Are there any “court-approved” mobile forensic tools?
Are there any "court-approved" mobile forensic tools?

There is no such thing as a "court-approved" mobile forensic device or standard forensic tool certification applicable to all the different legal systems across the globe. In general, a forensic tool has to demonstrate that it is fit for purpose in each independent nation, state or local legal system where it is used.

MSAB has supplied over 21,000 versions of XRY to customer organizations in over 100 countries worldwide. Our tools are relied upon for the production of evidence from mobile devices by thousands of organizations globally and it is has been used by law enforcement agencies on countless occasions as evidence in criminal proceedings since 2003.

While the mobile device itself remains the 'primary' evidence as the original source of the data in court cases, the XRY report is preferable in the vast majority of occasions because it makes it so much easier to display and understand relevant evidence in court.

In many countries, the government has independent legal bodies, which can be used to test devices, check their accuracy, and validate their use. The National Institute of Standards and Technology (NIST) in the United States is a good example. NIST regularly tests and provides objective independent assessments of XRY and other mobile forensic technologies to help law enforcement agencies and the courts evaluate the products.

Rules of evidence in many nations also state that a person submitting digital forensic evidence must be competent to do so, and that usually means they should have been properly trained, so that they can give evidence explaining the relevance and the implications of their actions. Good practice also indicates that an audit trail should be created to record all processes applied to the mobile device (which XRY automatically creates for you). That would enable an independent third party to examine those processes and achieve the same result.
While there is no single global standard, the United Kingdom has produced a useful guide about how to validate forensic tools and key principles to adhere to, the ACPO Good Practice Guide for Digital Evidence.

XRY is fully compatible with the key principles of this document:

**Principle 1**

No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

**Principle 2**

In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

**Principle 3**

An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

**Principle 4**

The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Principle 1 is very difficult to adhere to when dealing with mobile devices. As mobile phones tend to be proprietary embedded devices – the very moment we turn on the mobile phone it begins to alter its digital state, so for mobile phones we tend to look at Principle 2.

Principle 2 is critical when dealing with mobile devices and it means that the user should be trained if they are planning to use the XRY report as evidence in court. XRY is being used in courts daily across the globe and while MSAB does everything possible to ensure you have a product that reaches the highest standards in digital forensic evidence – it is imperative that investigators thoroughly understand the information they are presenting in a court of law.

Central to this is the ability to present and explain the XRY report as evidence. The court will base much of their assessment on the strength of the investigator’s explanation of the evidence. XRY Training Certification Courses are essential to help investigators and analysts become confident in the presentation of evidence and provide documentary proof of competency on the forensic analysis of mobile devices with XRY.

XRY easily meets Principle 3 by having a detailed ‘Audit Log’ file produced in every XRY report to show exactly how the data was gathered. This means that an independent party can follow the same steps in the log file to replicate the same results, even after considerable time has elapsed since the initial examination.

Principle 4 is generally for the prosecutor to ensure suitable oversight and this falls outside of the remit of forensic tool requirements.
As a manufacturer of digital forensic tools, MSAB ensures that it conducts thorough testing of its own for every device profile and app supported. A key component to this is repeat testing before any new release to ensure we can validate and verify the information being produced by XRY.

We maintain a complete library of every digital device supported by MSAB. Should you ever need Technical Support for a mobile device, we can set up an exact replica of your system and test the exact phone in our offices to verify your results.

Another standard that applies to Digital Forensic laboratories is ISO/IEC 17025:2005.

Using the UK as a benchmark for evidential standards, there are a set of guidelines produced by the Forensic Science Regulator. These state that the provider of digital forensic science shall comply with the Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System and be accredited to ISO/IEC 17025:2005 for any laboratory function (such as the recovery or imaging of electronic data).

Unfortunately, it is not possible for MSAB to help individual organizations attain their own ISO 17025 status since it is a vital component of the accreditation process that the organization producing digital evidence conduct their own independent testing.

Nevertheless, we can confirm that many of our customers have successfully been able to attain ISO 17025 status in their digital forensic laboratories, while using XRY as their primary tool for the recovery of digital forensic evidence from mobile devices.
Suitability
for Court

In court, defense lawyers are entitled to challenge evidence and that of course applies equally to XRY reports. XRY has been challenged numerous times in criminal courts across the globe, but we are not aware of a single occasion where XRY evidence has been dismissed due to unreliability or doubt about the forensic integrity of the system. For that reason, we believe that XRY is acceptable as evidence in a court of law.

In general, questions about the validity of our tools are most often asked in the early days of product adoption, when users are unfamiliar or do not fully understand the technology very well. As the courts become more familiar with the production of digital evidence from mobile devices, these questions tend to diminish.

In most countries, it is perfectly legitimate to submit the XRY report as a form of evidence. This is most often submitted in the form of an "exhibit" which is produced by someone (typically the phone examiner) in a sworn witness statement. The statement and exhibit are then submitted as evidence to the court and accepted. The witness statement should record how he or she examined the phone, give evidence of the examiner’s competency and then crucially produce the XRY report as evidence.

The actual format of the XRY report can be either as a printed-paper document, electronic document (e.g., PDF) or the original XRY report displayed via PC. More recently, due to the volume of data and multimedia files found on modern smartphones, it has become preferable to show XRY in its native format in order to play video or audio recordings to the court.

Local courts usually determine which media format they prefer to receive as evidence, however as smartphones containing Gigabytes of data; it is becoming a practical impossibility to produce paper evidence as these reports can often exceed 10,000 pages.

Best evidence rules suggest that forensic reports should always be validated. This can be done by either manually checking the phone against the XRY report to verify the contents in comparison or more often ‘dual tooling’ whereby you use another forensic product to validate the results of the XRY report.

Ultimately, only the criminal courts can make decisions about whether to accept the digital evidence or not for each case, on an individual basis. So ‘court approved’ mobile forensic tools do not exist – but this guidance should assist your court in making an informed decision about whether or not to accept the evidence.
About MSAB

MSAB is a pioneer in forensic technology for mobile device examination. With offices worldwide and our products in use in more than 100 countries, we have a global reach. The company has been involved with mobile communications since 1984, with a singular focus on the forensic recovery and analysis of data from mobile devices since 2003. MSAB’s products include XRY software for extraction, which can run on virtually any Windows-based computer; XAMN software for analysis and XEC Director software for management and reporting.