QOSMOS

Your Network is Information

Protocol Bundle 1.42.0

Release Notes

Revision History
Revision

Document revision	Document reference	Date
1.0	Q14T1923	2014.02.07

Legal Notice

Table of Contents

1. Protocol Bundle 1.42.0

1.1. What's new in the Protocol Bundle 1.42.0

1.1.1. Major enhancements in this release

65 new Protocols added, see Section 1.2, “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.

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.

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

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

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
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

1.2.2. 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

1.2.3. Deprecated Protocols

The following protocols have been deprecated in this version:

Table 2. 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.

1.3. Attributes

There are no updates to Attributes in this version.

1.4. Bug Fixes and Known Issues

1.4.1. 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

1.4.2. Known Issues

There are no Known Issues in this version.

2. Protocol Bundle 1.41.0

2.1. What's new in the Protocol Bundle 1.41.0

2.1.1. Major enhancements in this release

65 new protocols added, including several popular web portals (see Section 2.2, “Protocol Updates”).

Updated protocol signatures and supported versions for appstore, nba, facebook_apps. See Section 2.4.1, “Bug Fixes”.

Summary of major enhancements :

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

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.

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

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

2.2. Protocol Updates

2.2.1. New Protocols

The following new protocols have been added in this version:

Table 3. 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

2.2.2. Deprecated Protocols

No protocols have been deprecated in this version.

2.3. Attributes

This section describes the updates to Attributes.

2.3.1. New Event Attributes added in this version

The following Event Attributes have been added in this version.

2.3.1.1. Generic Events added in this version

No Generic Events have been added in this version.

2.3.1.2. Event Attributes added in this version

No Event Attributes have been added in this version.

2.3.2. Event Attributes deprecated in this version

No Event Attributes have been deprecated in this version.

2.3.3. Event Attributes modified in this version

No Event Attributes have been modified in this version.

2.4. Bug Fixes and Known Issues

2.4.1. 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

2.4.2. Known Issues

There are no Known Issues in this version.

3. Protocol Bundle 1.40.0

3.1. What's new in the Protocol Bundle 1.40.0

3.1.1. Major enhancements in this release

19 new Protocols added (see Section 3.2, “Protocol Updates”), including

- blackberry_messenger BBM 10 (audio/video)
- several P2P protocols (e.g. filesharepro, allmusic ...)

18 new Event Attributes added (see Section 3.3, “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**

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.

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 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

3.2. Protocol Updates

3.2.1. New Protocols

The following new protocols have been added in this version:

Table 4. 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).

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 5. 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

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

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 6. 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]

3.4. Bug Fixes and Known Issues

3.4.1. 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	

3.4.2. 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

4. Protocol Bundle 1.31.0

4.1. What's new in the Protocol Bundle 1.31.0

4.1.1. Note about the major enhancements of the release

- 22 new Protocols added. See Section 4.2, “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

4.1.2. 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

4.1.3. 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.

4.1.4. 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

4.2. Protocol updates

4.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 7. 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.

4.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

4.3. Attributes

This section describes the attribute updates.

4.3.1. New event attributes added in this version

There are no event attributes added in this version.

4.3.2. Deprecated event attributes in this version

There are no deprecated event attributes in this version.

4.3.3. Event attributes modified in this version

There are no event attributes modified in this version.

4.4. Bugs fixed and Known Issues

4.4.1. 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.

4.4.2. Known issues

There are no known issues raised in this version.

5. Protocol Bundle 1.30.0

5.1. What's new in the Protocol Bundle 1.30.0

5.1.1. Note about the major enhancements of the release

- 46 new Protocols added. See Section 5.2, “Protocol updates”
- 10 new Event Attributes added. See Section 5.3, “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`.

5.1.2. 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.

5.1.3. 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.

5.1.4. 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

5.2. Protocol updates

5.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 8. 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.

5.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

5.3. Attributes

This section describes the attribute updates.

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

There are no generic events added in this version.

5.3.1.2. Events added in this version

Table 9. 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

5.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 10. Deprecated event attributes

Protocol	Deprecated event attributes	Comments
rsh	remote_login	This attribute is now deprecated.

5.3.3. 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 11. 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]

5.4. Bug fixed and known issues

5.4.1. 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.

5.4.2. 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

6. Protocol Bundle 1.23.0

6.1. What's new in the Protocol Bundle 1.23.0

6.1.1. 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 6.2, “Protocol updates”.

6.1.2. 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.

6.1.3. 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.

6.1.4. 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

6.2. Protocol updates

6.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 12. 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

6.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

6.3. Attributes

This section describes the attribute updates.

6.3.1. New event attributes added in this version

6.3.1.1. Generic events added in this version

There are no generic events added in this version.

6.3.1.2. Events added in this version

There are no events added in this version.

6.3.2. Deprecated event attributes in this version

No event attributes have been deprecated in this version.

6.3.3. Event attributes modified in this version

No event attributes have been modified in this version.

6.4. Bug fixed and known issues

6.4.1. Bugs fixed in this version

There are no bugs fixed in this version.

6.4.2. Known issues

There are no known issues raised in this version.

7. Protocol Bundle 1.22.0

7.1. What's new in the Protocol Bundle 1.22.0

7.1.1. Note about the major enhancements of the release

- 127 new Protocols added. See Section 7.2, “Protocol updates”.
- 15 new Event Attributes added. See Section 7.3, “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).

7.1.2. 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.

7.1.3. 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.

7.1.4. 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

7.2. Protocol updates

7.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 13. 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.

7.2.2. Deprecated protocols in this version

Table 14. 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.

7.3. Attributes

This section describes the attribute updates.

7.3.1. New event attributes added in this version

The following event attributes have been added in this version.

7.3.1.1. Generic events added in this version

There are no generic events added in this version.

7.3.1.2. Events added in this version

Table 15. 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

7.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 16. 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.

7.3.3. Event attributes modified in this version

There's no modified event in this version.

7.4. Bug fixed and known issues

7.4.1. 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.

7.4.2. Known issues

There's no known issues raised in this version.

8. Protocol Bundle 1.21.0

8.1. What's new in the Protocol Bundle 1.21.0

8.1.1. 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 8.2, “Protocol updates”

8.1.2. 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.

8.1.3. 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.

8.1.4. 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

8.2. Protocol updates

8.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 17. 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.

8.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

8.3. Attributes

This section describes the attribute updates.

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

There are no generic events added in this version.

8.3.1.2. Events added in this version

There's no new attribute in this release.

8.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this release.

8.3.3. Event attributes modified in this version

There's no modified attribute in this version.

8.4. Bug fixed and known issues

8.4.1. Bugs fixed in this version

There's no bug fixed in this release.

8.4.2. Known issues

There's no known issue raised in this release.

9. Protocol Bundle 1.20.0

9.1. What's new in the Protocol Bundle 1.20.0

9.1.1. Note about the major enhancements of the release

- 12 new Protocols added. See Section 9.2, “Protocol updates”
- 40 new Event Attributes added. See Section 9.3, “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.

9.1.2. 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.

9.1.3. 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.

9.1.4. 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

9.2. Protocol updates

9.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 18. 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.

9.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

9.3. Attributes

This section describes the attribute updates.

9.3.1. New event attributes added in this version

The following event attributes have been added in this version.

9.3.1.1. Generic events added in this version

There are no generic events added in this version.

9.3.1.2. Events added in this version

Table 19. 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

9.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 20. 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.

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

Table 21. 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]

9.4. Bug fixed and known issues

9.4.1. 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.

9.4.2. 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

10. Protocol Bundle 1.19.0

10.1. What's new in the Protocol Bundle 1.19.0

10.1.1. Note about the major enhancements of the release

10.1.1.1. 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`

10.1.2. 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.

10.1.3. 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.

10.1.4. 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

10.2. Protocol updates

10.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 22. 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.

10.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

10.3. Attributes

This section describes the attribute updates.

10.3.1. New event attributes added in this version

No new event attributes added in this version.

10.3.2. Deprecated event attributes in this version

No event attributes have been deprecated in this release.

10.3.3. Event attributes modified in this version

No event attributes have been modified in this version.

10.4. Bug fixed and known issues

10.4.1. 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.

10.4.2. Known issues

There are no known issues raised in this release.

11. Protocol Bundle 1.18.0

11.1. What's new in the Protocol Bundle 1.18.0

11.1.1. Note about the major enhancements of the release

11.1.1.1. 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.

11.1.1.2. 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

11.1.2. 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.

11.1.3. 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.

11.1.4. 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

11.2. Protocol updates

11.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 23. 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.

11.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

11.3. Attributes

This section describes the attribute updates.

11.3.1. New event attributes added in this version

The following event attributes have been added in this version.

11.3.1.1. Generic events added in this version

There's no generic event added in this version.

11.3.1.2. Events added in this version

Table 24. 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

11.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 25. Deprecated event attributes

Protocol	Deprecated event attributes	
base	date	
base	string	
base	uint16	
base	uint32	
base	uint64	
base	uint8	

11.3.3. 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 26. 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]

11.4. Bug fixed and known issues

11.4.1. 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

11.4.2. Known issues

There's no known issue raised in this release.

12. Protocol Bundle 1.17.0

12.1. What's new in the Protocol Bundle 1.17.0

12.1.1. Note about the major enhancements of the release

12.1.1.1. 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.

12.1.1.2. 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.

12.1.2. 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.

12.1.3. 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.

12.1.4. 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

12.2. Protocol updates

12.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 27. 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.

12.2.2. Deprecated protocols in this version

There are no deprecated protocols for this version.

12.3. Attributes

This section describes the attribute updates.

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

There's no generic event added in this version.

12.3.1.2. Events added in this version

Table 28. 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

12.3.2. Deprecated event attributes in this version

There's no deprecated attribute 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

Table 29. 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]

12.4. Bug fixed and known issues

12.4.1. 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

12.4.2. 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

13. Protocol Bundle 1.16.0

13.1. What's new in the Protocol Bundle 1.16.0

13.1.1. Note about the major enhancements of the release

13.1.1.1. 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`.

13.1.2. 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.

13.1.3. 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.

13.1.4. 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

13.2. Protocol updates

13.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 30. 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.

13.2.2. Deprecated protocols in this version

Table 31. 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.

13.3. Attributes

This section describes the attribute updates.

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

There's no generic event added in this version.

13.3.1.2. Events added in this version

There's no added event in this version.

13.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

13.3.3. Event attributes modified in this version

There is no modified attributes in this version.

13.4. Bug fixed and known issues

13.4.1. 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

13.4.2. Known issues

There's no known issue raised in this release.

14. Protocol Bundle 1.15.0

14.1. What's new in the Protocol Bundle 1.15.0

14.1.1. Note about the major enhancements of the release

14.1.1.1. 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.

14.1.1.2. 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

14.1.2. 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.

14.1.3. 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.

14.1.4. 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

14.2. Protocol updates

14.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 32. 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.

14.2.2. Deprecated protocols in this version

There's no deprecated protocols for this version.

14.3. Attributes

This section describes the attribute updates.

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

There's no generic event added in this version.

14.3.1.2. Events added in this version

Table 33. 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

14.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 34. Deprecated event attributes

Protocol	Deprecated event attributes	
base	date	
base	string	
base	uint16	
base	uint32	
base	uint64	
base	uint8	

14.3.3. 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 35. 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]

14.4. Bug fixed and known issues

14.4.1. 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

14.4.2. Known issues

There's no known issue raised in this release.

15. Protocol Bundle 1.14.0

15.1. What's new in the Protocol Bundle 1.14.0

15.1.1. Note about the major enhancements of the release

15.1.1.1. 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`

15.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

15.1.3. 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.

15.1.4. 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

15.2. Protocol updates

15.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 36. 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.

15.2.2. Deprecated protocols in this version

Table 37. 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.

15.3. Attributes

This section describes the attribute updates.

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 new generic events have been added in this version.

15.3.1.2. Events added in this version

There's no event added in this version.

15.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

15.3.3. Event attributes modified in this version

There is no modified attributes in this version.

15.4. Bug fixed and known issues

15.4.1. 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.

15.4.2. Known issues

There's no issue raised in this release.

16. Protocol Bundle 1.13.0

16.1. What's new in the Protocol Bundle 1.13.0

16.1.1. Note about the major enhancements of the release

16.1.1.1. 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.

16.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

16.1.3. 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.

16.1.4. 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

16.2. Protocol updates

16.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 38. 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.

16.2.2. Deprecated protocols in this version

Table 39. 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.

16.2.3. 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

16.2.4. 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	

16.3. Attributes

This section describes the attribute updates.

16.3.1. New event attributes added in this version

The following event attributes have been added in this version.

16.3.1.1. Generic events added in this version

No new generic events have been added in this version.

16.3.1.2. 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 40. 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

16.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 41. Deprecated event attributes

Protocol	Deprecated event attributes	Comments
gizmo	callee, caller, login and service	The protocol is deprecated.

16.3.3. 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 42. 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]

16.4. Bug fixed and known issues

16.4.1. 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	

16.4.2. 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

17. Protocol Bundle 1.12.0

17.1. What's new in the Protocol Bundle 1.12.0

17.1.1. Note about the major enhancements of the release

17.1.1.1. 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).

17.1.1.2. 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.

17.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

17.1.3. 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.

17.1.4. 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

17.2. Protocol updates

17.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 43. 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.

17.2.2. Deprecated protocols in this version

Table 44. 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.

17.2.3. 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.

17.3. Attributes

This section describes the attribute updates.

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 new generic events have been added in this version.

17.3.1.2. Events added in this version

There's no added event in this version.

17.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

17.3.3. Event attributes modified in this version

There's no updated event in this version.

17.4. Bug fixed and known issues

17.4.1. 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.

17.4.2. Known issues

There's no known issue raised in this version.

18. Protocol Bundle 1.11.0

18.1. What's new in the Protocol Bundle 1.11.0

18.1.1. Note about the major enhancements of the release

18.1.1.1. 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`

18.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

18.1.3. 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.

18.1.4. 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

18.2. Protocol updates

18.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 45. 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.

18.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

18.2.3. 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

18.2.4. 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	

18.3. Attributes

This section describes the attribute updates.

18.3.1. New event attributes added in this version

The following event attributes have been added in this version.

18.3.1.1. Generic events added in this version

No new generic events have been added in this version.

18.3.1.2. 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 46. 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

18.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

18.3.3. Event attributes modified in this version

There is no modified attributes in this version.

18.4. Bug fixed and known issues

18.4.1. 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

18.4.2. 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

19. Protocol Bundle 1.10.0

19.1. What's new in the Protocol Bundle 1.10.0

19.1.1. Note about the major enhancements of the release

19.1.1.1. 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.

19.1.1.2. 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).

19.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

19.1.3. 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.

19.1.4. 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

19.2. Protocol updates

19.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 47. New protocols added in this version

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.

19.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

19.2.3. Other features

RT#	Description
17191	[ssl] Add port-based uppers classification documentation

19.2.4. 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	

19.3. Attributes

This section describes the attribute updates.

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 new generic events have been added in this version.

19.3.1.2. Events added in this version

There's no added event in this version.

19.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

19.3.3. Event attributes modified in this version

There's no updated event in this version.

19.4. Bug fixed and known issues

19.4.1. Bugs fixed in this version

There's not bug fixed in this version.

19.4.2. Known issues

There's no known issue raised in this version.

20. Protocol Bundle 1.9.0

20.1. What's new in the Protocol Bundle 1.9.0

20.1.1. Note about the major enhancements of the release

20.1.1.1. 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.

20.1.1.2. 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.

20.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

20.1.3. 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.

20.1.4. 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

20.2. Protocol updates

20.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 48. 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".

20.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

20.2.3. Other features

RT#	Description
15073	[offloading] change of "signaling" feature
15799	SF3918: [ICA] Report application as soon as possible

20.2.4. 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

20.3. Attributes

This section describes the attribute updates.

20.3.1. New event attributes added in this version

The following event attributes have been added in this version.

20.3.1.1. Generic events added in this version

No new generic events have been added in this version.

20.3.1.2. 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 49. 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

20.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 50. 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.

20.3.3. 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 51. 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]

20.4. Bug fixed and known issues

20.4.1. 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

20.4.2. 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

21. Protocol Bundle 1.8.0

21.1. What's new in the Protocol Bundle 1.8.0

21.1.1. 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.

21.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

21.1.3. 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.

21.1.4. 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

21.2. Protocol updates

21.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 52. New protocols added in this version

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".

21.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

21.3. Attributes

This section describes the attribute updates.

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 new generic events have been added in this version.

21.3.1.2. Events added in this version

There's no added attribute for this version.

21.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

21.3.3. Event attributes modified in this version

There's not attribute updates in this version.

21.4. Bugs fixed and known issues

21.4.1. Bugs fixed in this version

There's no bug fixed in this version.

21.4.2. Known issues

There's no known issue raised in this version.

22. Protocol Bundle 1.7.0

22.1. What's new in the Protocol Bundle 1.7.0

22.1.1. Note about the major enhancements of the release

22.1.1.1. 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.

22.1.1.2. Others features and enhancements

22.1.1.2.1. 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.

22.1.1.2.2. 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`.

22.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

22.1.3. 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.

22.1.4. 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

22.2. Protocol updates

22.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 53. 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.

22.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

22.2.3. 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

22.2.4. 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.

22.3. Attributes

This section describes the attribute updates.

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 new generic events have been added in this version.

22.3.1.2. 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 54. 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

22.3.2. Deprecated event attributes in this version

The following event attributes have been deprecated:

Table 55. Deprecated event attributes

Protocol	Deprecated event attributes	Comments
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.

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 56. 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]

22.4. Bug fixed and known issues

22.4.1. 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.

22.4.2. 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

23. Protocol Bundle 1.6.0

23.1. What's new in the Protocol Bundle 1.6.0

23.1.1. Note about the major enhancements of the release

23.1.1.1. 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.

23.1.1.2. Others features and enhancements

An avanced protection security system has been added to manage memory leaks.

23.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 and higher versions of ixEngine.

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. 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.

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

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

23.2. Protocol updates

23.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 57. New protocols added in this version

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).

23.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

23.2.3. 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

23.2.4. 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	

23.3. Attributes

This section describes the attribute updates.

23.3.1. New event attributes added in this version

The following event attributes have been added in this version.

23.3.1.1. Generic events added in this version

No new generic events have been added in this version.

23.3.1.2. 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 58. 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

23.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

23.3.3. 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 59. 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]

23.4. Bug fixed and known issues

23.4.1. 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	

23.4.2. 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

24. Protocol Bundle 1.5.1

24.1. What's new in the Protocol Bundle 1.5.1

24.1.1. Note about the major enhancements of the release

24.1.1.1. 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.

24.1.1.2. Others features and enhancements

The release stability during HTTP session flushing has been improved.

24.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 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. 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.

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

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

24.2. Protocol updates

24.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 60. 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.

24.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

24.2.3. Other features

RT#	Description
16199	[uwtp] add proto tune to discard duplicated packet

24.2.4. 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	

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

No new generic events have been added in this version.

24.3.1.2. 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 61. New event attributes in this version

Protocol	New event attributes
yandex_webmail	attach_id

24.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

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 62. 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]

24.4. Bug fixed and known issues

24.4.1. 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

24.4.2. 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

25. Protocol Bundle 1.5.0

25.1. What's new in the Protocol Bundle 1.5.0

25.1.1. Note about the major enhancements of the release

25.1.1.1. 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.

25.1.1.2. 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`.

25.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 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. 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.

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

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

25.2. Protocol updates

25.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 63. 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".

25.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

25.2.3. 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

25.2.4. 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	

25.3. Attributes

This section describes the attribute updates.

25.3.1. New event attributes added in this version

The following event attributes have been added in this version.

25.3.1.1. Generic events added in this version

No new generic events have been added in this version.

25.3.1.2. 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 64. 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

25.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

25.3.3. 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
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]

25.4. Bug fixed and known issues

25.4.1. 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	

25.4.2. 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

26. Protocol Bundle 1.4.0

26.1. What's new in the Protocol Bundle 1.4.0

26.1.1. Note about the major enhancements of the release

26.1.1.1. 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.

26.1.1.2. 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.

26.1.2. ixEngine compatibility

This protocol bundle is fully compatible with ixEngine 4.15.0-3 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. 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.

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

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

26.2. Protocol updates

26.2.1. New protocols in this version

The following new protocols have been added in this version:

Table 66. New protocols added in this version

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.

26.2.2. Deprecated protocols in this version

There's no deprecated protocol for this release.

26.2.3. 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

26.2.4. 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

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

No new generic events have been added in this version.

26.3.1.2. 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 67. 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

26.3.2. Deprecated event attributes in this version

There's no deprecated attribute in this version.

26.3.3. 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
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]

26.4. Bug fixed and known issues

26.4.1. 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.

26.4.2. 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