed and known issues

33.4.1. Bugs fixed in this version

- 15645 - **[squirrelmail] missing attach_id, wrong email address.**

Bug Info	Description
Reported against	4.12.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 15924 - **[gmail] corrections/enhancement**

Bug Info	Description
Reported against	4.12.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16535 - **[SF5744] [ssl] issue with Session ID Length when it's 0**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Wrong Session ID extracted when the Session ID Length field of the SSL handshake is 0

- 16585 - **[IXP][XLR] [tns] packets extraction missing in coreplus IXP**

Bug Info	Description
Reported against	ProtocolBundle 1.6.0,ProtocolBundle 1.7.0
Platform	CorePlus-arm
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16680 - **[SF5829] [Skype] version extraction on ios version**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16806 - **SF5040: [ymail_classic] missing attach event**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.13.0,ProtocolBundle 1.5.0,ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Missing the last attachment summary after uploading several files.

- 16939 - **[SF5834] [ymsg_webmessenger] ymail2 classified as ymsg_webmessenger protocol**

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17522 - **[SF6192] [ip6] [udp] crc is wrongly computed**

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17571 - **[gre][ip][XLR/IXP] false wrong_crc value for gre and ip protocol**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17577 - **[ssl] incorrect bounds for encrypted payload**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17611 - **[SF6223] [icmp6] RTT not extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly

Bug Info	Description
Expected versus actual behavior	

- 17638 - **[http] multiple lines header extraction issue**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17710 - **[wtp] Bad classification between wtp and t38**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17711 - **[radius] Bad classification between wtp and radius**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17728 - **[http] [unmerge] rtt/request_size attributes are raised with no parent**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17764 - **[unit_test] gtpv2**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17824 - **[ftp] do not extract login twice**

Bug Info	Description
Reported against	ixm-4.13.1

Bug Info	Description
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	FTP LI probe partially export sessions

- 17828 - **[ftp] filename was kept between 2 up/downloads**

Bug Info	Description
Reported against	ixm-4.13.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17877 - **[BUG IXE] SCCP not classified**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	x86_64_USER
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17890 - **[PB] [extflow] bad pkt accessor used in multiple plug-ins**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	

- 17931 - **[SF6287] [gmail chat] missing classification over SSL**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.7.0
Platform	x86_64_USER
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17933 - **[mysql] Query not always extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.15.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17936 - **[tds] fix regression**

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17940 - **[SF6193] [spotify] Classification issue with fallback protocol**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	If Spotify is blocked using its default protocol, it will fallback to another protocol that fails to be detected by the ixEngine

- 17978 - **[SF6312] [gtpv2] gtpv2.s1u_sgw_gtpu_{teid,address} are not extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17993 - **[l2tp] Missing extraction**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17998 - **[teredo] missing attributes extraction**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 18025 - **[sf6310] [http] http:index is incremented when "100 CONTINUE" is received before "200 OK"**

Bug Info	Description
Reported against	ixm-4.14.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	http:index should not be incremented when "100 CONTINUE" is received before "200 OK"

- 18026 - **[SF6351] [smtp] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Classification issue if the session only contains the server error message

- 18080 - **[SF6356] [youtube] title extraction issue**

Bug Info	Description
Reported against	df-pb-1.12.0,ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	title of youtube videos isn't always extracted

- 18122 - **[sf5929][orangemail] login only extracted if logout operation is performed**

Bug Info	Description
Reported against	iol-2.2.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	login extraction expected before logout action.

- 18139 - **[bmff] duplicated source file name**

Bug Info	Description
Reported against	ProtocolBundle 1.10.0
Platform	All
Effect of bug	Other anomaly
Expected versus actual behavior	

- 18146 - **[SF6413] [GTP] TEID not extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 18150 - **[SF6395] [skype] spid.bittorrent is stealing some packets**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	The SPID-based bittorrent classification is stealing some packets classification to skype.

- 18162 - **[SF6816][http] uhttp_is_content_end only works if packet contains no less than 4 bytes**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 18201 - **[SF6242][ldap] Delete request not extracted**

Bug Info	Description
Reported against	ixm-4.14.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 18221 - **[SF6403] [google_maps] wrong way of attributes**

Bug Info	Description
Reported against	df-pb-1.12.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	If a tuple contains any of the following attributes: google_maps:zoom, google_maps:south, google_maps:east, google_maps:west, google_maps:north. Lines may never be created

33.4.2. Known issues

There's no known issue raised in this release.

34. Protocol Bundle 1.14.0

34.1. What's new in the Protocol Bundle 1.14.0

34.1.1. Note about the major enhancements of the release

34.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release:

- `apple_siri`
- `buzzfeed`
- `citrix_online`
- `cloudme`
- `evernote`
- `google_docs`
- `hotfile`
- `imageshack`
- `imdb`
- `imeet`
- `imgur`
- `mapquest`
- `nimbuzz_web`
- `outlook`
- `peercast`
- `pinterest`
- `reddit`
- `sugar_sync`
- `thepiratebay`
- `webex_weboffice`
- `wikia`
- `xhamster`
- `zoho_notebook`

- `zoho_planner`
- `zoho_share`
- `zoho_sheet`
- `zoho_show`

The following protocols have been updated:

- `adnstream`
- `aim_express`
- `asmallworld`
- `blogger`
- `blogspot`
- `diino`
- `doubleclick_ads`
- `facebook_mail`
- `glide`
- `google_cache`
- `google_picasa`
- `google_plus`
- `gotomypc`
- `groove`
- `ibackup`
- `jabber`
- `lync_online`
- `meebo`
- `meetingplace`
- `mobile_me`
- `salesforce`
- `sharepoint_online`
- `skyblog`
- `slingbox`
- `windows_azure`
- `xboxlive`

- `ymsg_webmessenger`

34.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

34.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

34.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6

- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

34.2. Protocol updates

34.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 75. New protocols added in this version

Proto ID	Protocol	Description
1481	apple_siri	Advanced voice recognition system used on some Apple iPhone devices.
1476	buzzfeed	International news webportal.
1474	citrix_online	On-line collaboration suite for small businesses.
1471	cloudme	Free on-line file storage service.
1495	evernote	Web-based portal for note taking.
1489	google_docs	On-line file storage and sharing web-service by Google.
1485	hotfile	On-line file sharing service.
1486	imageshack	On-line free image sharing service.
1480	imdb	On-line information database related to movies and tv-shows.
1472	imeet	On-line video-conferencing service using cloud-based technology.
1483	imgur	A free online image hosting service.
1468	mapquest	This protocol plug-in classifies the http traffic to the hosts mapquest.com and mapquest.fr.
1488	nimbuzz_web	Instant Messaging client for mobile devices.
1478	outlook	On-line Microsoft Outlook encrypted service, from the Office 365 productivity suite.
1475	peercast	PeerCast is an open-source multimedia streaming protocol.
1470	pinterest	On-line service that allows users to attach personal elements on some kind of pinboard.
1479	reddit	Social news website.
1477	sugar_sync	On-line file backup and sync service.
1484	thepiratebay	The most popular Swedish Torrent indexing website.
1473	webex_weboffice	WebOffice is a collaboration suite for managing small businesses teams.
1482	wikia	A free Wiki website hosting service.
1487	xhamster	Pornographic videos streaming platform.
1490	zoho_notebook	Zoho Notebook application classification.
1491	zoho_planner	Zoho Planner application classification.
1492	zoho_share	Zoho Share application classification.
1493	zoho_sheet	Zoho Sheet application classification.
1494	zoho_show	Zoho Show application classification.

34.2.2. Deprecated protocols in this version

Table 76. Deprecated protocols in this version

Proto ID	Protocol	Description	Comments
287	mpquest	This protocol plug-in classifies the http traffic to the hosts mapquest.com and mapquest.fr.	This protocol is now identified as mapquest.
450	muxlin	This protocol plug-in classifies the http traffic to the host muxlim.com.	The Muxlim services have been closed in 2012.
1248	360buy	This protocol plug-in classifies the http traffic to the host 360buy.com.	The company's domain name changes to www.jd.com.

34.3. Attributes

This section describes the attribute updates.

34.3.1. New event attributes added in this version

The following event attributes have been added in this version.

34.3.1.1. Generic events added in this version

No new generic events have been added in this version.

34.3.1.2. Events added in this version

There's no event added in this version.

34.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

34.3.3. Event attributes modified in this version

There is no modified attributes in this version.

34.4. Bug fixed and known issues

34.4.1. Bugs fixed in this version

- 17922 - **[nokia_ovi.yahoo_maps] Missing classification**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17924 - **[zoho] Conflict on ssl common name**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17928 - **[google_maps] classification conflict**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17934 - **[opera_update] Conflict with my_opera**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 18011 - **[PDATA] lost information on the Protobook**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Other anomaly
Expected versus actual behavior	The classification methods and supported versions of "HTTP uppers" plugins are missing on the Protobook.

34.4.2. Known issues

There's no issue raised in this release.

35. Protocol Bundle 1.13.0

35.1. What's new in the Protocol Bundle 1.13.0

35.1.1. Note about the major enhancements of the release

35.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release:

- `espn`
- `mplus_messenger`
- `sina_video`
- `speedtest`
- `tunewiki`

The following protocols have been updated in this release:

- `gmx`: support for new JSON website (PDL).
- `youtube`: protocol update on PC and Mobile.
- `spotify`: support of the new web version of Spotify application.
- `whatsapp`: support of the classification and the extraction on the last verison.

Other enhancements:

- `SPID/bittorrent`: new classification of encrypted bittorrent-like streams as spid.bittorrent.
- `JSON` parser: support for embedded JAVASCRIPT code parsing in JSON.
- `PDL`: support for multiple JSON statemachines declaration.

35.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

35.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`

- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

35.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

35.2. Protocol updates

35.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 77. New protocols added in this version

RT#	Proto ID	Protocol	Description
17726	1455	mplus_messenger	M+ is a taiwanese mobile IM application with audio/image file send feature.
17671	1467	espn	American news website/resources about sports.
17668	1462	sina_video	Chinese on-line video streaming and VOD service.
17672	1465	speedtest	Web site and mobile application for testing both bandwidth and latency of any internet connection.
17470	1446	spid	SPID (Statistical Protocol IDentification) is a statistical classification engine, used to identify encrypted or obfuscated streams from advanced Peer-to-peer or VPN protocols (ex: BitTorrent RC4 streams).
17670	1466	tunewiki	Lyrics and photos sharing webservice, available in web and mobile-app versions.

35.2.2. Deprecated protocols in this version

Table 78. Deprecated protocols in this version

Proto ID	Protocol	Description	Comments
50	gizmo	Gizmo was an instant messaging service.	Gizmo has been acquired and closed by Google.

35.2.3. Other features

RT#	Description
17331	[SF6085] line: exploit HTTP POST call log
17470	[5875][SPID] implement spid layer for generic-p2p classification
17599	[ursh] group private events in is_proto function
17698	[protobook] add inherit key description
17777	HTTP request_size description update

35.2.4. Protocol Updates

- 15458

  [SF4541] [gmx] - Protocol now exchanges data in json format

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Rewrite protocol classification and extraction source code to match json format

- 15776

  [ares] unknown classification on data transfer traffic

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17105

  [whatsapp] support attribute extraction on last versions

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	extract version attribute

- 17320

  [SF5725][imp] protocol update

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	

- 17371

  [ares] support throttling use case with last ARES version

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17395

[SF6131] [mysql] login is not extracted on mysql version > 4.1

Bug Info	Description
Reported against	df-pb-1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17625

[SF6217][ProtocolBundle][PB] zshare hostname changed

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	x86_64_USER
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17659

[SF5824] [youtube] mobile & desktop protocol update needed

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

35.3. Attributes

This section describes the attribute updates.

35.3.1. New event attributes added in this version

The following event attributes have been added in this version.

35.3.1.1. Generic events added in this version

No new generic events have been added in this version.

35.3.1.2. Events added in this version

The following events have been added in this version:

Note:

Only non-generic event attributes are mentioned in this section. See the Qosmos ixEngine Protobook for details of generic events available for all protocols.

Table 79. New event attributes in this version

Protocol	New event attributes
bittorrent	peer_share_ip6
imp	msglist_receiver_email
spid	divergence
spid	end
spid	found_protocol
spid	result

35.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 80. Deprecated event attributes

Protocol	Deprecated event attributes	Comments
gizmo	callee, caller, login and service	The protocol is deprecated.

35.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 81. Event attributes modified

Protocol	Event attribute	Changes
bgp	error_notification_data	in p_1_12_0-20 [string,both,session_mod,message_entry] in p_1_13_0-20 [binary,both,session_mod,message_entry]
http	image	in p_1_12_0-20 [parent,server,session_mod,no_parent] in p_1_13_0-20 [parent,server,session_mod,request]
kakaotalk	login	in p_1_12_0-20 [int64,both,session_mod,no_parent] in p_1_13_0-20 [uint64,both,session_mod,no_parent]
slsk	file_id	in p_1_12_0-20 [int64,both,session_mod,file] in p_1_13_0-20 [uint64,both,session_mod,file]
viber	filesize	in p_1_12_0-20 [uint32,both,session_mod,no_parent] in p_1_13_0-20 [uint64,both,session_mod,no_parent]

35.4. Bug fixed and known issues

35.4.1. Bugs fixed in this version

- 15042 - **[SF4490][ymsg_webmessenger] html code in chat/message**

Bug Info	Description
Reported against	ProtocolBundle 1.1.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Expected behavior: get chat/message without any html code

- 15106 - **[viber] some attribute extraction lost on XLR platform**

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 15635 - **[jabber] caller/callee addr/port can be reversed.**

Bug Info	Description
Reported against	4.12.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	caller/callee addr/port should not be reversed.

- 15646 - **[orangemail] missing all-in-on-zip attachment**

Bug Info	Description
Reported against	4.12.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 15717 - **[SF5336] [PDL] uint64 data are extracted as int64 data**

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16372 - **[SF5622][Mailru] upload attachment missing**

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16406 - **[youtube] server extraction/classification in unidir and bidir.**

Bug Info	Description
Reported against	4.12.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16584 - **[socks4 - socks5] remote_addr is inverted in coreplus IXP and XLR**

Bug Info	Description
Reported against	ProtocolBundle 1.6.0,ProtocolBundle 1.7.0
Platform	CorePlus-arm
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16587 - **[viber][IXP][XLR] data packets are missing in coreplus IXP**

Bug Info	Description
Reported against	ProtocolBundle 1.6.0,ProtocolBundle 1.7.0
Platform	CorePlus-arm
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16709 - **[zimbra] extraction anomaly on parent email**

Bug Info	Description
Reported against	4.12.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17098 - **[sccp] SCCP/RTP inheritance not working**

Bug Info	Description
Reported against	ProtocolBundle 1.8.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17101 - **[ebuddy] support for mobile app (classification+extraction)**

Bug Info	Description
Reported against	ProtocolBundle 1.8.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17166 - **[SF5989] [gmail_basic] generated page not well parsed...**

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17193 - **[XLR][line] version attribute not extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17195 - **[XLR][smb] lost extraction**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17234 - **[SF5737] [ppstream] classification issue over TCP**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.9.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Binary PPStream flows over TCP are not classified

- 17340 - **[bittorrent] False positive**

Bug Info	Description
Reported against	ProtocolBundle 1.8.0,ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17346 - **[SF5843] [youtube] extraction issue**

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Description is not extracted

- 17494 - **[SF5944] [max_pkt] : documentation clarification**

Bug Info	Description
Reported against	ixE-4.17.1
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	

- 17510 - **[octeon-perf][teamviewer] False Classification**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	OcteonPlus
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17512 - **[octeon-perf][google] False Classification**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	OcteonPlus
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17579 - **[yahoo_transfer] Permissive pattern lead to false classification**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17582 - **[box_net] ambiguous Pattern (conflict with xbox)**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17584 - **[owa] Missing classification**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17587 - **[SF6132] [ftp] Classification issue in EXTFLOW**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	FTP is not correctly classified in External Flow mode

- 17611 - **[SF6223] [icmp6] RTT not extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17707 - **[http] [google_maps] segmentation fault**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	

- 17730 - **[live_hotmail] missing session_id**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17731 - **[yandex_webmail] wrong attach_type**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17732 - **[gmail_mobile] missing email_index**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17977 - **[SF6192] [UDP] wrong_crc : checksum is zero, then this field must be set to 0xFFFF.**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17982 - **[ip] leak**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Memory leak
Expected versus actual behavior	

35.4.2. Known issues

- 16806 - **SF5040: [ymail_classic] missing attach event**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0,ProtocolBundle 1.13.0,ProtocolBundle 1.5.0,ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Missing the last attachment summary after uploading several files.
Workaround	No workaround

- 17412 - **[h225] call_duration value is wrong**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	
Workaround	No workaround

- 17418 - **[tango] missing classification**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	
Workaround	No workaround

- 17877 - **[BUG IXE] SCCP not classified**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	x86_64_USER
Effect of bug	Classification anomaly
Expected versus actual behavior	
Workaround	No workaround

- 17922 - **[nokia_ovi.yahoo_maps] Missing classification**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	
Workaround	No workaround

- 17924 - **[zoho] Conflict on ssl common name**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	
Workaround	No workaround

- 17928 - **[google_maps] classification conflict**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	
Workaround	No workaround

- 17934 - **[opera_update] Conflict with my_opera**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	
Workaround	No workaround

- 17940 - **[SF6193] [spotify] Classification issue with fallback protocol**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	If Spotify is blocked using its default protocol, it will fallback to another protocol that fails to be detected by the ixEngine
Workaround	No workaround

- 17998 - **[teredo] missing attributes extraction**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	
Workaround	No workaround

- 18011 - **Lost information on the Protobook**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Other anomaly
Expected versus actual behavior	The classification methods and supported versions of "HTTP uppers" plugins are missing on the Protobook.
Workaround	No workaround

- 18015 - **[SPID][BITTORENT] sometimes ssh was classified as bittorrent**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	ssh established sessions can be classified sometimes as spid.bittorrent.
Workaround	No workaround

- 18020 - **[oomdynalloc][ip] check priv struct fails**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	
Workaround	No workaround

- 18023 - **[pdl] incorrect bounds**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	
Workaround	No workaround

- 18026 - **[SF6351] [smtp] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle 1.13.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Classification issue if the session only contains the server error message
Workaround	No workaround

36. Protocol Bundle 1.12.0

36.1. What's new in the Protocol Bundle 1.12.0

36.1.1. Note about the major enhancements of the release

36.1.1.1. New protocols, new attributes and updates

- New Office 365 plugins have been added (lync_live, sharepoint_live and office365),
- crocko (DDL),
- here (localization service),
- kankan (video streaming),
- meetme (social network),
- zoho (online professional applications).

36.1.1.2. Others features and enhancements

- Several plugins using the HTTP hosts and common names classification methods have been updated.
- Stability patchs have been also included in this version.

36.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

36.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

36.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

36.2. Protocol updates

36.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 82. New protocols added in this version

RT#	Proto ID	Protocol	Description
17660	1450	crocko	CROCKOTec is a Direct Download (DDL) file sharing website.
17660	1451	here	On-line maps and localization service brought by NAVTEQ and Nokia Maps.
17660	1447	kankan	Chinese video streaming website.
17660	1454	lync_online	On-line version of the Microsoft Lync IM and VoIP services (included in Office 365).
17660	1452	meetme	Social networking web-service available on PC and mobile devices.
17660	1448	office365	Office 365 is a Microsoft on-line service which gives access to Office applications from the internet.
17660	1453	sharepoint_online	On-line version of the Microsoft Sharepoint services (included in Office 365).
17660	1449	zoho	Online professional applications.

36.2.2. Deprecated protocols in this version

Table 83. Deprecated protocols in this version

Proto ID	Protocol	Description	Comments
456	myyearbook	This protocol plug-in classifies the http trafic to the host myyearbook.com.	On June 4, 2012, myYearbook was renamed Meet Me. A new meetme plugin has been created in this release.
475	present	This protocol plug-in classifies the http trafic to the host presentlyapp.com.	The site is no longer available.
1208	kbstar	This protocol plug-in classifies the http trafic to the host kbstar.com.	The trafic is already handled by the kb_bank plugin.

36.2.3. Protocol Updates

- 17625

  [SF6217][ProtocolBundle][PB] zshare hostname changed

Bug Info	Description
Reported against	ProtocolBundle 1.7.0

Bug Info	Description
Platform	x86_64_USER
Effect of bug	Classification anomaly
Expected versus actual behavior	zshare website activity failed to be classified.

36.3. Attributes

This section describes the attribute updates.

36.3.1. New event attributes added in this version

The following event attributes have been added in this version.

36.3.1.1. Generic events added in this version

No new generic events have been added in this version.

36.3.1.2. Events added in this version

There's no added event in this version.

36.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

36.3.3. Event attributes modified in this version

There's no updated event in this version.

36.4. Bug fixed and known issues

36.4.1. Bugs fixed in this version

- 17636 - **[bittorrent] [http] segmentation fault**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	Segmentation fault risk on the BitTorrent plugin. The code must be strengthened.

- 17641 - **[PDL] [APPSDK] re-establish (http-host) and (ssl-common-name)**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	The http-host and ssl-common-name limitations must be fixed.

36.4.2. Known issues

There's no known issue raised in this version.

37. Protocol Bundle 1.11.0

37.1. What's new in the Protocol Bundle 1.11.0

37.1.1. Note about the major enhancements of the release

37.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release:

- `winny` and `share` which are encrypted peer-to-peer protocols.
- `s1ap`, `m2pa`, `m2ua`, `m3ua`, `sccp_ss7`, `sua`, `v5ua` (LTE protocols).
- `gtalk` classification over jabber.

The following protocols have been updated in this release:

- `cloudflare`
- `diameter`
- `050plus`
- `line`
- `sina_weibo`
- `qq, qqdownload`
- `ymail_mobile_new`
- `youtube`
- `socks5`
- `bittorrent`

37.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

37.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`

- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

37.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

37.2. Protocol updates

37.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 84. New protocols added in this version

RT#	Proto ID	Protocol	Description
	1443	conduit	Conduit provides services for web sites audience increase.
17075	1441	gtalk	Google Talk is an instant messaging service, using XMPP, and provides both text and voice communication.
16487	1304	m2pa	M2PA is a signaling peer-to-peer protocol used by MTP2 in the Signaling System 7 (SS7).
16487	1302	m2ua	M2UA is an SCTP adaptation layer for encapsulated MTP2 messages in the Signaling System 7 (SS7).
16487	1301	m3ua	M3UA enables SS7 protocols stacking (ISUP, SCCP, ...) over an IP network.
16487	1306	s1ap	S1 Application Protocol (S1AP), tel que décrit dans 3GPP TS 36.413 version 11.2.1 Release 11 (2013-02).
16487	1307	sccp_ss7	SCCP is a network layer protocol that provides routing, flow control or error detection services in SS7 networks.
11470	1444	share	Share is a free peer-to-peer application allowing users to exchange files anonymously and in a secure way.
16487	1303	sua	This protocol defines the transport of SCCP signalization over an IP network through SCTP.
16487	1305	v5ua	V5UA is a transport mechanism for V5.2 messages in an IP network, through SCTP.
11471	1442	winny	Winny (also known as WinNY) is a Japanese peer-to-peer (P2P) file-sharing program.

37.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

37.2.3. Other features

RT#	Description
17075	[SF6100][SF4551][SF4597] Classify Gtalk as jabber.gtalk and not jabber.google_gen anymore
17144	[kazaa] Improve classification

RT#	Description
17191	[ssl] add port-based uppers classification documentation
17318	[H225] bad callee value
17319	[socks5] add support for SOCKS5 connections over UDP
17360	[SF6067] Deprecated tag in protocol.xml
17367	[SF6067] Protobook update: Deprecated tag in protocols.xml

37.2.4. Protocol Updates

- 15763

  [bittorrent] unknown classification with torrent client on socks proxy

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16517

  [SF5581] [diameter] SCTP support + new attribute

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	

- 17097

  [rtp] support ymsg-specific RTP streams

Bug Info	Description
Reported against	ProtocolBundle 1.8.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17107

  [line] classification enhancement

Bug Info	Description
Reported against	ProtocolBundle 1.8.0
Platform	All
Effect of bug	Classification anomaly

Bug Info	Description
Expected versus actual behavior	

- 17146

[qq] not classified on last beta version

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17175

[ymail_mobile_new][proto update] improve extraction

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 17185

[yahoo] Japanese classification update

Bug Info	Description
Reported against	ixm-4.14.0
Platform	x86_64_USER
Effect of bug	Classification anomaly
Expected versus actual behavior	

37.3. Attributes

This section describes the attribute updates.

37.3.1. New event attributes added in this version

The following event attributes have been added in this version.

37.3.1.1. Generic events added in this version

No new generic events have been added in this version.

37.3.1.2. Events added in this version

The following events have been added in this version:

Note:

Only non-generic event attributes are mentioned in this section. See the Qosmos ixEngine Protobook for details of generic events available for all protocols.

Table 85. New event attributes in this version

Protocol	New event attributes
diameter	command_flags
s1ap	end
s1ap	ep
s1ap	ep_code
s1ap	ep_enb_ue_id
s1ap	ep_ie
s1ap	ep_ie_cgi
s1ap	ep_ie_code
s1ap	ep_ie_name
s1ap	ep_ie_rab
s1ap	ep_ie_rab_addr
s1ap	ep_ie_rab_addr6
s1ap	ep_ie_rab_id
s1ap	ep_ie_rab_teid
s1ap	ep_ie_tai
s1ap	ep_ie_value_raw
s1ap	ep_mme_ue_id
s1ap	ep_name
s1ap	ep_value_raw

37.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

37.3.3. Event attributes modified in this version

There is no modified attributes in this version.

37.4. Bug fixed and known issues

37.4.1. Bugs fixed in this version

- 12581 - **SF3533 [GMAIL] BUG attributes last_activity/last_activity_timestamp**

Bug Info	Description
Reported against	4.12.1,4.13.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	the attributes last_activity/last_activity_timestamp are sent in two events.

- 16362 - **[http] unit test fails**

Bug Info	Description
Reported against	ProtocolBundle 1.5.1,ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The attribute "forward_redline" belonging to the http protocol was not always raised when asked unitarily.

- 16632 - **[ldap] Extraction improvement**

Bug Info	Description
Reported against	ProtocolBundle 1.6.0,ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Unitary extraction of ldap attributes issues.

- 16651 - **[ymsg] Unit test fails on inherit_parent**

Bug Info	Description
Reported against	ProtocolBundle 1.6.0,ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The attribute "inherit_parent" belonging to the ymsg protocol was not always raised when asked unitarily.

- 16667 - **[SF5786] [ymail_classic] contact entry not extracted**

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Some contacts are available but not extracted.

- 16687 - **[SF5741] [Youku] missing classification**

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Classification issue of youku for images and videos for both the web and the full client versions

- 16697 - **[mapi] unitary extraction issues**

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Several unitary extraction bugs.

- 16759 - **[ldap] suspicious name extraction**

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	In case of unexpected message the plugin returns wrong results.

- 16981 - **[SF5884] [ymsg_webmessenger] message not extracted due to statemachine anomaly**

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Extraction incomplete due to statemachine anomaly

- 16983 - **[SF5973] SMTP crash**

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	OcteonPlus
Effect of bug	Crash
Expected versus actual behavior	A crash occurs during the smtp_end extraction event without extracting attachment.

- 17038 - **[sina_weibo] Improve classification**

Bug Info	Description
Reported against	ProtocolBundle 1.8.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Missing "sina_weibo" classification. Added a valid discriminant to classify the protocol.

- 17106 - **[qqdownload] no classification**

Bug Info	Description
Reported against	ProtocolBundle 1.8.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	classify qqdownload

- 17114 - **[qq] bad login value**

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Bad extraction for qq:login.

- 17117 - **[tcp] crash on utcp_on_packet**

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	A crash occurs when malloc is failling randomely.

- 17147 - **[slsk] Classification improvement**

Bug Info	Description
Reported against	ProtocolBundle 1.8.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	The "slsk" protocol classification was sometimes lost and/or delayed. In some cases it is possible to get the flow classified earlier.

- 17171 - **[SF6066] [SMB] Request inside a request.**

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Two SMB requests are extracted at the same time and should be extracted separately.

- 17208 - **[SF6081] [GTP] Classification issue**

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Other anomaly

Bug Info	Description
Expected versus actual behavior	Classification issue (gtp over gtp).

- 17346 - **[SF5843] [youtube] extraction issue**

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Description is not extracted

- 17394 - **[SF6131] [mysql] can not extract mysql query with a length over 255 bytes**

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	The extraction is not done if the query length is bigger than 256.

- 17438 - **[split] Compatibility issue**

Bug Info	Description
Reported against	1.0.0
Platform	All
Effect of bug	Other anomaly
Expected versus actual behavior	The current protocol bundle does not compile with IxE_4_15_xx

37.4.2. Known issues

- 17587 - **[SF6132] [FTP] Classification issue in EXTFLOW**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	FTP is not correctly classified in External Flow mode
Workaround	No workaround

- 17623 - **[APPSDK] can't do http-register and ssl-common-name anymore**

Bug Info	Description
Reported against	ProtocolBundle 1.11.0
Platform	All
Effect of bug	Other anomaly
Expected versus actual behavior	The http-register/http-host and ssl-common-name keywords have been removed from PDL.
Workaround	No workaround

38. Protocol Bundle 1.10.0

38.1. What's new in the Protocol Bundle 1.10.0

38.1.1. Note about the major enhancements of the release

38.1.1.1. New protocols, new attributes and updates

- 27 Japanese web sites have been added in this release.
- The hostnames list of the Japanese version of Yahoo has been updated.
- Classification for the Cloudflare service has been added.

38.1.1.2. Others features and enhancements

- A new method of port-based classification over SSL has been added and documented in a specific section of the plugin details included in the Protobook (for the protocols which are classified with their destination port over SSL).

38.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

38.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

38.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

38.2. Protocol updates

38.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 86. New protocols added in this version

RT#	Proto ID	Protocol	Description
16997	1316	2ch	This protocol plug-in classifies the web traffic to the host "2ch.net", or associated to the SSL Common Name "2ch.net".
16997	1322	atwiki	This protocol plug-in classifies the web traffic to the host "atwiki.jp", or associated to the SSL Common Name "atwiki.jp".
16997	1334	auone	This protocol plug-in classifies the web traffic to the hosts "auone.jp" and "auone-net.jp", or associated to the SSL Common Names "auone.jp" and "auone-net.jp".
16997	1323	biglobe_ne	This protocol plug-in classifies the web traffic to the host "biglobe.ne.jp", or associated to the SSL Common Name "biglobe.ne.jp".
16997	1320	blogimg	This protocol plug-in classifies the web traffic to the host "blogimg.jp", or associated to the SSL Common Name "blogimg.jp".
16997	1328	cocolog_nifty	This protocol plug-in classifies the web traffic to the host "cocolog-nifty.com", or associated to the SSL Common Name "cocolog-nifty.com".
16997	1314	dmm_co	This protocol plug-in classifies the web traffic to the host "dmm.co.jp", or associated to the SSL Common Name "dmm.co.jp".
16997	1315	doorblog	This protocol plug-in classifies the web traffic to the host "doorblog.jp", or associated to the SSL Common Name "doorblog.jp".
16997	1330	exblog	This protocol plug-in classifies the web traffic to the host "exblog.jp", or associated to the SSL Common Name "exblog.jp".
16997	1308	fc2	This protocol plug-in classifies the web traffic to the host "fc2.com", or associated to the SSL Common Name "fc2.com".
16997	1310	goo_ne	This protocol plug-in classifies the web traffic to the host "goo.ne.jp", or associated to the SSL Common Name "goo.ne.jp".
16997	1333	gree	This protocol plug-in classifies the web traffic to the host "gree.jp", or associated to the SSL Common Name "gree.jp".
16997	1313	hatena_ne	This protocol plug-in classifies the web traffic to the host "hatena.ne.jp", or associated to the SSL Common Name "hatena.ne.jp".

RT#	Proto ID	Protocol	Description
16997	1331	impress	This protocol plug-in classifies the web traffic to the host "impress.co.jp", or associated to the SSL Common Name "impress.co.jp".
16997	1311	kakaku	This protocol plug-in classifies the web traffic to the host "kakaku.com", or associated to the SSL Common Name "kakaku.com".
16997	1332	ldblog	This protocol plug-in classifies the web traffic to the host "ldblog.jp", or associated to the SSL Common Name "ldblog.jp".
16997	1318	nifty	This protocol plug-in classifies the web traffic to the host "nifty.com", or associated to the SSL Common Name "nifty.com".
16997	1329	nikkei	This protocol plug-in classifies the web traffic to the host "nikkei.com", or associated to the SSL Common Name "nikkei.com".
16997	1325	okwave	This protocol plug-in classifies the web traffic to the host "okwave.jp", or associated to the SSL Common Name "okwave.jp".
16997	1319	pixiv	This protocol plug-in classifies the web traffic to the host "pixiv.net", or associated to the SSL Common Name "pixiv.net".
16997	1309	rakuten	This protocol plug-in classifies the web traffic to the host "rakuten.co.jp", or associated to the SSL Common Name "rakuten.co.jp".
16997	1321	sakura_ne	This protocol plug-in classifies the web traffic to the host "sakura.ne.jp", or associated to the SSL Common Name "sakura.ne.jp".
16997	1317	seesaa	This protocol plug-in classifies the web traffic to the host "seesaa.net", or associated to the SSL Common Name "seesaa.net".
16997	1324	sonet_ne	This protocol plug-in classifies the web traffic to the host "so-net.ne.jp", or associated to the SSL Common Name "so-net.ne.jp".
16997	1326	tabelog	This protocol plug-in classifies the web traffic to the host "tabelog.com", or associated to the SSL Common Name "tabelog.com".
16997	1327	yomiuri	This protocol plug-in classifies the web traffic to the host "yomiuri.co.jp", or associated to the SSL Common Name "yomiuri.co.jp".
16997	1312	ameba	This protocol plug-in classifies the web traffic to the hosts "amebame.com", "ameba.jp" and "ameblo.jp", or associated to the SSL Common Names "amebame.com", "ameba.jp" and "ameblo.jp".
17317	1445	cloudflare	CloudFlare CDN is a content delivery network with advanced security and analytics features.

38.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

38.2.3. Other features

RT#	Description
17191	[ssl] Add port-based uppers classification documentation

38.2.4. Protocol Updates

- 17185

  [yahoo] Japanese classification update

Bug Info	Description
Reported against	ixm-4.14.0
Platform	x86_64_USER
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 17291

  [http_upper] Global common_names updates

Bug Info	Description
Reported against	ProtocolBundle 1.10.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

38.3. Attributes

This section describes the attribute updates.

38.3.1. New event attributes added in this version

The following event attributes have been added in this version.

38.3.1.1. Generic events added in this version

No new generic events have been added in this version.

38.3.1.2. Events added in this version

There's no added event in this version.

38.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

38.3.3. Event attributes modified in this version

There's no updated event in this version.

38.4. Bug fixed and known issues

38.4.1. Bugs fixed in this version

There's not bug fixed in this version.

38.4.2. Known issues

There's no known issue raised in this version.

39. Protocol Bundle 1.9.0

39.1. What's new in the Protocol Bundle 1.9.0

39.1.1. Note about the major enhancements of the release

39.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release:

- `adc`, peer-to-peer protocol from DirectConnect application.
- `3gpp_li`, new core network link-layer protocols have been added.
- `pornhub` classifies the web traffic to the hosts "pornhub.com" and "pornhub.phncdn.com".

The following protocols have been updated in this release:

- `youtube:` add support for metadata extraction on new API,
- `bebo (social network):` new version of the plugin and protocol update,
- `facebook (social network):` classification update,
- `line (mobile VoIP):` plugin update to support the version 3.5,
- `tango (mobile VoIP):` plugin update to support version 2.6,
- `ultrasurf (tunneling):` protocol update,
- `imp (webmail):` protocol update,
- `mailru:` several protocol updates.
- `slsk(soulseek):` new version of the plugin,
- `kazaa(fasttrack):` new version of the plugin,
- `uusee:` new version of the plugin,
- `ebuddy:` new version of the plugin,
- `aim_express:` new version of the plugin,
- `ustream:` web stream metadata extraction has been added,
- `viber (mobile VoIP):` metadata extraction has been updated.

39.1.1.2. Others features and enhancements

- `ulayer_store`: capability to resize the hashtable using the API.
- Plugins management and configuration information have been added in the Protobook.

39.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

39.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

39.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x
- This version has been validated on Solaris 10 for x86 32-bit AMP with an external flow manager

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3

- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

39.2. Protocol updates

39.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 87. New protocols added in this version

RT#	Proto ID	Protocol	Description
15778	1437	3gpp_li	3gpp_li is a protocol which form a standard for telecoms operators and networks operators.
16896	1438	adc	ADC is a peer-to-peer protocol widely used in Direct Connect networks. It superseeds the protocol NMDC and corrects many flaws identified in this older protocol.
16378	1440	pornhub	This protocol plug-in classifies the web traffic to the hosts "pornhub.com" and "pornhub.phncdn.com".

39.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

39.2.3. Other features

RT#	Description
15073	[offloading] change of "signaling" feature
15799	SF3918: [ICA] Report application as soon as possible

39.2.4. Protocol Updates

- 16676

  [sf5824][youtube] mobile & desktop protocol update needed

Bug Info	Description
Reported against	df-pb-1.5.1,df-pb-1.6.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly

- 16793

  [http] improve classification and extraction of video and image metadata

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	

- 16887

  [ios_ota_update] add host in order to classify ios_ota protocol

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Add new ios_ota_update host in order to improve the classification of our plugin.

- 16969

  SF5949: [whatsapp] add whatsapp.net in HTTP fast host

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Add whatsapp.net in whatsapp hosts to classify earlier proxified HTTPS sessions

39.3. Attributes

This section describes the attribute updates.

39.3.1. New event attributes added in this version

The following event attributes have been added in this version.

39.3.1.1. Generic events added in this version

No new generic events have been added in this version.

39.3.1.2. Events added in this version

The following events have been added in this version:

Note:

Only non-generic event attributes are mentioned in this section. See the Qosmos ixEngine Protobook for details of generic events available for all protocols.

Table 88. New event attributes in this version

Protocol	New event attributes
3gpp_li	correlation_number
3gpp_li	country_code
3gpp_li	hi3_domain_id
3gpp_li	ice_type
3gpp_li	liid
3gpp_li	national_params
3gpp_li	sequence_number
3gpp_li	t_pdu_direction
3gpp_li	timestamp
3gpp_li	version
adc	client_version
adc	command
adc	command_code
adc	command_type
adc	end
adc	file
adc	file_chunk
adc	file_chunk_content
adc	file_chunk_data_offset
adc	file_chunk_len
adc	file_hash
adc	file_is_compressed
adc	filename
adc	filesize
adc	peer_hash
adc	peer_id
adc	query

Protocol	New event attributes
slsk	account
slsk	end
slsk	file
slsk	file_chunk_content
slsk	file_id
ustream	account
ustream	end
ustream	login
ustream	password
ustream	query
ustream	query_raw
ustream	query_text
viber	end
viber	filesize

39.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 89. Deprecated event attributes

Protocol	Deprecated event attributes	Comments
amqp	inherit_key	No more inheritance in the plugin.
amqp	inherit_parent	No more inheritance in the plugin.
facebook	application	The information can be retreived with the facebook_apps plugin.
facebook	application_name	The information can be retreived with the facebook_apps plugin.
facebook	application_action	The information can be retreived with the facebook_apps plugin.
line	call	No more extracted. This information is available in SIP.
line	call_id	No more extracted. This information is available in SIP.
line	callee	No more extracted. This information is available in SIP.
line	caller	No more extracted. This information is available in SIP
line	end	No more extracted. This information is available in SIP.
slsk	content	This attribute has been replaced by file_chunk_content.
slsk	inherit_key	No more inheritance in the plugin.
slsk	inherit_parent	No more inheritance in the plugin.
ssl	inherit_key	No more inheritance in the plugin.
ssl	inherit_parent	No more inheritance in the plugin.

39.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 90. Event attributes modified

Protocol	Event attribute	Changes
bebo	account	in p_1_8_0-20 [parent,client,session_fix,no_parent] in p_1_9_0-10 [parent,both,session_mod,no_parent]
bebo	is_mobile_service	in p_1_8_0-20 [uint32,client,session_fix,no_parent] in p_1_9_0-10 [uint32,both,session_mod,no_parent]
bebo	login	in p_1_8_0-20 [string,client,session_prt,account] in p_1_9_0-10 [string,both,session_mod,account]
bebo	password	in p_1_8_0-20 [string,client,session_prt,account] in p_1_9_0-10 [string,both,session_mod,account]
ebuddy	chat_im	in p_1_8_0-20 [string,both,session_prt,chat] in p_1_9_0-10 [string,both,session_mod,chat]
ebuddy	client_message	in p_1_8_0-20 [string,both,session_prt,account] in p_1_9_0-10 [string,both,session_mod,account]
ebuddy	client_status	in p_1_8_0-20 [string,both,session_prt,account] in p_1_9_0-10 [string,both,session_mod,account]
ebuddy	contact_blocked	in p_1_8_0-20 [string,both,session_prt,contact_entry] in p_1_9_0-10 [string,both,session_mod,contact_entry]

Protocol	Event attribute	Changes
ebuddy	contact_im	in p_1_8_0-20 [string,both,session_prt,contact_entry] in p_1_9_0-10 [string,both,session_mod,contact_entry]
ebuddy	contact_login	in p_1_8_0-20 [string,both,session_prt,contact_entry] in p_1_9_0-10 [string,both,session_mod,contact_entry]
ebuddy	contact_message	in p_1_8_0-20 [string,both,session_prt,contact_entry] in p_1_9_0-10 [string,both,session_mod,contact_entry]
ebuddy	contact_nickname	in p_1_8_0-20 [string,both,session_prt,contact_entry] in p_1_9_0-10 [string,both,session_mod,contact_entry]
ebuddy	contact_status	in p_1_8_0-20 [string,both,session_prt,contact_entry] in p_1_9_0-10 [string,both,session_mod,contact_entry]
ebuddy	e_action	in p_1_8_0-20 [string,both,session_prt,account] in p_1_9_0-10 [string,both,session_mod,account]
ebuddy	im_network	in p_1_8_0-20 [string,both,session_prt,account] in p_1_9_0-10 [string,both,session_mod,account]
ebuddy	login	in p_1_8_0-20 [string,both,session_prt,account] in p_1_9_0-10 [string,both,session_mod,account]
ebuddy	message	in p_1_8_0-20 [string,both,session_prt,chat] in p_1_9_0-10 [string,both,session_mod,chat]
ebuddy	nickname	in p_1_8_0-20 [string,client,session_prt,account] in p_1_9_0-10 [string,both,session_mod,account]
ebuddy	password	in p_1_8_0-20 [string,both,session_prt,account] in p_1_9_0-10 [string,both,session_mod,account]
ebuddy	receiver	in p_1_8_0-20 [string,both,session_prt,chat] in p_1_9_0-10 [string,both,session_mod,chat]
ebuddy	sender	in p_1_8_0-20 [string,both,session_prt,chat] in p_1_9_0-10 [string,both,session_mod,chat]
kazaa	filename	in p_1_8_0-20 [string,client,session_fix,no_parent] in p_1_9_0-10 [string,both,session_mod,no_parent]

Protocol	Event attribute	Changes
kazaa	login	in p_1_8_0-20 [string,client,session_fix,no_parent] in p_1_9_0-10 [string,both,session_mod,no_parent]
kazaa	mime_type	in p_1_8_0-20 [string,server,session_fix,no_parent] in p_1_9_0-10 [string,both,session_mod,no_parent]
slsk	filename	in p_1_8_0-20 [string,client,session_mod,no_parent] in p_1_9_0-10 [string,both,session_mod,file]
slsk	filesize	in p_1_8_0-20 [uint32,both,session_mod,no_parent] in p_1_9_0-10 [uint32,both,session_mod,file]
slsk	login	in p_1_8_0-20 [string,client,session_mod,no_parent] in p_1_9_0-10 [string,both,session_mod,account]
slsk	password	in p_1_8_0-20 [string,client,session_fix,no_parent] in p_1_9_0-10 [string,both,session_mod,account]
slsk	query	in p_1_8_0-20 [string,client,session_mod,no_parent] in p_1_9_0-10 [string,both,session_mod,no_parent]
slsk	version	in p_1_8_0-20 [uint32,client,session_fix,no_parent] in p_1_9_0-10 [uint32,both,session_mod,no_parent]

39.4. Bug fixed and known issues

39.4.1. Bugs fixed in this version

- 16471

  [icq] Improve classification

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Some ICQ packets may be not correctly classified.

- 16575

  [sf5053][sip] caller/callee inverted

Bug Info	Description
Reported against	ProtocolBundle 1.6.0,ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Callee and caller attributes are inverted.

- 16576

  [sf5116][ftp] missing data_port extraction

Bug Info	Description
Reported against	ProtocolBundle 1.6.0,ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The ftp control connection data_port attribute is not extracted.

- 16681

  [poco] Improve classification over UDP

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	We miss classification on some pkts that contain the POCO pattern inside. It should be fixed

- 16790

  [split][facebook] bundle switching fails

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Memory leak
Expected versus actual behavior	We leak memory during hot swap on facebook protocol

- 16820

[ymail2] [ymail_mobile_new] classification over yahoo

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Classification issues on ymail depending on the server hostname.

- 16917

SF5923: [facebook] classification improvements

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Following facebook traffic is not correctly classified: * fb.me * fbstatic-a.akamaihd.net * fbshare.me

- 16945

[SF5944] [SIP] Flow not classified as SIP because first UDP content length is 3

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	When first packets are UDP packet with 3bytes length payload, the flow couldn't be classified as SIP.

- 16954

SF5955: [youporn] classification issue

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Youporn content hosted on third party CDN is not classified as youporn

- 16965

[rtp] segfault

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	Segfault should not occure on RTP/IPv6.

- 17005

SF5933: [GTP] QoS is not extracted from update PDP context requests or responses

Bug Info	Description
Reported against	df-pb-1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	QoS is not extracted from update PDP context requests or responses

- 17071

[SF5950] [amazon] Classification issue

Bug Info	Description
Reported against	ProtocolBundle 1.8.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	HTTP traffic to images-amazon.com and HTTPS traffic to ssl-images-amazon.com are not classified as amazon

39.4.2. Known issues

- 16137

[wtp] [octeonplus] Missing classification

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	OcteonPlus
Effect of bug	Classification anomaly
Expected versus actual behavior	WTP classification regression.
Workaround	No workaround

- 16732

SF5815 [http] mime part extraction issue

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All

Bug Info	Description
Effect of bug	Extraction anomaly
Expected versus actual behavior	Extra \r\n are extracted at the end of a mime part.
Workaround	No workaround

- 16782

[krb5] extra bytes raised

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Extra square brackets and a dot are extracted in the text64 attribute of krb5 protocol.
Workaround	No workaround

- 16792

[dcerpc] Classification issue over smb on Octeon Plus

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	OcteonPlus
Effect of bug	Classification anomaly
Expected versus actual behavior	On octeon-plus we miss dcerpc classification. This issue seems to be platform related. We should uniform the classification in order to get the same result we have on x86
Workaround	No workaround

- 16888

[SF5926] [Gmail_mobile] contact_uid not in contact_entry parent and email_index not in email parent

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	contact_uid and email_index are not extracted in the parent they are identifying.
Workaround	No workaround

- 16955

SF5958: [facebook] mark application_name and application_action as deprecated

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Other anomaly

Bug Info	Description
Expected versus actual behavior	facebook:application_name and facebook:application_action are now extracted in facebook_apps
Workaround	No workaround

- 17190

Issue on the search engine included in the Protobook

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	
Workaround	No workaround

- 17208

[SF6081] [GTP] Classification issue

Bug Info	Description
Reported against	ProtocolBundle 1.9.0
Platform	All
Effect of bug	Other anomaly
Expected versus actual behavior	
Workaround	No workaround

40. Protocol Bundle 1.8.0

40.1. What's new in the Protocol Bundle 1.8.0

40.1.1. Note about the major enhancements of the release

This Protocol Bundle brings major enhancements on Chinese hostnames: 105 new `upper_http` protocols have been added.

40.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

40.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Make sure you specify the location of the libraries in the `LD_LIBRARY_PATH` linker option.

40.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x

Specific high-performance platforms

- Intel DPDK 1.2.2

- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

40.2. Protocol updates

40.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 91. New protocols added in this version

RT#	Proto ID	Protocol	Description
16950	1339	10050net	This protocol plug-in classifies the web traffic to the host "10050.net".
16950	1336	104com	This protocol plug-in classifies the web traffic to the host "104.com.tw".
16950	1338	1111tw	This protocol plug-in classifies the web traffic to the host "1111.com.tw".
16950	1340	17173com	This protocol plug-in classifies the web traffic to the host "17173.com".
16950	1341	17u	This protocol plug-in classifies the web traffic to the host "17u.cn".
16950	1337	591tw	This protocol plug-in classifies the web traffic to the host "591.com.tw".
16950	1342	7k7k	This protocol plug-in classifies the web traffic to the host "7k7k.com".
16950	1335	91com	This protocol plug-in classifies the web traffic to the host "91.com".
16950	1343	9game	This protocol plug-in classifies the web traffic to the host "9game.cn".
16950	1344	aili	This protocol plug-in classifies the web traffic to the host "aili.com".
16950	1345	anzhi	This protocol plug-in classifies the web traffic to the host "anzhi.com".
16950	1346	appchina	This protocol plug-in classifies the web traffic to the host "appchina.com".
16950	1347	appledaily	This protocol plug-in classifies the web traffic to the hosts "appledaily.com.tw" and "appledaily.com".
16950	1348	appshopper	This protocol plug-in classifies the web traffic to the host "appshopper.com".
16950	1349	babyhome	This protocol plug-in classifies the web traffic to the host "babyhome.com.tw".
16950	1350	backpackers	This protocol plug-in classifies the web traffic to the host "backpackers.com.tw".
16950	1351	baike	This protocol plug-in classifies the web traffic to the host "baike.com".
16950	1352	baofeng	This protocol plug-in classifies the web traffic to the host "baofeng.com".
16950	1353	beanfun	This protocol plug-in classifies the web traffic to the host "beanfun.com".
16950	1354	books	This protocol plug-in classifies the web traffic to the host "books.com.tw".

RT#	Proto ID	Protocol	Description
16950	1355	businessweekly	This protocol plug-in classifies the web traffic to the host "businessweekly.com.tw".
16950	1356	china_airlines	This protocol plug-in classifies the web traffic to the host "china-airlines.com".
16950	1357	chinanews	This protocol plug-in classifies the web traffic to the host "chinanews.com".
16950	1358	chinatimes	This protocol plug-in classifies the web traffic to the host "chinatimes.com".
16950	1359	ck101	This protocol plug-in classifies the web traffic to the host "ck101.com".
16950	1360	cnyes	This protocol plug-in classifies the web traffic to the host "cnyes.com".
16950	1361	ctrip	This protocol plug-in classifies the web traffic to the host "ctrip.com".
16950	1362	dangdang	This protocol plug-in classifies the web traffic to the host "dangdang.com".
16950	1363	duowan	This protocol plug-in classifies the web traffic to the host "duowan.com".
16950	1364	eastmoney	This protocol plug-in classifies the web traffic to the host "eastmoney.com".
16950	1365	easytravel	This protocol plug-in classifies the web traffic to the host "easytravel.com.tw".
16950	1366	elle_tw	This protocol plug-in classifies the web traffic to the host "elle.com.tw".
16950	1367	etao	This protocol plug-in classifies the web traffic to the host "etao.com".
16950	1368	ettoday	This protocol plug-in classifies the web traffic to the host "ettoday.net".
16950	1369	eyny	This protocol plug-in classifies the web traffic to the host "eyny.com".
16950	1370	ezfly	This protocol plug-in classifies the web traffic to the host "ezfly.com".
16950	1371	eztravel	This protocol plug-in classifies the web traffic to the host "eztravel.com.tw".
16950	1372	fashionguide	This protocol plug-in classifies the web traffic to the host "fashionguide.com.tw".
16950	1373	fortunechina	This protocol plug-in classifies the web traffic to the host "fortunechina.com".
16950	1374	gamebase_tw	This protocol plug-in classifies the web traffic to the host "gamebase.com.tw".
16950	1375	gamer_tw	This protocol plug-in classifies the web traffic to the host "gamer.com.tw".
16950	1376	gamesmomo	This protocol plug-in classifies the web traffic to the host "gamesmomo.com".
16950	1377	gfan	This protocol plug-in classifies the web traffic to the host "gfan.com".
16950	1378	gohappy	This protocol plug-in classifies the web traffic to the host "gohappy.com.tw".
16950	1379	hexun	This protocol plug-in classifies the web traffic to the host "hexun.com".

RT#	Proto ID	Protocol	Description
16950	1380	hinet_games	This protocol plug-in classifies the web traffic to the host "games.hinet.net".
16950	1383	iapp	This protocol plug-in classifies the web traffic to the host "iapp.com.tw".
16950	1384	ifeng_finance	This protocol plug-in classifies the web traffic to the host "finance.ifeng.com".
16950	1381	i_gamer	This protocol plug-in classifies the web traffic to the host "i-gamer.net".
16950	1385	intalking	This protocol plug-in classifies the web traffic to the host "intalking.com".
16950	1382	i_part	This protocol plug-in classifies the web traffic to the host "i-part.com.tw".
16950	1386	kuxun	This protocol plug-in classifies the web traffic to the host "kuxun.cn".
16950	1387	lady8844	This protocol plug-in classifies the web traffic to the host "lady8844.com".
16950	1388	lativ	This protocol plug-in classifies the web traffic to the host "lativ.com.tw".
16950	1389	liontravel	This protocol plug-in classifies the web traffic to the host "liontravel.com".
16950	1390	lotour	This protocol plug-in classifies the web traffic to the host "lotour.com".
16950	1391	lvping	This protocol plug-in classifies the web traffic to the host "lvping.com".
16950	1392	mail_189	This protocol plug-in classifies the web traffic to the host "189.cn".
16950	1393	mail2000	This protocol plug-in classifies the web traffic to the host "mail2000.com.tw".
16950	1394	mangocity	This protocol plug-in classifies the web traffic to the host "mangocity.com".
16950	1395	mobile01	This protocol plug-in classifies the web traffic to the host "mobile01.com".
16950	1396	momoshop	This protocol plug-in classifies the web traffic to the host "momoshop.com.tw".
16950	1397	money_163	This protocol plug-in classifies the web traffic to the host "money.163.com".
16950	1398	moneydj	This protocol plug-in classifies the web traffic to the host "moneydj.com".
16950	1399	nba_china	This protocol plug-in classifies the web traffic to the host "china.nba.com".
16950	1400	nduoa	This protocol plug-in classifies the web traffic to the host "nduoa.com".
16950	1401	nownews	This protocol plug-in classifies the web traffic to the host "nownews.com".
16950	1402	payeasy	This protocol plug-in classifies the web traffic to the host "payeasy.com.tw".
16950	1403	pcgames	This protocol plug-in classifies the web traffic to the host "pcgames.com.cn".
16950	1404	pchome	This protocol plug-in classifies the web traffic to the host "pchome.com.tw".

RT#	Proto ID	Protocol	Description
16950	1405	pclady	This protocol plug-in classifies the web traffic to the host "pclady.com.cn".
16950	1406	pixnet	This protocol plug-in classifies the web traffic to the host "pixnet.net".
16950	1407	qq_blog	This protocol plug-in classifies the web traffic to the host "blog.qq.com".
16950	1408	qq_finance	This protocol plug-in classifies the web traffic to the host "finance.qq.com".
16950	1409	qq_games	This protocol plug-in classifies the web traffic to the host "games.qq.com".
16950	1410	qq_lady	This protocol plug-in classifies the web traffic to the host "lady.qq.com".
16950	1411	qq_mail	This protocol plug-in classifies the web traffic to the host "mail.qq.com".
16950	1412	qq_news	This protocol plug-in classifies the web traffic to the host "news.qq.com".
16950	1413	qunar	This protocol plug-in classifies the web traffic to the host "qunar.com".
16950	1414	ruten	This protocol plug-in classifies the web traffic to the host "ruten.com.tw".
16950	1415	sdo	This protocol plug-in classifies the web traffic to the host "sdo.com".
16950	1416	sina_blog	This protocol plug-in classifies the web traffic to the host "blog.sina.com.cn".
16950	1417	sina_finance	This protocol plug-in classifies the web traffic to the host "finance.sina.com.cn".
16950	1418	sina_news	This protocol plug-in classifies the web traffic to the host "news.sina.com.cn".
16950	1419	soft4fun	This protocol plug-in classifies the web traffic to the host "ifree.soft4fun.net".
16950	1420	sohu_blog	This protocol plug-in classifies the web traffic to the host "blog.sohu.com".
16950	1421	stockq	This protocol plug-in classifies the web traffic to the host "stockq.org".
16950	1422	suning	This protocol plug-in classifies the web traffic to the host "suning.com".
16950	1423	taiwanlottery	This protocol plug-in classifies the web traffic to the host "taiwanlottery.com.tw".
16950	1424	tencent	This protocol plug-in classifies the web traffic to the host "tencent.com".
16950	1425	tgbus	This protocol plug-in classifies the web traffic to the host "tgbus.com".
16950	1426	udn	This protocol plug-in classifies the web traffic to the host "udn.com".
16950	1427	wallstreetjournal_china	This protocol plug-in classifies the web traffic to the host "cn.wsj.com".
16950	1428	wandoujia	This protocol plug-in classifies the web traffic to the host "wandoujia.com".
16950	1429	wretch	This protocol plug-in classifies the web traffic to the host "wretch.cc".

RT#	Proto ID	Protocol	Description
16950	1430	xiami	This protocol plug-in classifies the web traffic to the host "xiami.com".
16950	1431	xuite	This protocol plug-in classifies the web traffic to the host "xuite.net".
16950	1432	yahoo_buy	This protocol plug-in classifies the web traffic to the host "buy.yahoo.com.tw".
16950	1433	yahoo_stock_tw	This protocol plug-in classifies the web traffic to the host "tw.stock.yahoo.com".
16950	1434	yam	This protocol plug-in classifies the web traffic to the host "yam.com".
16950	1435	yihaodian	This protocol plug-in classifies the web traffic to the host "yihaodian.com".
16950	1436	yoka	This protocol plug-in classifies the web traffic to the host "yoka.com".

40.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

40.3. Attributes

This section describes the attribute updates.

40.3.1. New event attributes added in this version

The following event attributes have been added in this version.

40.3.1.1. Generic events added in this version

No new generic events have been added in this version.

40.3.1.2. Events added in this version

There's no added attribute for this version.

40.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

40.3.3. Event attributes modified in this version

There's not attribute updates in this version.

40.4. Bugs fixed and known issues

40.4.1. Bugs fixed in this version

There's no bug fixed in this version.

40.4.2. Known issues

There's no known issue raised in this version.

41. Protocol Bundle 1.7.0

41.1. What's new in the Protocol Bundle 1.7.0

41.1.1. Note about the major enhancements of the release

41.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release:

- `mega`, the new Kim Dotcom’s file sharing service. The classification handles the administrations stream and the upload/download streams classifications.
- `mitalk - known as Miliao`, `kik`, `wechat` and `youni` which are Chinese instant messaging services.
- `poco`, a chinese webportal.

Attributes have been added in this release for the following protocols:

- `ldap`: names extraction (RFC2511) and `CLDAP` support (`LDAP` over `UDP`).
- `mapi`: full extract support.
- `icmp6`: support of IPv6 Network Discovery Protocol and IPv6 metadata
- ospf : authentication metadata added
- `smb`: new file-related metadata added.

The following protocols have been updated in this release:

- `yahoo`: classification improvement.
- `aim_express`, `gmail_chat`, `pricerunner`, `ymail` and `youtube` have been updated.

41.1.1.2. Others features and enhancements

41.1.1.2.1. Video and image metadata extraction

Among all the several improvements of the release, this Protocol Bundle brings an advanced video and image metadata extractions from HTTP streams from or to mobile device. The image and video metadata items which support extraction are:

- Advanced support for bmff container/MPEG4 on youtube and ustream,
- Generic MP4/h264 support (video_type=bmff),
- 3GP/3GP2 video support (video_type=bmff),
- FLV video support (video_type=flv),
- Adobe Live Streaming (HLS) support (video_type=hls),
- Metadata extraction from GIF, PNG, JPEG,

- Download support on iOS, Android and Windows Phone,
- Upload support on iOS.

Note:

bmff:brand and bmff:uuid are now referenced as Multi Protocol Attributes (MPA).

Video metadata are now extracted only under http:request:video attributes. The extraction from bmff plug-in over a multimedia streaming protocol like Youtube or Netflix is deprecated.

41.1.1.2.2. JSON parser for PDL

The PDL JSON parser has been enhanced and simplified. Thanks to this new parser implementation, the protocol plugin `yandex_webmail` has been rewritten and new metadata items have been added in `niconico_douga`.

41.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

41.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

41.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP

- This version has been validated on LSB (Linux Standard Base) 3.x

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

41.2. Protocol updates

41.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 92. New protocols added in this version

RT#	Proto ID	Protocol	Description
16315	1294	yahoo	Yahoo is a pseudo-protocol which classifies generic web services related to Yahoo.
16447	1295	kik	KIK Messenger is a Chinese Instant Messaging service.
16673	1299	mega	This protocol plug-in classifies the web traffic to the host "mega.co.nz", or associated to the SSL Common Name "mega.co.nz".
16394	1298	mitalk	MiTalk (aka Miliao) is a mobile instant messaging application from Xiaomi Tech.
11923	1300	poco	Poco is a Chinese webportal, which allow users to share pictures, chat, exchange files, etc.
16267	1296	wechat	WeChat is a text and voice messaging application for mobile.
16446	1297	youni	Youni SMS is a totally free mobile messaging application.

41.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

41.2.3. Other features

RT#	Description
16514	[ulayer_store] last hashtable-to-ulayer_store conversions
16643	SF5733: [radius] make multiplexing tunable
16644	[PDL] add support for nested statemachines

41.2.4. Protocol Updates

- 15781

  [youtube] login workflow is over SSL we can't extract account, login and password attributs

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16236

  [pricerunner] Protocol update

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Extraction of pricerunner attributes

- 16238

  [gmail_chat] Protocol update

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Support of gmail_chat

- 16315

  [ymail] Improve classification for new ymail version

Bug Info	Description
Reported against	ProtocolBundle 1.5.1,ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Classification issues due to a new version of Yahoo.

41.3. Attributes

This section describes the attribute updates.

41.3.1. New event attributes added in this version

The following event attributes have been added in this version.

41.3.1.1. Generic events added in this version

No new generic events have been added in this version.

41.3.1.2. Events added in this version

The following events have been added in this version:

Note:

Only non-generic event attributes are mentioned in this section. See the Qosmos ixEngine Protobook for details of generic events available for all protocols.

Table 93. New event attributes in this version

Protocol	New event attributes
bmff	video_brand
bmff	video_type
bmff	video_uuid
http	accept_encoding
http	audio_datarate
http	content_encoding
http	image
http	image_alpha_channel
http	image_height
http	image_index_color
http	image_type
http	image_width
http	start_time
http	total_datarate
http	video
http	video_avgdatarate
http	video_brand
http	video_datarate
http	video_duration
http	video_framerate
http	video_height
http	video_type
http	video_url
http	video_width
icmp6	end
icmp6	link_layer_addr
icmp6	link_layer_addr_type

Protocol	New event attributes
icmp6	link_layer_eui64_addr
icmp6	link_layer_mac_addr
icmp6	link_layer_raw_addr
icmp6	ndp_prefix
icmp6	prefix
icmp6	prefix_len
icmp6	target_address
ldap	name
mapi	action
mapi	appointment_location
mapi	attach
mapi	attach_content
mapi	attach_filename
mapi	attach_id
mapi	attach_size
mapi	contact_alias
mapi	contact_email
mapi	contact_entry
mapi	content
mapi	date
mapi	email
mapi	email_type
mapi	end
mapi	flags
mapi	importance
mapi	msglist_date
mapi	msglist_entry
mapi	msglist_flags
mapi	msglist_importance
mapi	msglist_msgid
mapi	msglist_receiver
mapi	msglist_receiver_email
mapi	msglist_receiver_entry
mapi	msglist_receiver_type
mapi	msglist_sender
mapi	msglist_sender_entry
mapi	msglist_sensivity
mapi	msglist_size
mapi	msglist_subject
mapi	receiver
mapi	receiver_alias
mapi	receiver_email
mapi	receiver_entry
mapi	receiver_type
mapi	sender

Protocol	New event attributes
mapi	sender_alias
mapi	sender_email
mapi	sender_entry
mapi	sensivity
mapi	size
mapi	subject
niconico_douga	account
niconico_douga	date
niconico_douga	description
niconico_douga	end
niconico_douga	login
niconico_douga	nickname
niconico_douga	query
niconico_douga	query_raw
niconico_douga	query_text
niconico_douga	tag
niconico_douga	title
niconico_douga	video
niconico_douga	video_duration
niconico_douga	videoid
ospf	auth_data
smb	attributes
smb	command_string
smb	dialect
smb	dialect_index
smb	dialect_name
smb	ext_attributes
smb	file
smb	file_chunk_len
smb	information_level
smb	native_lan_manager
smb	path
smb	search_attributes
smb	search_pattern
smb	search_storage_type
ssl	handshake_type

41.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 94. Deprecated event attributes

Protocol	Deprecated event attributes	Comments
bmff	brand	This attribute is now extracted from `http` protocol.

Protocol	Deprecated event attributes	Comments
bmff	uuid	This attribute is now extracted from `http` protocol.
http	returnmsg	This attribute has the same content as `Q_HTTP_CODE`.
http	urilast64	This attribute should be computed from `Q_HTTP_URI` in customer app.
http	urilen	This attribute should be computed from `Q_HTTP_URI` in customer app.
http	urimd5	This attribute should be computed from `Q_HTTP_URI` in customer app.
tcp	client_os	The socket usage behavior is no more relevant to identify the client OS.
youtube	bytelength	Obsolete due to the new video and image metadata extractions from HTTP streams.

41.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 95. Event attributes modified

Protocol	Event attribute	Changes
bmff	video_height	in p_1_6_0-20 [uint16,server,session_prt,video] in p_1_7_0-10 [uint32,server,session_prt,video]
bmff	video_width	in p_1_6_0-20 [uint16,server,session_prt,video] in p_1_7_0-10 [uint32,server,session_prt,video]
smb	filename	in p_1_6_0-20 [string,client,session_mod,request] in p_1_7_0-10 [string,client,session_mod,file]

Protocol	Event attribute	Changes
smb	filesize	in p_1_6_0-20 [uint32,client,session_mod,request] in p_1_7_0-10 [uint64,client,session_mod,file]
yandex_webmail	msglist_folder	in p_1_6_0-20 [string,both,session_mod,no_parent] in p_1_7_0-10 [string,both,session_mod,msglist_entry]

41.4. Bug fixed and known issues

41.4.1. Bugs fixed in this version

- 16272

  [SF5551] [TCP / Doc] - tcp:client_os should be set as deprecated

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Other anomaly
Expected versus actual behavior	Switch the tcp:client_os to deprecated

- 16428

  [smb] information_level attribute is not always extracted

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The information_level attribute is sometimes not extracted.

- 16509

  [SF5726][Linkedin] Wrong receiver extraction

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The extraction of the receiver attribute (protocol Linkedin) is sometimes wrong.

- 16513

  [SF5727] [Rambler_Webmail] bugs on email extraction

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Senders and receivers are inverted: senders are extracted as receivers and receivers are extracted as senders.

- 16551

  [bmff] attributes extraction on http status 206

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Extracting BMFF metadata on HTTP returns status code 206: "Partial Content".

- 16625

[paltalk] deadlock in timeout callbacks

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Crash
Expected versus actual behavior	Paltalk protocol may induce a dead lock in SMP mode.

- 16638

[SF5399] [Yandex_Webmail] Wrong Extractions

Bug Info	Description
Reported against	ProtocolBundle 1.5.1,ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Wrong behavior : msglist_folder should be available for each messages, reply-to receipts are extracted as receiver, some msg_id are missing and some attach_id are missing.

41.4.2. Known issues

- 15042

[SF4490][ymsg_webmessenger] html code in chat/message

Bug Info	Description
Reported against	ProtocolBundle 1.1.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Expected behavior: get chat/message without any html code
Workaround	No workaround

- 16097

[bittorrent] Improve classification

Bug Info	Description
Reported against	ProtocolBundle 1.5.0,ProtocolBundle 1.6.0
Platform	All
Effect of bug	Classification anomaly

Bug Info	Description
Expected versus actual behavior	Bittorrent classification enhancement required to take into account specific behaviors in case of network blocking mechanism.
Workaround	No workaround

- 16575

[sf5053][sip] caller/callee inverted

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Callee and caller attributes are inverted.
Workaround	No workaround

- 16576

[sf5116][ftp] missing data_port extraction

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The ftp control connection data_port attribute is not extracted.
Workaround	No workaround

- 16632

[ldap] Extraction improvement

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Unitary extraction of ldap attributes issues.
Workaround	No workaround

- 16732

SF5815 [http] mime part extraction issue

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Extra \r\n are extracted at the end of a mime part.
Workaround	No workaround

- 16782

[krb5] Extra bytes raised

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Extra square brackets and a dot are extracted in the text64 attribute of krb5 protocol.
Workaround	No workaround

- 16792

[dcerpc] Classification issue over smb on Octeon Plus

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	OcteonPlus
Effect of bug	Classification anomaly
Expected versus actual behavior	
Workaround	No workaround

- 16796

[gmail] Classification issues on XLR

Bug Info	Description
Reported against	ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Classification regressions for the gmail plugin on XLR.
Workaround	No workaround

- 16806

SF5040: [ymail_classic] missing attach event

Bug Info	Description
Reported against	ProtocolBundle 1.5.0,ProtocolBundle 1.7.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Missing the last attachment summary after uploading several files.
Workaround	No workaround

- 16820

[ymail2] [ymail_mobile_new] classification over yahoo

Bug Info	Description
Reported against	ProtocolBundle 1.7.0

Bug Info	Description
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Classification issues on ymail depending on the server hostname.
Workaround	No workaround

42. Protocol Bundle 1.6.0

42.1. What's new in the Protocol Bundle 1.6.0

42.1.1. Note about the major enhancements of the release

42.1.1.1. New protocols, new attributes and updates

The following protocols have been added or updated in this release:

- `bmff` MPEG4 metadata extraction on streaming sites: Netflix, YouTube, Veohtv, qqstream and other video streaming websites.
- `YouTube`: updated to fit with the new website interface and rtmp support added.
- `Tor`: protocol update.
- `Badoo`, `squirrelmail` and `vkontakte`: several updates.
- `BitTorrent`: classification enhancement.
- `Dailymotion`: extraction enhancement.
- `Http`: The attribute `uri_full` contains the complete URL of the HTTP packet. A faster classification based on specific headers has been added to enhance performances.
- `SSL`: performance enhancement.
- `Radius`: new 3GPP attributes added.
- `Established`: prototune added to configure the number of packets which must be analyzed on a new session without tcp handshake prior to “established” classification.
- `LDAP`: CLDAP support added and metadata extraction enhancement.

42.1.1.2. Others features and enhancements

An avanced protection security system has been added to manage memory leaks.

42.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

42.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`

- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

42.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x

Specific high-performance platforms

- Intel DPDK 1.2.2
- Napatech 4.25H (2GD version)
- Netronome 2.5.2
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

42.2. Protocol updates

42.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 96. New protocols added in this version

RT#	Proto ID	Protocol	Description
16091	1293	bmff	The ISO Base Media File Format, as described in ISO/IEC 14496-12:2008 (MPEG-4 Part 12).

42.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

42.2.3. Other features

RT#	Description
11630	[PDL] private attributes should be typed
13557	[SF3853] [established] add proto_tune
16185	[PDL] add optimized wrappers for HTTP priv_struct stored attributes
16265	[bittorrent] allocate default shared table => make tests smoking legit
16314	[ssl] [performance] stop implicit upper classification after handshake

42.2.4. Protocol Updates

- 11551

  [gmail_basic] Only the Inbox is extract on browse boxes workflow

Bug Info	Description
Reported against	4.12.2
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 15665

  [SF5289] [TOR] No more classification due to protocol evolution

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Classification anomaly

Bug Info	Description
Expected versus actual behavior	No more classification since protocol update on ssl certificates

- 15766

  [qq] audio and video data not classified

Bug Info	Description
Reported against	ixE-4.16.1
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	

- 15785

  [google_groups] protocol update over SSL cannot be deactivated

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 15786

  [live_groups] protocol update over SSL cannot be deactivated

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16095

  [SF5480] [Badoo] - (Protocol Update) Fix extraction of messages

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Fix extraction of messages since protocol update

- 16257

  [youtube] protocol update: add classification over rtmp

Bug Info	Description
Reported against	ProtocolBundle 1.6.0

Bug Info	Description
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16328

[SF5593] [squirrelmail] [PCR Weekly] protocol Squirelmail is not classified anymore

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	squirrelmail installation directory do not impact classification anymore

- 16330

SF5596: [vkontakte] Protocol update

Bug Info	Description
Reported against	ProtocolBundle 1.5.1,ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Classification and Extraction issue with vkontakte

- 16500

[SF5731] [SMTP] - Support for RFC 3030 BDAT extension

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

42.3. Attributes

This section describes the attribute updates.

42.3.1. New event attributes added in this version

The following event attributes have been added in this version.

42.3.1.1. Generic events added in this version

No new generic events have been added in this version.

42.3.1.2. Events added in this version

The following events have been added in this version:

Note:

Only non-generic event attributes are mentioned in this section. See the Qosmos ixEngine Protobook for details of generic events available for all protocols.

Table 97. New event attributes in this version

Protocol	New event attributes
bmff	brand
bmff	end
bmff	uuid
bmff	video
bmff	video_avgdatarate
bmff	video_datarate
bmff	video_duration
bmff	video_height
bmff	video_width
cotp	tpdu_code
dailymotion	email
dns	dns_query
h245	media_control_channel_addr_v6
ldap	assertion_value
ldap	assertion_value_raw
ldap	attribute_desc
ldap	filter_expression
ldap	hostname
netflix	login
qq	callee
qq	caller
qq	service
qq_transfer	login
qq_transfer	service
radius	3gpp_sgsn_address

Protocol	New event attributes
radius	3gpp_sgsn_mcc_mnc
rdp	default_username

42.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

42.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 98. Event attributes modified

Protocol	Event attribute	Changes
bgp	error_code	in PB 1.5.1 [string_index, both, session_mod, message_entry] in PB 1.6.0 [uint8, both, session_mod, message_entry]
bgp	error_subcode	in PB 1.5.1 [string_index, both, session_mod, message_entry] in PB 1.6.0 [uint8, both, session_mod, message_entry]
dns	ancount	in PB 1.5.1 [uint32, both, session_mod, no_parent] in PB 1.6.0 [uint32, both, session_mod, dns_query]
dns	arcount	in PB 1.5.1 [uint32, both, session_mod, no_parent] in PB 1.6.0 [uint32, both, session_mod, dns_query]
dns	dns_entry	in PB 1.5.1 [parent, both, session_mod, no_parent] in PB 1.6.0 [parent, both, session_mod, dns_query]
dns	message_type	in PB 1.5.1 [string_index, both, session_mod, no_parent] in PB 1.6.0 [string_index, both, session_mod, dns_query]

Protocol	Event attribute	Changes
dns	nscount	in PB 1.5.1 [uint32, both, session_mod, no_parent] in PB 1.6.0 [uint32, both, session_mod, dns_query]
dns	qdcount	in PB 1.5.1 [uint32, both, session_mod, no_parent] in PB 1.6.0 [uint32, both, session_mod, dns_query]
dns	query	in PB 1.5.1 [string, both, session_mod, no_parent] in PB 1.6.0 [string, both, session_mod, dns_query]
dns	query_type	in PB 1.5.1 [string_index, both, session_mod, no_parent] in PB 1.6.0 [string_index, both, session_mod, dns_query]
dns	reply_code	in PB 1.5.1 [string_index, both, session_mod, no_parent] in PB 1.6.0 [string_index, both, session_mod, dns_query]
dns	response_time	in PB 1.5.1 [timeval, both, session_mod, no_parent] in PB 1.6.0 [timeval, both, session_mod, dns_query]
dns	transaction_id	in PB 1.5.1 [uint32, both, session_mod, no_parent] in PB 1.6.0 [uint32, both, session_mod, dns_query]

42.4. Bug fixed and known issues

42.4.1. Bugs fixed in this version

- 14783

  [SF4525] [SMB] - Handle Trans2 Response and Trans2 Request/FIND_FIRST2 subcommands

Bug Info	Description
Reported against	ProtocolBundle 1.2.0,ProtocolBundle 1.5.0,ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 14790

  [http] On xlr we raise many extra http request/end/header empty

Bug Info	Description
Reported against	ProtocolBundle 1.2.0
Platform	CCPU PP50
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 14885

  [SF4686] [rdp] flags on negotiation response are not supported

Bug Info	Description
Reported against	ProtocolBundle 1.2.0,ProtocolBundle 1.5.0,ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	If encryption flags are set as recommended by the specifications, the ixEngine fails to see them

- 15130

  [SDK-example] dpi-bundle returns valgrind error in process_packet func

Bug Info	Description
Reported against	ixE-4.16
Platform	All
Effect of bug	Memory leak
Expected versus actual behavior	

- 15350

  [krb5] improve extraction over rpc (AP-REP)

Bug Info	Description
Reported against	ProtocolBundle 1.4.0,ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 15613

[SF5096] [ymsg_webmessenger] message truncated

Bug Info	Description
Reported against	ixE-4.16
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 15689

[http][sf5354] same flow_id, same http_index on 2 consecutive http request, tcp port reused

Bug Info	Description
Reported against	ixm-4.14.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	http:index shall always unique for a given flow_id.

- 15752

[SF5376][ICMP]wrong value in some attributes descriptions (rtt, type, etc,.

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	The possible value in the attributes description should match with the reality.

- 15816

[SF][zimbra_standard] parent attach not set when the attach_content is extracted

Bug Info	Description
Reported against	ProtocolBundle 1.4.0,ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The parent zimbra:attach should be setwhen the zimbra:attach_content is extracted.

- 16034

[gmail_basic] wrong sender and sender_alias extraction

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16086

[SF4422][gmail_basic] email_read: wrong date and content extraction

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Expected behavior: get receivers and date extracted on Turkish version of gmail_basic

- 16092

[bgp] Q_BGP_ERROR_CODE: wrong event size

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16106

[http] Missing semicolon in http mime_type_main

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	OcteonPlus
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16144

[veohtv][octeonplus] Missing classification over UDP

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	OcteonPlus
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16156

  [qvod][radius] a qvod packet is now classified as radius

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16161

  [maktoob] Receiver/sender inversion

Bug Info	Description
Reported against	ProtocolBundle 1.5.0,ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16195

  [SDK] [C++] C++ headers compliancy

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Other anomaly
Expected versus actual behavior	

- 16240

  [pb 1.5.1][pop3]login password not extracted anymore

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16251

  SF5528: [smtp] unitary extraction issue

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	There is a false dependency between smtp:mailfrom and smtp:request

- 16253

  [t38] unitary extraction fails for some attributes

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16254

  [gnutella] unitary attributes extraction is broken

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16275

  [http] uri_full set the old behaviour

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16294

  [SF5575] [Mailru] sender attribute is not extracted when we don't request msglist_sender_entry

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16321

  SF5590: [IMAP] extraction issue on OCTEONPLUS SMP EXTFLOW

Bug Info	Description
Reported against	ixE-4.16.3,ixE-4.17
Platform	OcteonPlus
Effect of bug	Extraction anomaly

Bug Info	Description
Expected versus actual behavior	

- 16323

[SF5594] [Mailru] Not classifed over SSL

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 16332

[krb5] Unit test fails

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16353

[owa] owa_find_by_sid error

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Memory leak
Expected versus actual behavior	

- 16358

[owa] Conditional jump or move depends on uninitialised value(s)

Bug Info	Description
Reported against	ProtocolBundle 1.6.0
Platform	All
Effect of bug	Memory leak
Expected versus actual behavior	

- 16463

[SF5718][Silverlight] add classification over akamai

Bug Info	Description
Reported against	ProtocolBundle 1.5.1

Bug Info	Description
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

42.4.2. Known issues

- 15753

  [SF5374][SMB] packet_offset issue

Bug Info	Description
Reported against	ProtocolBundle 1.4.0,ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Attributes SMB not extracted and strange filename extracted.
Workaround	No workaround

- 15773

  [SF5374][SMB] filename bad values extracted - directories, strange files

Bug Info	Description
Reported against	ProtocolBundle 1.4.0,ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Attributes SMB not extracted and strange filename extracted.
Workaround	No workaround

- 16137

  [wtp] [octeonplus] Missing classification

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	OcteonPlus
Effect of bug	Classification anomaly
Expected versus actual behavior	WTP classification regression.
Workaround	No workaround

43. Protocol Bundle 1.5.1

43.1. What's new in the Protocol Bundle 1.5.1

43.1.1. Note about the major enhancements of the release

43.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release: `capwap` and `mobile_ip` (tunneling).

Protocol updates have been done on:

- `tango`: last client versions support.
- `viber`: last client versions support.
- `yandex_webmail`: support of the new web site API.
- `bittorrent`: classification enhancement.

43.1.1.2. Others features and enhancements

The release stability during HTTP session flushing has been improved.

43.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

43.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don’t have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don’t forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn’t be found by the dynamic linker when your starts.

43.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x

Specific high-performance platforms

- Intel DPDK 1.0
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

43.2. Protocol updates

43.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 99. New protocols added in this version

RT#	Proto ID	Protocol	Description
14954	1290	802_11	The 802.11 protocol is used to carry data (at MAC level) on IEEE 802.11 Wireless Local Area Networks.
14954	1289	capwap	CAPWAP stands for Control And Provisioning of Wireless Access Points. It is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points.
14954	1291	dtls	DTLS stands for Datagram Transport Layer Security protocol. It provides communications privacy for datagram protocols, and prevents eavesdropping, tampering, or message forgery.
15312	1292	mobile_ip	Mobile IP is an IETF standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.

43.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

43.2.3. Other features

RT#	Description
16199	[uwtp] add proto tune to discard duplicated packet

43.2.4. Protocol Updates

- 15801

  [SF5399] [Yandex_Webmail] Protocol Evolution

Bug Info	Description
Reported against	ProtocolBundle 1.4.0,ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

43.3. Attributes

This section describes the attribute updates.

43.3.1. New event attributes added in this version

The following event attributes have been added in this version.

43.3.1.1. Generic events added in this version

No new generic events have been added in this version.

43.3.1.2. Events added in this version

The following events have been added in this version:

Note:

Only non-generic event attributes are mentioned in this section. See the Qosmos ixEngine Protobook for details of generic events available for all protocols.

Table 100. New event attributes in this version

Protocol	New event attributes
yandex_webmail	attach_id

43.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

43.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 101. Event attributes modified

Protocol	Event attribute	Changes
ftp	filename	in PB 1.5.0 [string,server,session_mod,no_parent] in PB 1.5.1 [string,both,session_mod,no_parent]
ftp	loadway	in PB 1.5.0 [string,server,session_mod,no_parent] in PB 1.5.1 [string,both,session_mod,no_parent]
yandex_webmail	action	in PB 1.5.0 [string,both,session_prt,email] in PB 1.5.1 [string,both,session_mod,email]
yandex_webmail	attach_type	in PB 1.5.0 [string,both,session_prt,attach] in PB 1.5.1 [string,both,session_mod,attach]
yandex_webmail	content	in PB 1.5.0 [string,both,session_mod,email] in PB 1.5.1 [buffer,both,session_mod,email]
yandex_webmail	date	in PB 1.5.0 [string,both,session_prt,email] in PB 1.5.1 [string,both,session_mod,email]
yandex_webmail	draft	in PB 1.5.0 [uint32,both,session_prt,email] in PB 1.5.1 [uint32,both,session_mod,email]
yandex_webmail	msg_id	in PB 1.5.0 [string,both,session_prt,email] in PB 1.5.1 [string,both,session_mod,email]
yandex_webmail	msglist_date	in PB 1.5.0 [string,both,session_prt,msglist_entry] in PB 1.5.1 [string,both,session_mod,msglist_entry]
yandex_webmail	msglist_msgid	in PB 1.5.0 [string,both,session_prt,msglist_entry] in PB 1.5.1 [string,both,session_mod,msglist_entry]
yandex_webmail	msglist_sender_entry	in PB 1.5.0 [parent,both,session_prt,msglist_entry] in PB 1.5.1 [parent,both,session_mod,msglist_entry]
yandex_webmail	msglist_subject	in PB 1.5.0 [string,both,session_prt,msglist_entry] in PB 1.5.1 [string,both,session_mod,msglist_entry]
yandex_webmail	msglist_unread	in PB 1.5.0 [uint32,both,session_prt,msglist_entry] in PB 1.5.1 [uint32,both,session_mod,msglist_entry]
yandex_webmail	receiver_type	in PB 1.5.0 [string,both,session_prt,receiver_entry] in PB 1.5.1 [string,both,session_mod,receiver_entry]
yandex_webmail	sender_entry	in PB 1.5.0 [parent,both,session_prt,email] in PB 1.5.1 [parent,both,session_mod,email]

43.4. Bug fixed and known issues

43.4.1. Bugs fixed in this version

- 15400

  SF5118: [FTP] Filename extraction issue

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	If the FTP data transfer begins before the 150 accept code reply from the server, the filename will be reported after the transfer starts

- 15642

  [SF5335] [ymail2] [HTTP] ymail2:attach_content missing because http:content_len not extracted

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 15790

  [SF5169][youtube] videoid attribute is not extracted

Bug Info	Description
Reported against	ProtocolBundle 1.4.0,ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 15816

  [SF][zimbra_standard] parent attach not set when the attach_content is extracted

Bug Info	Description
Reported against	ProtocolBundle 1.4.0,ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The parent zimbra:attach should be setwhen the zimbra:attach_content is extracted.

- 15904

  [SF5461][Facebook] - No extraction of comments

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Add extraction of comments

- 15911

[SF5448] [ymail2] contact_name attribute is extracted with some json codes

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16022

SF5452: [MMSE] Extraction issue

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	If the MMS version is 1.3, nothing is extracted while we could

- 16036

[SF5414] [Facebook] - No extraction of share_text/share_with

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Fix facebook:share_with and facebook:share_text attributes extraction

- 16136

[SF5506][bloomberg] Enhancing classification

Bug Info	Description
Reported against	4.14.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 16160

[http] priv is null

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Crash
Expected versus actual behavior	SegFault on __http_priv access.

- 16251

SF5528: [smtp] unitary extraction issue

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	There is a false dependency between smtp:mailfrom and smtp:request

43.4.2. Known issues

- 14885

SF4686: [RDP] Flags on negotiation response are not supported

Bug Info	Description
Reported against	ProtocolBundle 1.2.0,ProtocolBundle 1.5.0,ProtocolBundle 1.5.1
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	If encryption flags are set as recommended by the specifications, the ixEngine fails to see them
Workaround	No workaround

44. Protocol Bundle 1.5.0

44.1. What's new in the Protocol Bundle 1.5.0

44.1.1. Note about the major enhancements of the release

44.1.1.1. New protocols, new attributes and updates

The following protocols have been added in this release:

- Partial support of `everquest` (video game)
- `lineage2` (video game)
- `jajah` (IM/video-conference)
- `zynga` (online video game)

New Content Delivery Network (CDN) for web services: `akamai`, `level3`, `llnwd` and `windows_azure`.

Updates on the HTTP/HTTPS uppers protocols: `windowslive`, `showmypc`, `sportsillustrated`, `the_auteurs`, `tumblr`, `usejump`, `xm_radio`, `yahoo_realestate`, `yammer`, `three`, `seoul_news` and `yahoo_korea`.

Protocol updates:

- `bittorrent/utp`: classification enhancement of the workaround strategies.
- `paltalk`: classification added on mobile phones.
- `skype`: chat/MSN classifications added.
- `bbc_player`: iPhone support added.
- `whatsapp` and `odnoklassniki` have been updated.
- `twitter`: the extraction from the HTTP twitter interface has been added.

New attributes haves been added in this release:

- `bing`: itinary metadata extraction.
- `twitter`: attributes added for attached items correlation (from the legacy twitter API).
- `rdp`: username and return code extraction.
- `netflix`: QoE metadata extraction.

44.1.1.2. Others features and enhancements

The following stress tests have been added on our validation procedures:

- Random test on dynamic memory allocation errors,

- Enforced data corruption on network flows.

The performances of this release has been improved:

- Memory allocation improvment for the HTTP statemachine.
- Packets processing enhancements on `msn` and `gizmo`.

44.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

44.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

44.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x

Specific high-performance platforms

- Intel DPDK 1.0
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6

- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

44.2. Protocol updates

44.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 102. New protocols added in this version

RT#	Proto ID	Protocol	Description
12029	1284	akamai	This protocol plug-in classifies the web traffic to the hosts "akamai.net", "akamaihd.net", "akamaiedge.net", "edgesuite.net", "edgekey.net" and "srip.net", or associated to the SSL Common Names "akamai.net" and "akamaihd.net".
12022	1282	everquest	Everquest is a 3D fantasy massively multiplayer online role-playing game (MMORPG), for Windows platforms, developed by Sony Online Entertainment(SOE).
12029	1280	facebook_apps	Facebook Applications.
14288	1281	jajah	Jajah is a VoIP provider owned by Telefonica Europe.
12029	1287	level3	This protocol plug-in classifies the web traffic to the hosts "l3.net", "level3.net" and "level3.com".
12020	1283	lineage2	Lineage2 is a MMORPG developed by NCSoft.
12029	1286	llnwd	This protocol plug-in classifies the web traffic to the host "llnwd.net".
14310	1288	windows_azure	This protocol plug-in classifies the web traffic associated to the SSL Common Name "msecnd.net".
12029	1285	zynga	This protocol plug-in classifies the web traffic to the host "zynga.com".

44.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

44.2.3. Other features

RT#	Description
14735	[bittorrent] store IP-ports couples in a shared memory rather than in a per thread hashtable
14875	[SF4568] [bittorrent] [backport] better dht
15741	[Memory NULL pointer protection] Check every pointer assignement in classification functions
15742	[Internal code review] Classification code for each protocol

RT#	Description
15747	[Enhance coding rule] Protocol Factory : Never trust a data read from the network. Review existing code

44.2.4. Protocol Updates

- 15218

  [utp][bittorrent][backport]: add addr/port of utp session (SYN type only) in l3l4 cache to classify bittorrent

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 15238

  [SF4997] [twitter] protocol update

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

44.3. Attributes

This section describes the attribute updates.

44.3.1. New event attributes added in this version

The following event attributes have been added in this version.

44.3.1.1. Generic events added in this version

No new generic events have been added in this version.

44.3.1.2. Events added in this version

The following events have been added in this version:

Note:

Only non-generic event attributes are mentioned in this section. See the Qosmos ixEngine Protobook for details of generic events available for all protocols.

Table 103. New event attributes in this version

Protocol	New event attributes
facebook_apps	application
facebook_apps	application_action
facebook_apps	application_name
facebook_apps	end
facebook_mail	attach_size
facebook_mail	attach_type
facebook_mail	session_id
ftp	transfer_duration
gmail_basic	date
netflix	date
netflix	description
netflix	end
netflix	title
netflix	video
netflix	video_duration
netflix	videoid
twitter	date
twitter	media_url

44.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

44.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 104. Event attributes modified

Protocol	Event attribute	Changes
bing	encoding	in PB 1.4.0 [string,client,session_mod,no_parent] in PB 1.5.0 [string,both,session_mod,no_parent]
bing	query	in PB 1.4.0 [parent,client,session_mod,no_parent] in PB 1.5.0 [parent,both,session_mod,no_parent]
bing	query_index	in PB 1.4.0 [uint32,client,session_prt,query] in PB 1.5.0 [uint32,both,session_mod,query]
bing	query_raw	in PB 1.4.0 [string,client,session_prt,query] in PB 1.5.0 [string,both,session_mod,query]
bing	query_text	in PB 1.4.0 [string,client,session_prt,query] in PB 1.5.0 [string,both,session_mod,query]
bing	query_type	in PB 1.4.0 [string,client,session_prt,query] in PB 1.5.0 [string,both,session_mod,query]
diameter	acct_input_octets	in PB 1.4.0 [,both,session_mod,request] in PB 1.5.0 [int64,both,session_mod,request]
diameter	acct_output_octets	in PB 1.4.0 [,both,session_mod,request] in PB 1.5.0 [int64,both,session_mod,request]
diameter	acct_sub_session_id	in PB 1.4.0 [,both,session_mod,request] in PB 1.5.0 [int64,both,session_mod,request]
kakaotalk	login	in PB 1.4.0 [,both,session_mod,no_parent] in PB 1.5.0 [int64,both,session_mod,no_parent]
perfspot	account	in PB 1.4.0 [parent,client,session_fix,no_parent] in PB 1.5.0 [parent,both,session_mod,no_parent]
perfspot	is_mobile_service	in PB 1.4.0 [uint32,client,session_fix,no_parent] in PB 1.5.0 [uint32,both,session_mod,no_parent]
perfspot	login	in PB 1.4.0 [string,client,session_prt,account] in PB 1.5.0 [string,both,session_mod,account]
perfspot	password	in PB 1.4.0 [string,client,session_prt,account] in PB 1.5.0 [string,both,session_mod,account]

44.4. Bug fixed and known issues

44.4.1. Bugs fixed in this version

- 13197

  SF3816 : [WTP] false positive (should be RTP)

Bug Info	Description
Reported against	4.15.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	False positive with WSP.

- 14232

  SF4240 - [smb] Real Unicode file names are not supported

Bug Info	Description
Reported against	ProtocolBundle 1.0.0,ProtocolBundle 1.1.0,ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The extraction of file names with special characters stops right after the first one encountered.

- 14570

  SF4196 - [bittorrent] [backport] classification issue

Bug Info	Description
Reported against	ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	In some cases, the tracker's announce is not classified as bittorrent and peer's extraction fails

- 14571

  [SF4422][gmail_basic] email_read, TO & date are missing

Bug Info	Description
Reported against	ProtocolBundle 1.1.0,ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Expected behavior: get receivers and date extracted on Turkish version of gmail_basic

- 14710

  [SF4501] [rambler_webmail] - statemachine_anomaly, no content extracted

Bug Info	Description
Reported against	ProtocolBundle 1.2.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	missing some mail content due to a statemachine anomaly

- 14723

SF3857 : [DNS] Set the right half-session's type based on packet's information

Bug Info	Description
Reported against	ProtocolBundle 1.2.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	expected, server and client packect should not be inverted.

- 14726

[SF4494] [Wikipedia] - No extraction on some queries

Bug Info	Description
Reported against	ProtocolBundle 1.2.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Missing extraction of automated proposed queries

- 15017

[smb] native_os attribute

Bug Info	Description
Reported against	ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The attribute native_os is not raised.

- 15171

[bittorrent] [backport] update peer table from ping request

Bug Info	Description
Reported against	PRotocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Address gathering feature must be integrated in the release to classify obfuscated sessions.

- 15222

[SF5003][POP3] extraction issue

Bug Info	Description
Reported against	ProtocolBundle 1.0.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	If the message header doesn't start with: * Received * Return-Path * Message-ID * Authentication-Results * X-Originating-IP * X-Apparently-To * MIME-Version We will miss some field's extraction

- 15273

[SF4272] [gmail_mobile] subject not decoded

Bug Info	Description
Reported against	ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	subject is extacted from uri but is not decoded.

- 15289

SF5017: [Gnutella] Classification regression

Bug Info	Description
Reported against	ProtocolBundle 1.2.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Gnutella isn't correctly classified over HTTP when using BearShare

- 15298

[SF4272] [gmail_mobile] remove = char from email_index

Bug Info	Description
Reported against	ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	unexpected = char is extracted in email_index attribute

- 15331

[SF5091][facebook_mail] email content extraction failure

Bug Info	Description
Reported against	PRotocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	If the message content is the first field of the HTTP content, the extraction of facebook_mail:content will fail.

- 15332

[SF4771] Wrong SSL classification

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

- 15408

[SF4996][Youtube] Attribute description not extracted.

Bug Info	Description
Reported against	ProtocolBundle 1.1.0
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	The attribute description should be extracted.

- 15435

[SF5220] [sina_weibo] - Missing classification

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Add sina_weibo classification over api.weibo.cn http server

- 15533

[SF5170] [gmail_basic] - Change http uri used to classify gmail_basic

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Match /mail/u/0/h instead of /mail/h to classify gmail_basic

- 15553

[SF5305] [http] charset extracted in mime_type

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	If the charset has a colon instead of an equal sign after it, it will be extracted in mime_type

- 15612

  [h245] Wrong event size (add_sz instead of add)

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	

- 15682

  [SF5018] [sip] line classification is too permissive

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Line's classification over SIP is too permissive and some SIP flows may end up being classified as Line.

- 15813

  [SF5019] [RADIUS] - No classification due to unknown radius attributes

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Classify radius protocol even if there are some unknown attributes in request message

- 15828

  SF5040: [ymail_classic] missing attach event

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Missing the last attachment summary after uploading several files.

- 15833

  SF5015: [telnet] classification issue

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	

44.4.2. Known issues

- 14783

  [SF4525] [SMB] - Handle Trans2 Response and Trans2 Request/FIND_FIRST2 subcommands

Bug Info	Description
Reported against	ProtocolBundle 1.2.0,ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	
Workaround	No workaround

- 14885

  SF4686: [RDP] Flags on negotiation response are not supported

Bug Info	Description
Reported against	ProtocolBundle 1.2.0,ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	If encryption flags are set as recommended by the specifications, the ixEngine fails to see them
Workaround	No workaround

- 15019

  [smb] filesize attribute limitation

Bug Info	Description
Reported against	ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Only one file transfer is processed at any one time.
Workaround	No workaround

- 15042

  [SF4490][ymsg_webmessenger] html code in chat/message

Bug Info	Description
Reported against	ProtocolBundle 1.1.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Expected behavior: get chat/message without any html code
Workaround	No workaround

- 15068

  [smb] smb 2.0 query_id is wrong

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The smb query_id attribute is extracted from Command Sequence Number which in some cases is negative.
Workaround	No workaround

- 15400

SF5118: [FTP] Filename extraction issue

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	If the FTP data transfer begins before the 150 accept code reply from the server, the filename will be reported after the transfer starts
Workaround	No workaround

- 15832

SF5015: [telnet] classification issue

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	
Workaround	No workaround

- 15977

[gmail_basic]pdl statemachine generation bug

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	
Workaround	No workaround

- 16100

[pdl] fix debug mode

Bug Info	Description
Reported against	ProtocolBundle 1.5.0
Platform	All
Effect of bug	Extraction anomaly

Bug Info	Description
Expected versus actual behavior	
Workaround	No workaround

- 16160

[http] priv is null

Bug Info	Description
Reported against	ProtocolBundle 1.5.1
Platform	All
Effect of bug	Crash
Expected versus actual behavior	SegFault on __http_priv access.
Workaround	No workaround

45. Protocol Bundle 1.4.0

45.1. What's new in the Protocol Bundle 1.4.0

45.1.1. Note about the major enhancements of the release

45.1.1.1. New protocols, new attributes and updates

Kakaotalk, a Voip protocol on mobiles and Blubster, a peer-to-peer protocol have been included in this release.

Hostname or common name has been changed for protocols bolt, box_net, campfire, epernicus, fetlife, fly_proxy, hovrs, mog, abcnews, acrobat, americainexpress, capitalone, monster, lintasberita and kb_bank.

New classification of audio/video rtmp flows (Adobe Flash technology) for the protocols blip_tv, cnet_tv, iheartradio, mogulus, slacker, vevo and yahoo_screen.

Metadatas extraction on FLV videos have been added for Youtube.

The folowing protocols have been also updated:

- OpenVPN: better support over HTTPS.
- tns: major update to support last Oracle server versions.
- facebook and facebook_mail: support added on mobiles (web and application modes) and update of the Facebook CDN support.

45.1.1.2. Others features

Several features have been implemented on this release:

- eDonkey:classification enhancement based on session prediction (edonkey peers cache).
- Krb5: classification enhancement upper dcercp, dns, ldap and smb.
- BitTorrent: global classification enhancement of utp/BitTorrent.

The peformance has been improved for this release on the following features:

- "Inconclusive protocols": performance enhancement for the classification upper utp and stun.
- IPv4/IPv6 defragmentation lock management has been improved.

45.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

45.1.3. Installation procedure

This protocol bundle can be directly included in your ixEngine or loaded via the hot swap capabilities.

- To integrate this protocol bundle inside your application without hot swap usage, your application must be linked with the libqmprotocols which will become the default bundle of the ixEngine. In example: `gcc user_application.c -L. -lqmengine -lqmprotocols -o application`
- If you plan to use the hot swap API brought by the SPLIT project, you don't have to link your application with a libqmprotocols. For example: `gcc user_application.c -L. -lqmengine -o application`

Note:

Don't forget to specify the locations of the libqmprotocols and libqmengine in the `LD_LIBRARY_PATH` otherwise these libraries shouldn't be found by the dynamic linker when your starts.

45.1.4. Supported platforms

This version has been validated on the following hardware platforms:

Linux x86 prevalidated versions

The following x86 platforms have been validated on this version:

- x86 32-bit User mode LSB monothread
- x86 64-bit User mode LSB monothread
- x86 32-bit User mode LSB SMP
- x86 64-bit User mode LSB SMP
- This version has been validated on LSB (Linux Standard Base) 3.x

Specific high-performance platforms

- Intel DPDK 1.0
- CCPU PP50 based on dual XLR 700 Processor Series - SDK version 1.6
- Broadcom XLP Processor Family - SDK version 2.2.3
- Cavium OCTEON Plus CN58XX - SDK version 1.7.1
- Cavium OCTEON II CN68XX - SDK version 2.3
- Tilera Multicore Development Environment (MDE) version 3.0.0

45.2. Protocol updates

45.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 105. New protocols added in this version

RT#	Proto ID	Protocol	Description
11859	1279	blubster	Blubster is a peer-to-peer music file sharing software. Blubster uses the manolito protocol, therefore part of its traffic is classified as manolito.
13646	1186	kakaotalk	KakaoTalk is an instant messenging platform for mobile devices; users or group of users can send messages, share photos, videos and contact information.

45.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

45.2.3. Other features

RT#	Description
14383	SF4282 [Youtube] upload method with json
14643	[FLV] provide a FLV file parser module for video streaming plug-ins
15217	SF4549 - [OpenVPN] support of openvpn over https

45.2.4. Protocol Updates

- 13804

  SF3990 - [krb5] Need support over ldap

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	Add suport of Kerberos over ldap

- 13805

  [krb5] Need support on top of dcerpc

Bug Info	Description
Reported against	ProtocolBundle 1.3.0

Bug Info	Description
Module	ixE: LibAFC
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	

- 13807

SF3992 - [krb5] add kerberos classification over smb

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Not applicable
Expected versus actual behavior	add kerberos classification over smb

- 14649

SF4385 - [facebook] support third party CDN - second pass

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Module	ixProtocols
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Expected behavior: Facebook should be up-to-date with third party CDN Actual behavior: Facebook isn't up-to-date with third party CDN

45.3. Attributes

This section describes the attribute updates.

45.3.1. New event attributes added in this version

The following event attributes have been added in this version.

45.3.1.1. Generic events added in this version

No new generic events have been added in this version.

45.3.1.2. Events added in this version

The following events have been added in this version:

Note:

Only non-generic event attributes are mentioned in this section. See the Qosmos ixEngine Protobook for details of generic events available for all protocols.

Table 106. New event attributes in this version

Protocol	New event attributes
kakaotalk	end
kakaotalk	file_chunk
kakaotalk	filename
kakaotalk	login
kakaotalk	mime_type
kakaotalk	request
smb	krb5_blob
smb	krb5_blob_len
yandex_webmail	folderlist
yandex_webmail	folderlist_item
yandex_webmail	folderlist_item_id
yandex_webmail	folderlist_item_name
youtube	audio_datarate
youtube	bytelength
youtube	start_time
youtube	total_datarate
youtube	video_datarate
youtube	video_duration
youtube	video_framerate
youtube	video_height
youtube	video_totalduration
youtube	video_width

45.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

45.3.3. Event attributes modified in this version

The following event attributes have been modified in this version.

Note:

The format of the changes mentioned in the following table is [data_type, cnx_type, session_scope, parent] with:

- data_type is the type of data of the attribute (string, integer...)
- cnx_type is the "way" of extraction (from the server, from the client or in both way)
- session_scope gives information on how the value is set. The different values are:
  - pkt: the attribute changes in each packet
  - session_mod: the attribute value is set for the whole session but may change
  - session_fix: the attribute value is fixed for the whole session
  - session_prt: the attribute value is fixed in the parent, but can change in the session
- parent is the parent attribute

Table 107. Event attributes modified

Protocol	Event attribute	Changes
ldap	message_id	in p_1_3_0-20 [uint32,both,session_mod,no_parent] in p_1_4_0-10 [uint32,both,session_mod,element]
ldap	message_type	in p_1_3_0-20 [string,both,session_mod,no_parent] in p_1_4_0-10 [string,both,session_mod,element]
ldap	payload_is_crypted	in p_1_3_0-20 [uint32,both,session_mod,no_parent] in p_1_4_0-10 [uint32,both,session_mod,element]
ldap	seal_algo	in p_1_3_0-20 [string,both,session_mod,no_parent] in p_1_4_0-10 [string,both,session_mod,element]

45.4. Bug fixed and known issues

45.4.1. Bugs fixed in this version

- 11240

  [SF3023] [live_hotmail] email not extracted when the preview message is enabled

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	We should extractt email metadata/data when the preview message is enabled.

- 12932

  [SF3695] [gmail_mobile] problem with msglist_receiver_alias

Bug Info	Description
Reported against	4.13.1,ProtocolBundle 1.1.0,ProtocolBundle 1.2.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Gmail Mobile plugins msglist_receiver_alias is not properly extracted.

- 13568

  [SF3944][yandex_webmail] issue with the msglist_folder

Bug Info	Description
Reported against	4.13.1
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Folder list should be extracted under folderlist parent. On "message-nearest" and "message-thread-nearest" (which is a view of all email about the same thread) yandex_webmail request pages should be supported (message list is extracted). msglist_folder should be extracted once.

- 14227

  [SF4251][YMAIL_CLASSIC] contact_entry and receiver type for BCC and CC not extracted

Bug Info	Description
Reported against	4.15.0
Module	ixProtocols

Bug Info	Description
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	contact_entry and receiver type for BCC and CC not extracted.

- 14598

  SF4404 - [myspace] query not extracted

Bug Info	Description
Reported against	ProtocolBundle 1.1.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	MySpace was updated : queries couldn't be extracted.

- 14755

  SF4528 [ymsg] [sip/rtp] inheritance issue in a Yahoo Messenger workflow

Bug Info	Description
Reported against	ProtocolBundle 1.0.0,ProtocolBundle 1.2.0,ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The SIP/RTP inheritance doesn't work although correlation keys are present and extracted

- 14800

  SF4560 - [tns] plug-in update to support last Oracle versions

Bug Info	Description
Reported against	ProtocolBundle 1.2.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Unexpected ^A char are added in the query output.

- 14812

  [SF4589] [facebook] - No extraction on sent messages on POST

Bug Info	Description
Reported against	ProtocolBundle 1.2.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Need to extract facebook sent messages in POST (client to server way).

- 14874

[skydrive] Classification issues

Bug Info	Description
Reported against	ProtocolBundle 1.1.0,ProtocolBundle 1.2.0
Module	ixEngine
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Classification issues mainly raised on the apps for smartphone. Some flows previously classified as windows_live are also now classified as skydrive.

- 14884

[krb5] need to declassify krb5

Bug Info	Description
Reported against	ProtocolBundle 1.2.0
Module	ixEngine
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	The protocol krb5 was not declassified over smb so after classification we were missing some others protocols later on.

- 14900

[SF4750] [live_hotmail] attribute live_hotmail:action not raised during an upload.

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Attribute action should be raised during an upload.

- 14934

[SF4780] [smtp] garbage at the beginning of the attach_content and attach_content_decoded

Bug Info	Description
Reported against	ProtocolBundle 1.2.0,ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	attribute attach_content and attach_content_decoded should contain only the data file, not anymore.

- 14950

[SF3546] [gmail] draft and saved_mode extract bug

Bug Info	Description
Reported against	4.15.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The manual save after the send action is suspicious.

- 14969

[SF4829][gmail] Wrong attachment : this attachment is not an attachment ...

Bug Info	Description
Reported against	ProtocolBundle 1.2.0,ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	We should extract only attachment, not google html pages.

- 14970

[bittorrent] [backport] overflow at bencoded string parsing

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Module	ixProtocols
Platform	All
Effect of bug	Crash
Expected versus actual behavior	Some new bittorrent clients give wrong sizes for bencoded strings this caused an overflow and dpi engine crash.

- 15043

[SF4272][gmail_mobile] bugs

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	receiver_type and receiver_alias are swapped.

- 15075

[SF4853] [facebook] friends list is not extracted

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Module	ixProtocols
Platform	All

Bug Info	Description
Effect of bug	Extraction anomaly
Expected versus actual behavior	Friends list should be extracted.

- 15077

[twitter] add typeahead query extraction support

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	We should be able to extract metadata while typing a query on linkedin.

- 15080

[ymsg] protocol update (inheritance problems)

Bug Info	Description
Reported against	4.13.1
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	On new version of ymsg, inheritance with sip is not possible.

- 15081

[irc] unitary attribute extraction issues

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Unit test errors on nickname, mode, mode_channel and mode_status.

- 15105

[SF4922][ymail_classic] session_id extracted only once when the event is stored

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	session_id attributes is extracted twice. the first one is incorrect. We should extract only the 2nd one.

- 15117

[SF4853][facebook] : update status not extracted when a picture is posted

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Status update is no longer extracted if done when uploading a picture.

- 15123

[bittorrent] file_completed, file_downloaded, file_incomplete not extracted.

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The attributes file_completed, file_downloaded and file_incomplete are not extracted on specific traces.

- 15169

[SF4945] [facebook_mail] only extract last message when preloading thread

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Some facebook_mail messages are not extracted.

- 15200

[SF5004] [aim_express] - Contacts are extracted as sender/receiver

Bug Info	Description
Reported against	ProtocolBundle 1.2.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	aim_express aim contacts should be extracted as "contact" and not "sender".

- 15201

[SF4978][IMAP] login extracted to many times and with wrong values

Bug Info	Description
Reported against	ProtocolBundle 1.3.0

Bug Info	Description
Module	ixProtocols
Platform	x86_64_USER
Effect of bug	Extraction anomaly
Expected versus actual behavior	The login should be extracted once and with a right value.

- 15202

[krb5] Regression on krb5 classification

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixEngine
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	The regression is a late classification. The krb5 protocol was not classified on client packet.

- 15214

[SF5044][radius] : packet are not classified

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	All radius packets should be classified.

- 15221

[SF4979][H225/Q931] Callee attribute is not extracted from call session

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixE: LibAFC
Platform	x86_32_KERNEL
Effect of bug	Extraction anomaly
Expected versus actual behavior	callee value should be extracted from the layer q931.

- 15253

[SF4943][tcp] cnx_duration sometimes NULL even if tcp:fin is seen

Bug Info	Description
Reported against	ProtocolBundle 1.0.0
Module	ixProtocols
Platform	x86_64_USER
Effect of bug	Extraction anomaly

Bug Info	Description
Expected versus actual behavior	tcp:cnx_duration should be NULL even if there is only a FIN flag detected

- 15254

[SF5052][live_hotmail] subject truncated

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The subject attribute is truncated on specific traces.

- 15262

[SF5054][live_hotmail] recipient extracted as reply to attributes

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	"Recipient" information is wrongly extracted on the attribute "reply to".

- 15268

[SF5029][radius] parsing, classification BUG

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Limited password size caused missing classification.

- 15271

[SF4976] [linkedin] - No extraction of auto completed search

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	We must extract auto completed search.

- 15283

[gmail_mobile] in unidirectional mode, parent is not set

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The unitary extraction of some attrbutes is done without extraction of their parents, which leads to wrong attribute structuration. The bug occurs only in unidirectionnal mode.

- 15301

[socks4] [socks5] remote addr and port are not extracted

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Port and address extraction were missing because a wrong extraction callback was used.

- 15353

[krb5] Extra bytes raised

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixEngine
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The attribute ticket_enc_part contained some extra trailing zeros.

45.4.2. Known issues

- 14232

SF4240 - [smb] Real Unicode file names are not supported

Bug Info	Description
Reported against	ProtocolBundle 1.0.0,ProtocolBundle 1.1.0,ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The extraction of file names with special characters stops right after the first one encountered.
Workaround	No workaround

- 14570

SF4196 - [bittorrent] [backport] classification issue

Bug Info	Description
Reported against	ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Module	ixProtocols
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	In some cases, the tracker's announce is not classified as bittorrent and peer's extraction fails
Workaround	No workaround

- 14571

[SF4422][gmail_basic] email_read, TO & date are missing

Bug Info	Description
Reported against	ProtocolBundle 1.1.0,ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	We should get receivers and date extracted on Turkish version of gmail_basic.
Workaround	No workaround

- 14661

[pop3] classification failed in unidirectional (client side)

Bug Info	Description
Reported against	ProtocolBundle 1.2.0,ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Bad classification of pop3 in unidirectionnal flows (client side). ftp is classified instead of pop3
Workaround	No workaround

- 14665

SF4476 - [bittorrent] [backport] (vuze client) peers not extracted from UDP packet

Bug Info	Description
Reported against	4.14.0,ProtocolBundle 1.3.0
Module	ixEngine
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Peers are not extracted from UDP packets
Workaround	No workaround

- 14933

[SF4713] [edonkey] classification issue with obfuscated traffic

Bug Info	Description
Reported against	ProtocolBundle 1.0.0,ProtocolBundle 1.1.0,ProtocolBundle 1.2.0
Module	ixProtocols
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	The classification of edonkey must be enhanced with obfuscated traffic.
Workaround	No workaround

- 15017

[smb] native_os attribute

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The attribute native_os is not raised.
Workaround	No workaround

- 15019

[smb] filesize attribute limitation

Bug Info	Description
Reported against	ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Only one file transfer is processed at any one time.
Workaround	No workaround

- 15068

[smb] smb 2.0 query_id is wrong

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The smb query_id attribute is extracted from Command Sequence Number which in some cases is negative.
Workaround	No workaround

- 15090

SF4927 - [bittorrent] [backport] peers extraction from UDP Tracker Protocol

Bug Info	Description
Reported against	4.14.0
Module	ixEngine
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The peers extraction from UDP tracker protocol must be enhanced.
Workaround	No workaround

- 15107

[live_hotmail] session_id missing on XLR platform

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	The attribute session_id is missing on specific traces.
Workaround	No workaround

- 15171

[bittorrent] [backport] update peer table from ping request

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	Address gathering feature must be integrated in the release to classify obfuscated sessions.
Workaround	No workaround

- 15187

[smptest] [aim] memory leak

Bug Info	Description
Reported against	ProtocolBundle 1.4.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Memory leak
Expected versus actual behavior	Potential memory leak in intensive SMP usage for aim.
Workaround	No workaround

- 15222

[SF5003][POP3] extraction issue

Bug Info	Description
Reported against	ProtocolBundle 1.0.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	If the message header doesn't start with: * Received * Return-Path * Message-ID * Authentication-Results * X-Originating-IP * X-Apparently-To * MIME-Version We will miss some field's extraction
Workaround	No workaround

- 15273

[SF4272] [gmail_mobile] subject not decoded

Bug Info	Description
Reported against	ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	subject is extacted from uri but is not decoded.
Workaround	No workaround

- 15298

[SF4272] [gmail_mobile] remove = char from email_index

Bug Info	Description
Reported against	ProtocolBundle 1.3.0,ProtocolBundle 1.4.0
Module	ixProtocols
Platform	All
Effect of bug	Extraction anomaly
Expected versus actual behavior	unexpected '=' char is extracted in email_index attribute
Workaround	No workaround

- 15435

[SF5220] [sina_weibo] - Missing classification

Bug Info	Description
Reported against	ProtocolBundle 1.3.0
Module	ixE: LibAFC
Platform	All
Effect of bug	Classification anomaly
Expected versus actual behavior	Add sina_weibo classification over api.weibo.cn http server.
Workaround	No workaround