XRY 7.6 - Release Notes

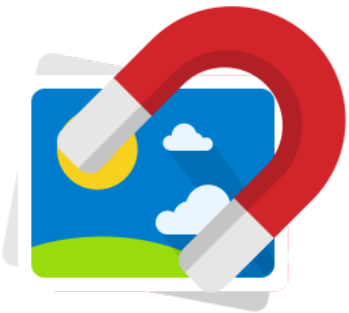
Summary

XRY Mobile Forensic Profiles	v7.6	Total
> Logical Extraction	52	7497
> Physical Dumping	35	4690
> Physical Decoding	35	4625
> Passcode & Bypass	33	2907
> App Versions	222	2109
> XRY Untested	10	1419
> Total	**387**	**23247**

Enhanced File Decoders - Decode more data than ever!

XRY now supports the extraction and decoding of significantly higher volumes of data within modern smartphone devices.

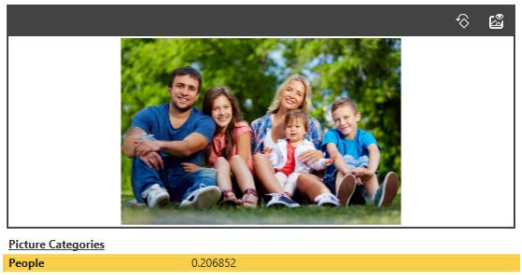
XRY now recovers additional data from a wide variety of sources thanks to newly enhanced decoders. The additional data recovered represents significant volumes of previously inaccessible data within a device and includes pictures, XML, PList and user generated data.



The extraction process is fast and efficient, and results in many newly found data items of interest. A test by our Development department of the same mobile device extracted with both XRY v7.5 and XRY v7.6 showed an increase in recovered data artifacts of well over 100%.

Image Recognition

We have introduced a new Image Recognition engine into the MSAB Ecosystem of tools and you will be able to view the results in XAMN. This feature is activated in the 'Process Options' of XRY. The capability is the first iteration and will have the ability to analyze and classify picture contents, using built-in image recognition technology, into the following categories:

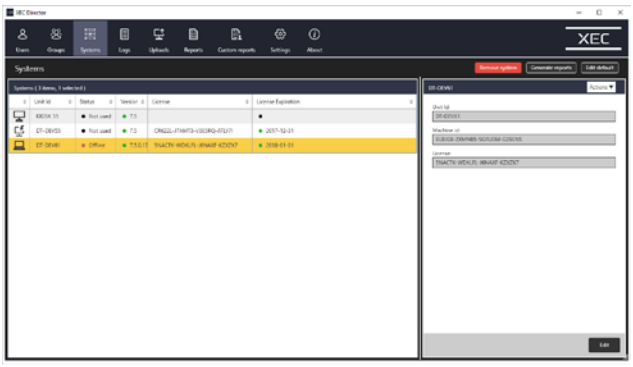


- WEAPON
- DRUGS
- VEHICLES
- FINANCIAL
- ELECTRONICS
- PEOPLE

More development will be undertaken in 2018 and we hope to be able to expand the categories of classification, along with identification accuracy. Please be aware that activating the image recognition feature will of course extend the time it takes to complete the extraction and decoding process. The first version is typically capable of classifying 2-3 pictures per second.

XEC Capable

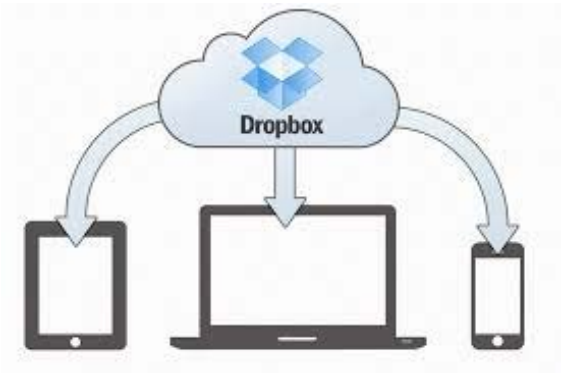
XRY is now capable of being centrally controlled and managed by XEC Director. Users can download an additional install package to enable XRY software to be connected via a LAN to an XEC Director suite.



The functions offered in this first XEC-enabled version are the ability to monitor central logging and to deploy software updates to remote XRY computers from XEC Director. These functions will offer huge savings in terms of administration and resource costs for large-scale deployments of XRY.

For XEC support to function, it is necessary that the XRY setup has an additional SQL Server Express installation (in the same way as is required for XEC Express). XEC Director requires an available domain network for connectivity to XRY-enabled devices to allow these new features.

Android - Offline File Identification



XRY now decodes metadata for files even though the actual file data is not present on a device. This includes smartphone apps such as Dropbox, Google Drive and also previously inserted SD cards.

For Android devices, XRY will now report any residual metadata and identify the existence of offline files recorded as being held in the Dropbox Cloud account. This will happen even if the files were not physically downloaded to the mobile device. This will help point investigators to new sources of potential evidence via the use of XRY Cloud to gather further data.

Data Decoding default triage profile

Starting from now, all decoding performed by XRY that does not use a decoding profile will use the default profile “Finish”.

Improvements

- We have improved support for Drone file decoders and updated support for the DJI Mavic Drone
- To meet the demands of increased IT security, we have upgraded the driver for all our serial based XRY cables, which are now certified for “secure boot” and “drive guard” mode on Windows 7,8 & 10 Operating systems.

End of Life for XRY Reader

MSAB will end of life the XRY Reader v6 application on 31 December 2018. We are letting users know of our plans, in order to allow time for adjustment. After this date, no future versions of XRY Reader will be produced and support for viewing XRY files will no longer be guaranteed in Reader. If you have not already tried it, please download the XAMN Viewer application for free. This is the replacement software for XRY Reader: https://www.msab.com/products/xamn

NEW DEVICES IN XRY LOGICAL

Alcatel	OT-4047d U5
Amgoo	AM303
Apple	iPhone 8 Plus TD-LTE (A1897), iPhone 8 TD-LTE (A1905), iPhone X TD-LTE (A1901)
Argom Tech	E400
BLU	R1 Plus Dual SIM LTE, T274t Diva II
Bmobile	AX1035
Budget Mobile	X410
Chinese Chipsets	388+ Watchphone, Q8 Watch Phone, U80 Smart Watch, V888 Pocket Watch Warcraft BMW
DJI	Phantom 4 (WM330A)
Fiesta Duo	A860
General Mobile	GM 6 d, GM5 Plus LTE-A Dual SIM
Goophone	iX, SM-9500 Note 8i Edge
Huawei	Mate 8 NXT-AL10 Dual SIM TD-LTE, MediaPad M3 BTV-DL09 TD-LTE,
LG	G3 US990 LTE-A, G5 US992 LTE-A, K120 Spree, L62VL Premier LTE (TracFone), LS620y Pulse, M160 K Series K4 2017 LTE, M200n K Series K8 2017 4G LTE, M250n K Series K10 2017 LTE, MP260 K Series K20 plus 2017 LTE-A, MS210 Aristo
M4tel	SS1050 Joy
Meiigoo	M1
Nokia	105 2017 (TA-1010), 105 2017 (TA-1037), 1208 (RH-86) CN, 150 (RM-1189), 150 Dual SIM (RM-1190)
OnePlus	5 Dual SIM Global TD-LTE A5000
Optus	X Play (4034x), X Smart (5056i)
Plum	Z404 Axe Plus 2
reeder	P10s
Samsung	SM-G935t Galaxy S7 Edge LTE-A
Smooth	SNAP Amigo
Stark	Impress Cool
Telstra	4GX Smart (ZTE Blade A112)
TruConnect	D351w
Uniwa	V708
Wogiz	WX10 Plus
ZTE	555 Coral

NEW DEVICES IN XRY PHYSICAL DUMPING

Amgoo	AM303
BLU	T274t Diva II
Bmobile	AX1035
Budget Mobile	X410

Chinese Chipsets	388+ Watchphone, Nokia 105 Dual Sim (RH-XY2017), U80 Smart Watch, V888 Pocket Watch Warcraft BMW
DJI	Phantom 4 (WM330A)
General Mobile	GM 6 d
JERSA	SAMRT G109
LG	G3 US990 LTE-A, K120 Spree, LS620y Pulse, M160 K Series K4 2017 LTE, M200n K Series K8 2017 4G LTE, M250n K Series K10 2017 LTE, MS210 Aristo
Nokia	105 2017 (TA-1010), 105 2017 (TA-1037), 1208 (RH-86) CN, 150 (RM-1189), 150 Dual SIM (RM-1190), 222 (RM-1137), 222 Dual SIM (RM-1136)
Optus	X Play (4034x)
Plum	Z404 Axe Plus 2
Slider	Intelligent C3033
Smooth	SNAP Amigo
Stark	Impress Cool
Telstra	4GX Smart (ZTE Blade A112)
Uniwa	V708
Virgin Mobile	VM585
Wogiz	WX10 Plus
ZTE	555 Coral

NEW DEVICES IN XRY PHYSICAL DECODING

Amgoo	AM303
BLU	T274t Diva II
Bmobile	AX1035
Budget Mobile	X410
Chinese Chipsets	388+ Watchphone, Nokia 105 Dual Sim (RH-XY2017), U80 Smart Watch, V888 Pocket Watch Warcraft BMW
DJI	Phantom 4 (WM330A)
General Mobile	GM 6 d
JERSA	SAMRT G109
LG	G3 US990 LTE-A, K120 Spree, LS620y Pulse, M160 K Series K4 2017 LTE, M200n K Series K8 2017 4G LTE, M250n K Series K10 2017 LTE, MS210 Aristo
Nokia	105 2017 (TA-1010), 105 2017 (TA-1037), 1208 (RH-86) CN, 150 (RM-1189), 150 Dual SIM (RM-1190), 222 (RM-1137), 222 Dual SIM (RM-1136)
Optus	X Play (4034x)
Plum	Z404 Axe Plus 2
Slider	Intelligent C3033
Smooth	SNAP Amigo
Stark	Impress Cool
Telstra	4GX Smart (ZTE Blade A112)
Uniwa	V708

Virgin Mobile	VM585
Wogiz	WX10 Plus
ZTE	555 Coral

NEW DEVICES IN XRY PASSCODE & BYPASS

Alcatel	OT-4009d Pixi 3 3.5 Dual SIM, OT-5044y U5 LTE
Amgoo	AM303
Blackview	A5
BLU	T274t Diva II
Bmobile	AX1035, AX512
Budget Mobile	X410
Chinese Chipsets	388+ Watchphone, Nokia 105 Dual Sim (RH-XY2017), U80 Smart Watch, V888 Pocket Watch Warcraft BMW
FinoWatch	Q7 Plus Smart Watch Phone
General Mobile	GM 6 d
JERSA	SAMRT G109
LG	G3 US990 LTE-A, LS620y Pulse, K120 Spree, M160 K Series K4 2017 LTE, M200n K Series K8 2017 4G LTE, M250n K Series K10 2017 LTE, M322 X Charge Series X Power 2 LTE-A, MS210 Aristo
Nokia	1208 (RH-86) CN
Optus	X Play (4034x)
Plum	Z404 Axe Plus 2
Stark	Impress Cool
Telstra	4GX Smart (ZTE Blade A112)
UTStarcom	CDM-7126c
Verykool	s4005 Leo 3G Jr.
Vortex	Pulse
Wogiz	WX10 Plus
ZTE	555 Coral

NEW APP VERSIONS: ANDROID

- DJI GO 4 (4.1.15)
- Dropbox (68.2.2), (72.2.2), (74.2.2)
- Facebook (144.0.0.27.91), (149.0.0.40.71), (150.0.0.38.138), (151.0.0.44.205)
- Facebook Messenger (138.0.0.20.92),(139.0.0.17.85), (140.0.0.43.91), (141.0.0.31.76), (142.0.0.18.63), (143.0.0.20.69), (144.0.0.22.136), (145.0.0.25.203), (146.0.0.33.136), (98.0.0.18.71)
- GMail (7.10.22.174510681), (7.10.8.172533986), (7.11.5.176133587), (7.11.5.176568039), (7.11.5.177402951), (7.9.10.169126262)
- Google Allo (20.0.023_RC05), (20.0.023_RC06), (21.0.023_RC06), (22.0.023_RC09), (23.0.024_RC06), (24.0.020_RC06)
- Google Maps (9.62.1__9.34.1), (9.64.1), (9.65.1), (9.66.1__9.34.1), (9.67.1__9.34.1)
- Grindr (3.15.0), (3.16.0), (3.17.0), (3.18.0), (3.20.0), (3.21.0)

- Instagram (17.0.0.15.91), (18.0.0.18.85), (19.1.0.31.91), (20.0.0.29.75), (21.0.0.11.62), (22.0.0.17.68), (23.0.0.14.135), (24.0.0.12.201)
- Kik Messenger (11.36.0.18816), (11.37.0.18906), (11.38.0.18991), (11.39.0.19149)
- Line (7.14.0), (7.14.1), (7.15.0), (7.15.1), (7.15.2), (7.16.1), (7.16.2), (7.16.3), (7.17.0), (7.17.1)
- QQ (7.2.5), (7.3.0)
- Skype (8.10.0.4), (8.12.0.2), (8.7.0.59973), (8.8.0.61630), (8.9.0.64295)
- Snapchat (10.18.5.0), (10.19.0.0), (10.21.6.0), (10.22.6.0), (10.22.7.0), (10.23.0.0)
- Telegram (4.4.0), (4.4.1), (4.4.2), (4.5.0), (4.5.1),
- Tinder (8.0.0), (8.0.1), (8.1.0), (8.1.1), (8.2.0), (8.2.1), (8.2.2),
- Twitter (7.15.2), (7.16.0), (7.17.0), (7.18.0), (7.19.0), (7.20.0), (7.21.0), (7.22.0), (7.23.0), (7.24.0), (7.24.1)
- Waze - GPS, Maps & Traffic (4.31.0.2), (4.32.0.3)
- WeChat (6.5.16)
- WhatsApp (2.17.364), (2.17.365), (2.17.367), (2.17.368), (2.17.369), (2.17.370), (2.17.371), (2.17.373), (2.17.374), (2.17.375), (2.17.377), (2.17.379), (2.17.381), (2.17.385), (2.17.387), (2.17.389), (2.17.390), (2.17.392), (2.17.394), (2.17.395), (2.17.396), (2.17.397), (2.17.399), (2.17.400), (2.17.401), (2.17.402), (2.17.403), (2.17.404), (2.17.405), (2.17.406), (2.17.407), (2.17.408), (2.17.409), (2.17.410), (2.17.411), (2.17.412), (2.17.414), (2.17.416), (2.17.417), (2.17.419), (2.17.421), (2.17.423), (2.17.425), (2.17.428), (2.17.429), (2.17.430), (2.17.431), (2.17.432), (2.17.434), (2.17.436), (2.17.437)
- Viber (7.7.0.21), (7.8.0.0), (7.8.1.1), (7.9.0.6), (7.9.2.10), (7.9.4.11), (7.9.4.7)
- Yahoo Mail (5.18.2), (5.21.2)
- YouTube (12.37.59), (12.37.59__11.41.56), (12.39.60), (12.41.55), (12.43.52__11.41.56), (12.44.53__11.41.56), (12.45.56__11.41.56)

NEW APP VERSIONS: iOS

- Dropbox (68.2), (70.2), (72.2)
- Facebook (151.0), (55.0), (85), (96.0),
- Facebook Messenger (121.0), (138.1)
- GMail (5.0.170910), (5.0.170925), (5.0.171020), (5.0.171104.697219), (5.0.171119.701303)
- Grindr (3.6.0)
- Kik Messenger (11.32.0), (11.32.0.19336), (11.33.0.19389), (11.35.0.19619), (11.36.0.19732)
- Line (7.14.0), (7.15.0), (7.16.0), (7.17.0)
- QQ (腾讯 QQ) (7.1.8), (7.2.0)
- Tinder (8.1.0), (8.2.0)
- Twitter (7.8), (7.9), (7.10), (7.11), (7.11.1), (7.12), (7.12.1)
- WeChat (6.5.19), (6.5.20.32), (6.5.21.33), (6.5.23.32)
- WhatsApp (2.17.20.1127), (2.17.52), (2.17.61), (2.17.70.939), (2.17.71.71), (2.17.81.82), (2.17.82.19)
- Viber (7.7.1), (7.8.0.472), (7.9.0.168), (7.9.2.348), (7.9.4.61), (7.9.5.9)
- YouTube (12.38.8)