

A nighttime photograph of a city skyline reflected in water. A prominent clock tower with a green patina and a decorative top is the central focus. The sky is a mix of orange and blue, suggesting dusk or dawn. The water in the foreground shows clear reflections of the city lights and the tower. The overall mood is serene yet urban.

MSAB

Mobile Forensics Solutions for Border Control

21 November 2018

The MSAB logo is displayed in large, dark, three-dimensional block letters mounted on a light-colored stone wall. The letters are bold and have a slight shadow, giving them a 3D appearance. The wall is composed of large, rectangular stone tiles with visible grout lines.

MSAB

Our company:

Swedish Company, founded in 1984, HQ in Stockholm

XRY launched 2005

Shipped +21,000 kits since then

Customers in over 120 countries

Offices around the globe

AAA rated with no debt

“The cell phone is probably the single most important piece of evidence you will find at a crime scene today.”

James Comey, Former FBI Director



The building blocks of the Ecosystem – our products and services

Customer organization



Products

- | | | |
|--|---|--|
| XL
XRY Logical
Extract and recover data communicating with the operating system. | XS
XAMN Spotlight
Powerful multi-mode review and search tool. | XD
XEC Director
Remote management of systems and users. |
| XP
XRY Physical
Extract and recover raw data directly from the device memory. | XV
XAMN Viewer
The easiest way to view XRY extraction files. | XX
XEC Export
Batch export and conversion of XRY files into other formats. |
| XC
XRY Cloud
Extract and recover data from connected cloud based storages. | XH
XAMN Horizon
Overview of multiple device files. Case level wide examination. | |
| XPS
XRY Express
Controlled workflows for speed, efficiency and compliance. | XE
XAMN Elements
Enabling the true experts to examine binary and hex data with the aim of reconstructing content. | |
| XDU
XRY Drone
Extract and recover drone forensic data. | | |

Platforms

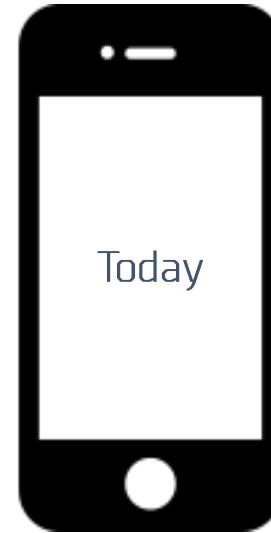
- | | |
|-----------------------|------------------------|
|
MSAB Kiosk |
MSAB Office |
|
MSAB Field |
MSAB Tablet |

Services

- | | |
|---------------------|---------------------------|
|
Strategy |
Implementation |
|
Training |
Support |

3rd party solutions

Is mobile forensics relevant for Border Control?




MSAB

Mobile Phones may provide additional information



- Identity
- country of origin
- travelling route
- Suspect contacts & networks
- Other incriminating data

What can we find? - Examples

Artifacts 			
Calls	80	Bookmarks	19
Contacts	1331 (707)	History	410
Contacts	1328 (707)	Searches	66
Social Groups	3	Messages	559 (42)
Device	4168 (291)	Chat	425 (29)
Device Accounts	2	Emails	36
Event Log	3165 (291)	MMS	14 (6)
Installed Apps	676	SMS	84 (7)
Keyboard Cache	293	Organizer	1176 (263)
Network Information	23	Calendar Events	956 (256)
Notifications	9	Notes	20 (6)
Files	117251 (3393)	Tasks	200 (1)
Application Binaries	1549 (1)	Security	23
Archives	238	Accounts	23
Audio	957	Web	1661 (70)
Databases	1794 (4)	Bookmarks	224 (18)

Case study: Metropolitan Counter Terrorism Command



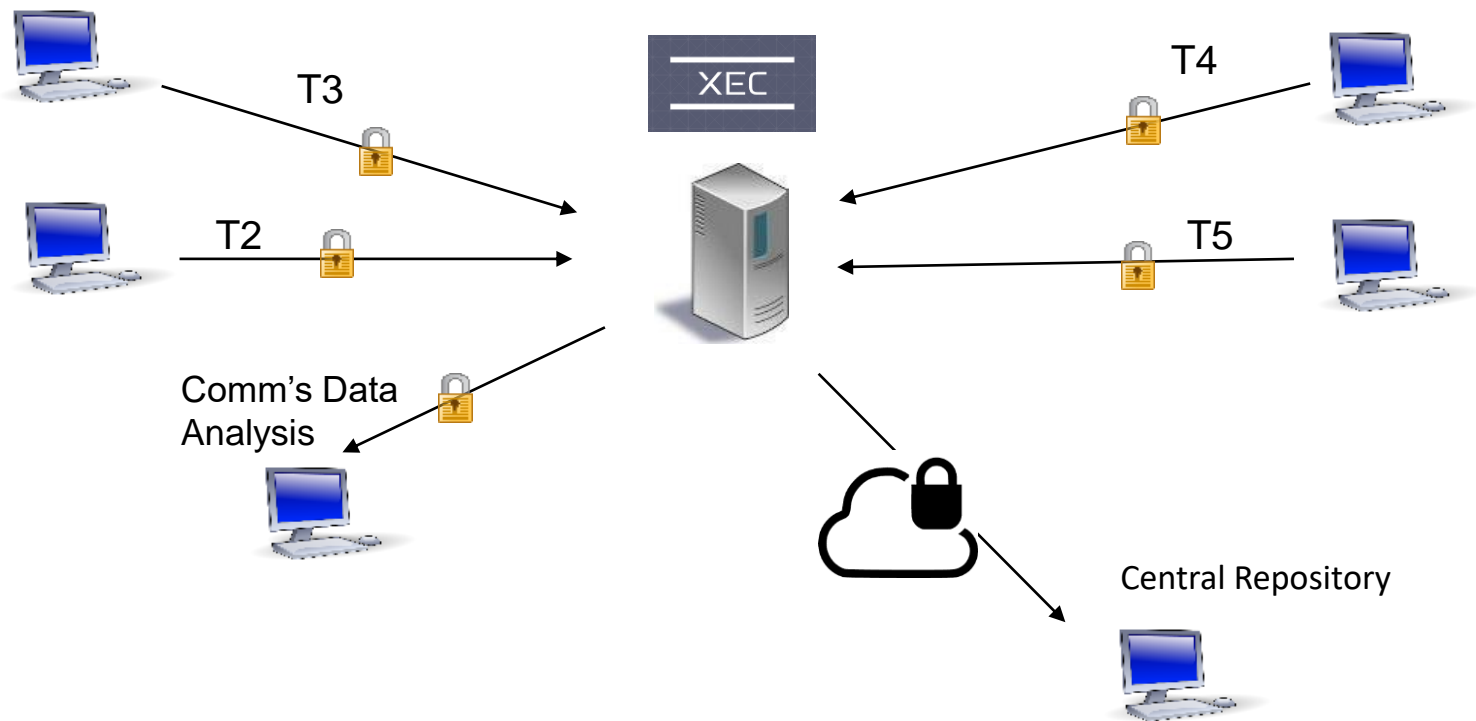
Task:

- Identify persons entering to UK via London Heathrow who may be a potential risk for national security.
- Operate under Sch7 Terrorism Act

Mobile forensic unit:

- Set up Digital Forensics Unit in 2011 at Heathrow
- 5 airport terminals, + 60 officers, 4 forensic experts
- initially stand a lone XRY kits at the 5 terminals





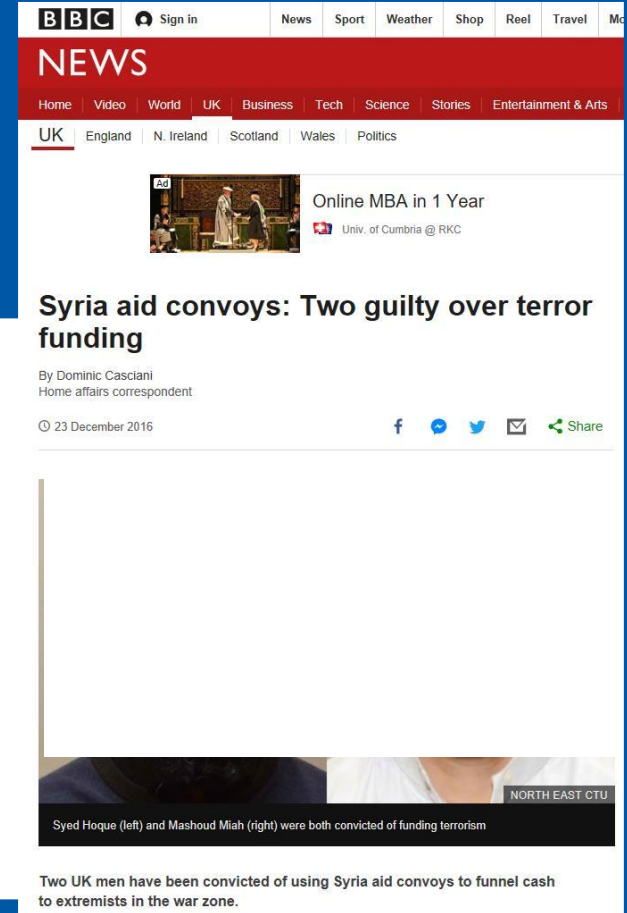
Results

Operational efficiency

- Easier to use for officers who are not digital forensic experts
- Reduced costs for operations

Example of a case solved

- Phone extraction at Heathrow b
- Chat messages show compelling that accused were financing terrorism
used aid convoys to forward the



Challenge 2015–2016:

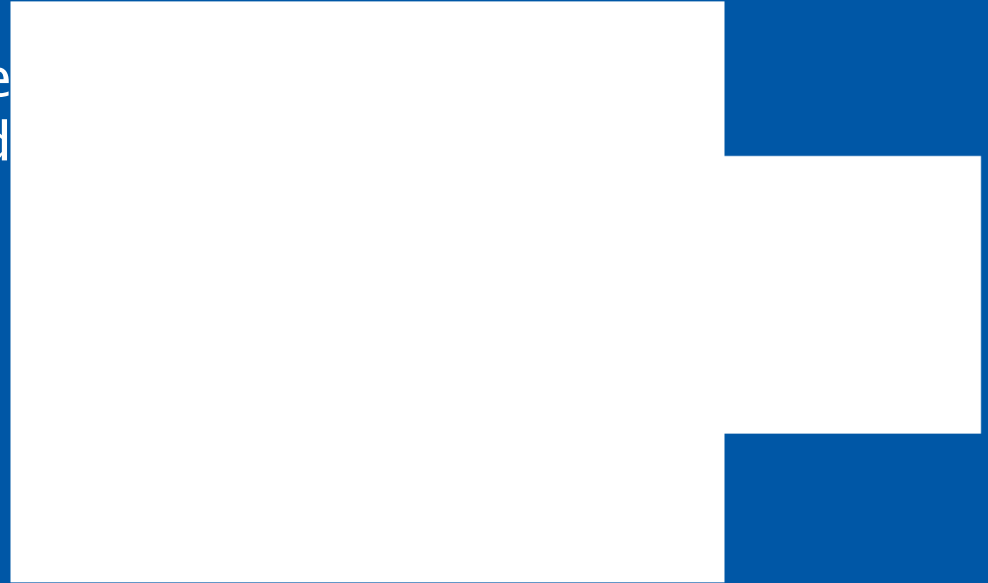
- Extreme volumes of asylum seekers lead to heavy workload and unacceptable long asylum application process
- Asylum seeker's origin important criteria for asylum right
- Many refugees have no passport or other ID document
- Need for a fair process to help refugees demonstrate their identity

Use mobile forensics to help determine country of origin?



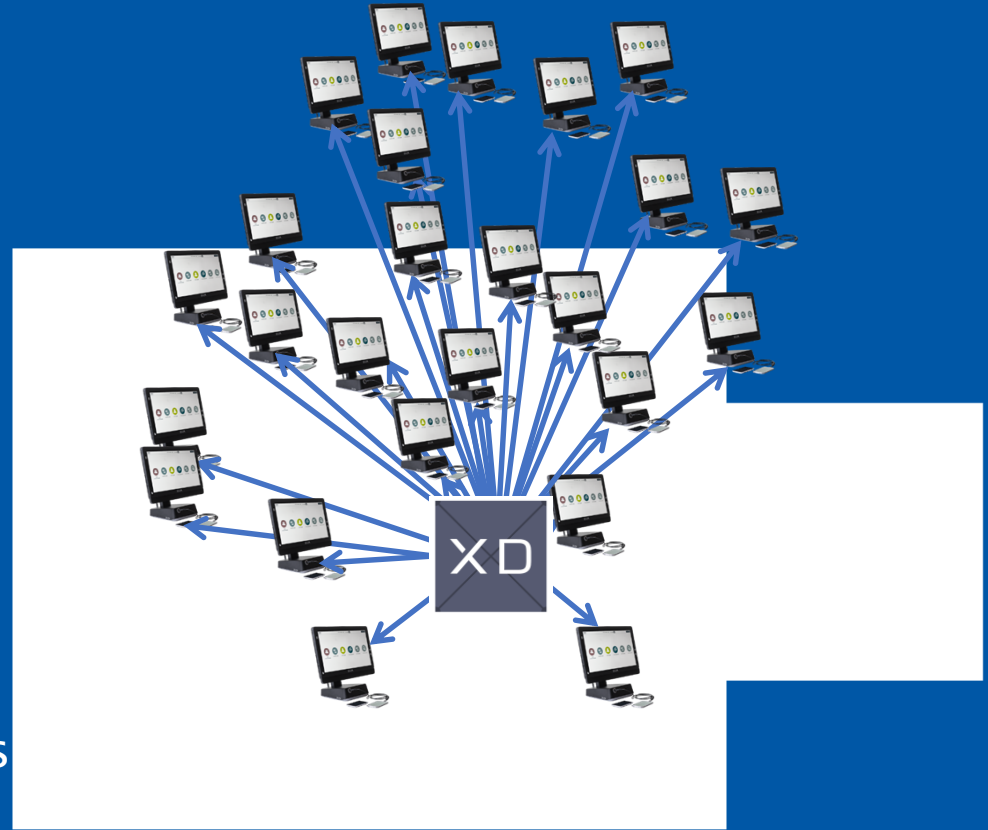
Phone data of potential interest

- Calls list (country code)
- Messages (country code)
- Geotags
- Account information



Solution

- MSAB Kiosks at local migration centres managed centrally
- Customized workflow and triage for phone extraction
- 3rd party solution for automatic language and location analyses
- Provides data helping to confirm the asylum seeker's country origin



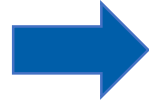
The Process

Extraction

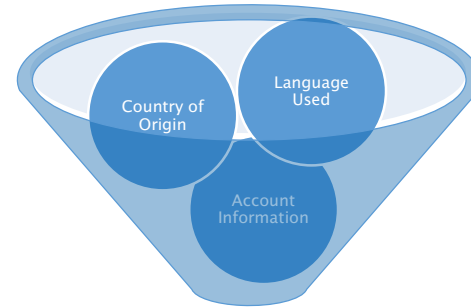


Workflow
Triage

Automatic Export



Automatic analyses



Report

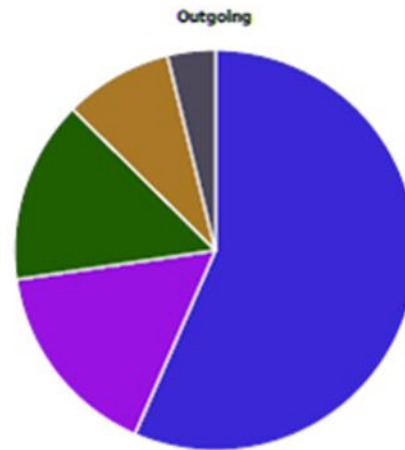


MSAB

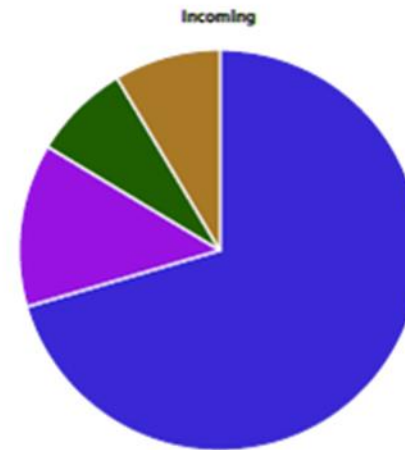
The report: Country data

Analysis of country codes for calls (phone and comm. apps)

Calls (Phone/Messenger)



Austria (+43)	207
Egypt (+20)	59
[pos. valid] (~)	54
[not valid] (-)	32
Other countries	14

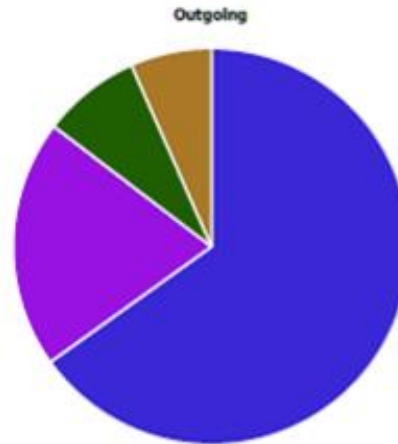


Austria (+43)	198
Egypt (+20)	37
United Arab Emirates	22
Other countries	24

The report: Country data

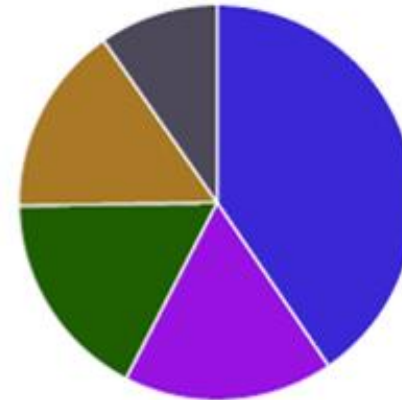
Analysis of country codes for messages & chats

Messages (SMS/MMS/Chat)



Egypt (+20)	138
Greece (+30)	43
Slovakia (+421)	17
Other countries	14

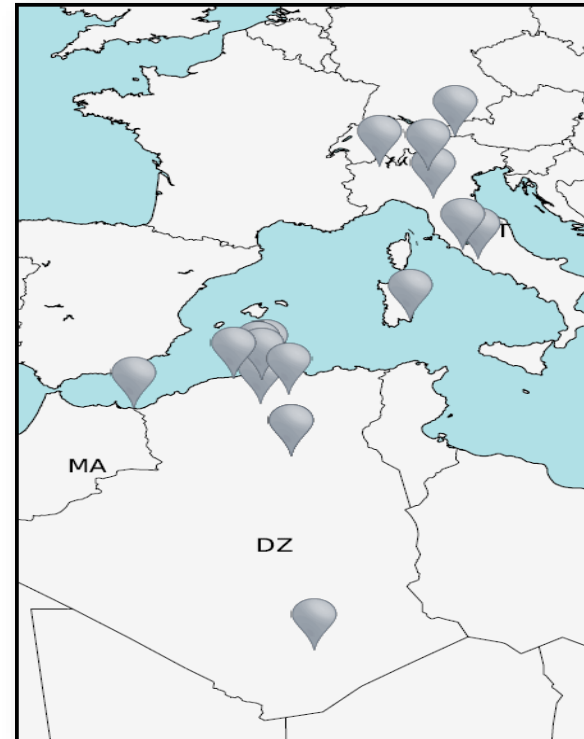
Incoming



Egypt (+20)	125
(not valid) (-)	53
Greece (+30)	53
United Arab Emirates	48
Austria (+43)	30

The report: Country data

Analysis of location data



MSAB

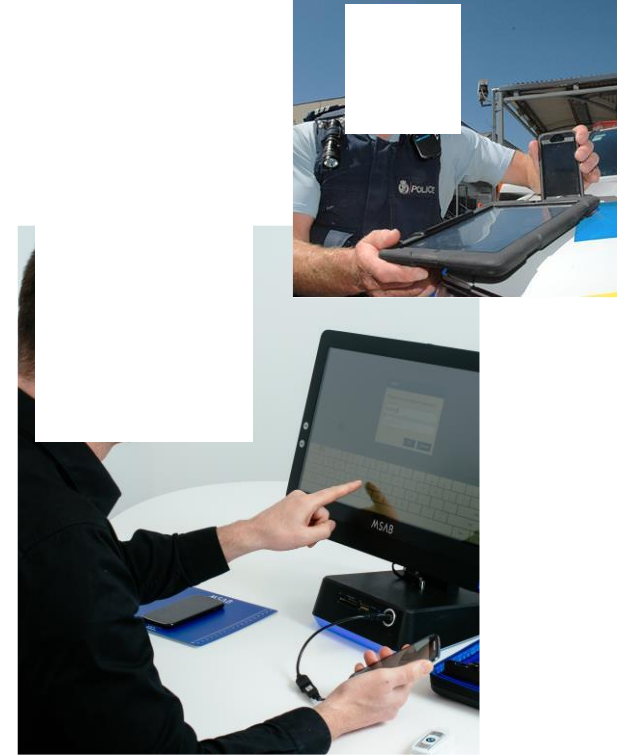
Commercial Information

MSAB

Why customers choose MSAB Kiosk/Tablet?

Customer needs

- Allow non-forensic experts to perform extractions
- Increase efficiency
- Quality assurance (follow SOPs)
- Prevent unauthorized use
- Making more information available/extract more devices
- Quicker response time, actionable intelligence
- Give forensic experts time to dedicate for advanced tasks
- Control of costs and usage



MSAB

XRY Kiosk/XRY Tablet

How does they differ from "standard" XRY

Controlled environment

- Locked down
- Login
- User administration

Designed for non-technical users

- GUI
- Viewer
- Work Flow



What does workflow bring

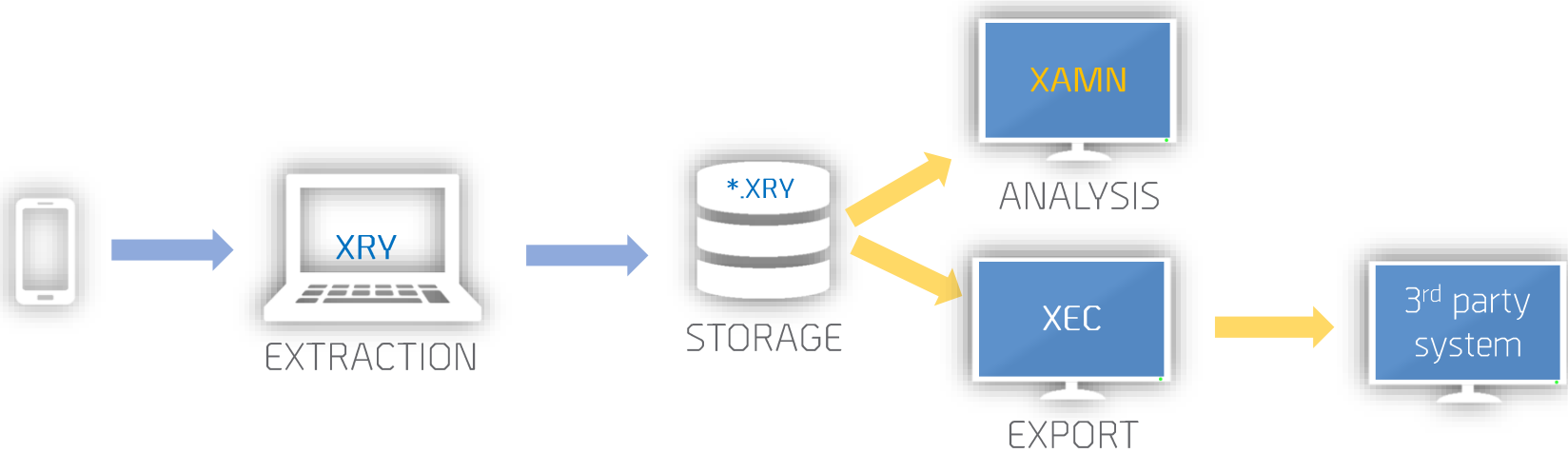
Available for Kiosk/Tablet/Office with XRY Express



- Less trained staff can perform extractions
- Control of users
- Control of process using tailored workflow
- Tailor process/workflow to different user groups
- Less IT support
- Statistics and management reports







MSAB



Products

- | | | |
|---|--|---|
| XL XRY Logical
Extract and recover data communicating with the operating system. | XS XAMN Spotlight
Powerful multi-mode review and search tool. | XD XEC Director
Remote management of systems and users. |
| XP XRY Physical
Extract and recover raw data directly from the device memory. | XV XAMN Viewer
The easiest way to view XRY extraction files. | XX XEC Export
Batch export and conversion of XRY files into other formats. |
| XC XRY Cloud
Extract and recover data from connected cloud based storages. | XH XAMN Horizon
Overview of multiple device files, Case level wide examination. | |
| XPS XRY Express
Controlled workflows for speed, efficiency and compliance. | XE XAMN Elements
Enabling the true experts to examine binary and hex data with the aim of reconstructing content. | |
| XDU XRY Drone
Extract and recover drone forensic data. | | |

Platforms

- | | |
|--|---|
| 
MSAB Kiosk | 
MSAB Office |
| 
MSAB Field | 
MSAB Tablet |

Services

- | | |
|--|--|
| 
Strategy | 
Implementation |
| 
Training | 
Support |

3rd party solutions

MSAB



Contact information:



MSAB