



Forensic Litigation Support

Digital electronic evidence is probative information stored in digital form that a party may use at trial. It includes computer print outs, emails, digital photographs, ATM transaction logs, spread sheets and others. With increased computerisation and technology as well as the rise of the digital office, courts have been forced to allow for the admittance of digital evidence. In Kenya Section 65 of the Evidence Act allows admittance of microfilms, fax copies and computer printouts for use in trial.

Security Risk Solutions has built a world-class Computer Forensic Services program. The core team of professionals is regarded as some of the 'forefathers' of the computer forensic field. We have drawn on this expertise and have made significant investments in both equipment / tools and human capital to establishing a preeminent Computer Forensics capability for our clients. **Forensic Litigation Support** – We provide technical and investigative assistance to law firms and corporate counsel in requesting and responding to legal processes, including Electromagnetic Media Discovery (EMD). Using Computer Forensic tools and methods, our team can assist the legal team recover otherwise elusive information to aid their legal case and testify in court to the origins of electronic evidence and signatures.

What are the Requirements of Sections 65, 106A and 106D of the Kenyan Evidence Act?

- Electronic Records are now admissible as evidence:** Any information contained in an electronic record which is printed on a paper, stored, recorded or copied on optical or electro-magnetic media produced by a computer is deemed to be also a document, and is admissible in court (Definitions and Section 65).
- The Electronic Record should meet specified conditions:** The electronic record should be generated by an authorized person and the source information of the electronic record should be fed into the computer in the ordinary course. The computer ought to be operating properly and if not, the fault should not have affected the accuracy of the electronic record. Additionally, it should be possible to reproduce electronic record or to derive it from the source information by feeding it into a computer through the ordinary course of activities (Section 65).
- Proceedings referring to Electronic Evidence:** In proceedings where electronic records are used as evidence, the identity of the electronic record and the manner in which its was produced have to be described. Additionally, the particulars of any devices involved in the production of the electronic record ought to be given as part of ascertaining that the electronic record was produced by a computer (Sections 106A-D).
- Electronic Signatures are now recognised:** Agreements can be concluded by affixing the digital signatures of the parties. Where an electronic signature has been affixed to an electronic record, it must be proved that the signature is that of the subscriber. The courts presume that unless the contrary is proved, a secure electronic record has not been altered from the time when a secure electronic signature was affixed (Section 106D).



Relevant Experience

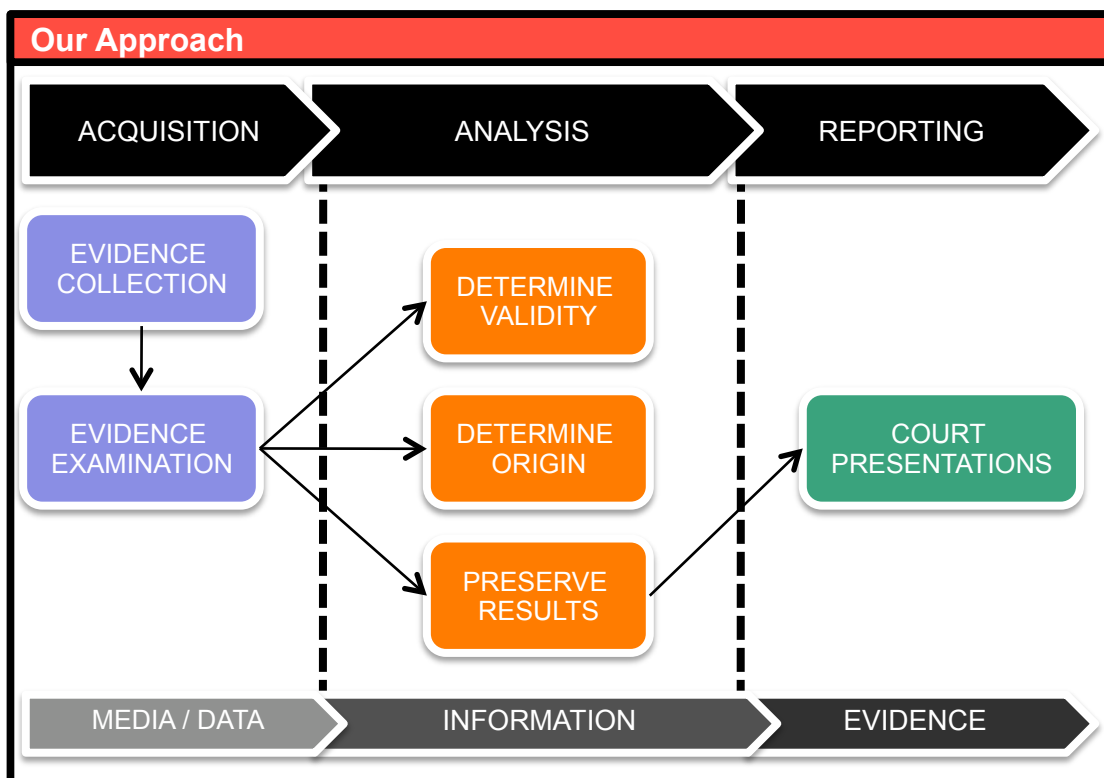
- Security Risk Solutions since our inception over 6 years ago, has been working to the leading International Law Enforcement guidelines in order to bring admissible evidence to court wherever we operate.
- SRS have seized evidence for Governments, Banks and Corporates over all of East Africa, West Africa, Central America (Belize) and the Middle East (Bahrain and Qatar).
- We have given affidavits on legal privilege here in Kenya.
- Our case histories are many, varied and sensitive. We do not tell tales out of court. **We do tell tales in court.** Our expert witness capabilities have been used in Bahrain (International Terrorism) and in Kenya (Bank Fraud).
- Our examiners belong to the best respected world-wide law enforcement and software providers forums where we **share our knowledge** and experience with other practitioners whose cases range (like ours) from multi-national frauds and associated mismanagement to the domestic criminal situation and from international terrorism to specialist Government requirements.
- We use **state-of-the-art** Computer Forensic tools and technologies to achieve the most successful results for our clients.
- We work **with** our clients to ensure that our investigative and forensic analysis strategies will achieve the business and legal objectives and expectations.

World-class Approach

- Obtain evidence, perform analysis and give testimony.
- Cost-effective and time-saving process to ensure evidence can be presented in court subject to the provisions and requirements of the act.
- Results are hard facts, backed up by reasoned and repeatable processes that we self validate and that can be validated world-wide.

Value

- Compelling court-type evidence provided with Expert Witness experience meeting the requirements of the Kenyan Evidence Act 2009.



Forensic Litigation Support

This service constitutes a highly evolved and structured approach, compliant with the latest forensic standards, to examining the evidence of computer-based incidents. The focus of this service is on identifying data and person(s) relevant to a legal case or to aid an ongoing investigation.



Learn More

To learn more about how Security Risk Solutions can assist you with Computer Forensic services, call your usual SRS contact, or our team of security advisers on +254-20-883312, or visit our Web site at www.securityrisksolutions.net

Security Risk Solutions Ltd.
Karen Connection, Karen Road
P.O. Box 15306-00509 Karen
Nairobi, KENYA
+254(20)883312
info@securityrisksolutions.net

