



- ◆ computer forensic evidence
- ◆ mobile phone evidence
- ◆ digital document discovery



Karl Obayi Esq.

MCSE, CCNA, MCT, CCA, LL.B, BL

Computer forensic Solicitor

Principal Consultant

What we do

We act as Specialist Solicitors in legal matters that concern Computer evidence, Mobile phone evidence and Digital document discovery.

We undertake the discovery, extraction and presentation of computer and mobile phone evidence; formulate and implement strategies for electronic document management, conduct the review of forensic expert report and undertake the relevant direct examination, cross examination and rebuttal of computer forensic expert witnesses and document custodians.

Our unique Advantage

We are well grounded in the knowledge of the relevant law and technology. Our Principal Consultant previously practiced as a Barrister for more than a decade, a former university law lecturer, and presently, a practicing Solicitor in England and Wales. In addition, he is a Certified Computer Systems Engineer and Certified Computer Forensic investigator with more than 20years, combined experience in information technology and legal practice.

We provide Strategic leverage

Our presence in your team, removes the need for a digital forensic expert. Because as lawyers who doubly qualify as digital forensic engineers we are well positioned to advice on the relevance and strategic steps necessary to implement a successful digital evidence discovery and forensic litigation protocol. We take ownership of the digital evidence component of your case while you concentrate on other matters.

Independent Forensic laboratory

We maintain our own forensic laboratory, where we undertake the extraction, analysis and review of digital evidence from Computers, Mobile phones and other digital devices. Our review of digital evidence and expert witness report helps contradict or support forensic expert opinion. Our approach to digital evidence analysis will provide a clear picture of the strength and weakness inherent in any item of digital evidence.

Our Clients

We work with, private clients, Barristers, Solicitors ,insurance firms, Banks, legal training institutions, Judicial officers; providing the required digital forensics expertise and electronic document strategy from pre action protocols to Case management conference and court room advocacy. If your case (Criminal or Civil) has a shred of Computer or technology input, contact us before you proceed.

“What you don’t know can hurt you”



Computer forensic evidence

What is the scope and meaning of Computer forensics?

Computer forensics involves the application of scientific techniques and procedures for investigating, gathering and presenting evidence, from any computer equipment, various storage devices and digital media, which can be presented in a court of law in a coherent, admissible and probative manner.

Computer forensics deals with the familiar questions of the Who, What, Where and How; surrounding the use of a computer in a criminal activity or civil dispute. Subject to certain variables, computer data can be located, even in cases where evidence has deliberately been deleted.

In the 21st century, computers and other digital devices like mobile phones form the popular channel of communication in social and business circles. Consequently, computers hold a huge resource of evidence to prove or disprove a fact in issue before a court of law. Computer and digital evidence can decide where the balance of justice swings in the following matters:

- ✚ Financial, Insurance & Bank fraud
- ✚ High technology crimes
- ✚ Divorce proceedings
- ✚ Employment dispute proceedings
- ✚ Contract & commercial Disputes
- ✚ Arbitration and mediation

Proof of the existence or non existence of a fact in issue is based on hard evidence. In the case of Computer generated evidence, much of the what, who, where and how is buried in the inner recess of the Computer in non human readable form as binary digits (1, 0).

Given the technical characteristics of Computer evidence, expert assistance in extracting, analysing and presenting this specie of evidence, is not only a necessary step but it is indeed mandatory. Failure to adhere to established and recognised protocols in extracting and analysing computer evidence can render otherwise probative evidence utterly useless.

How can we help?

We provide an end-end service when it comes to computer evidence. We review incriminating digital evidence and investigate the existence of exculpatory evidence, conduct the direct and cross examination of forensics expert witnesses. We take care of the digital evidence component of your case, thus giving you time to concentrate on other relevant legal issues while preparing and conducting your case.

We verify, and where necessary contest the procedures, methodologies and findings of forensic investigators based on reports from our own independent forensic laboratory. When we join your team, you strategically avoid the use of a computer forensic expert and consequently have the advantage of a technical expert Attorney assisting with strategies, at Directions hearings, Pre trial proceedings, Case management conferences and during trial.



Mobile phone evidence

Mobile phones have become the medium of choice for communication for individuals and businesses. The advent of the smart phone has practically transformed the mobile phone to a mobile computer capable of any form of communication word processing, email, voice and video. Today's smart mobile phones hold a huge deposit of legal evidence that can be used in a court of law.

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methodologies. This, however, is not a task for the non professional investigator.

Mobile phones as an object may not constitute the main focus of a crime or dispute but the evidence it holds may go a long way to support an assertion as to the true state of disputed facts. Its role in social and business interactions makes the mobile phone an indispensable source of digital evidence for the prosecution and defence.

Evidence from mobile phones have been used to resolve puzzles in murder cases, Terrorism trials, Bank fraud cases, proof and disproof of alibi. In civil cases, it has been used in divorce matters, disputes in commercial transactions etc.

When a mobile phone is encountered during an investigation, many questions arise for consideration, chief amongst which is whether the mobile phone contains responsive data relevant to the investigation at hand and whether the necessary laboratory protocols and best practices have been followed in the extraction and analysis of the evidence contained in the mobile phone.

Different models of mobile phones from different manufactures usually will require a customised protocol to extract, examine, and preserve the evidence they hold. Although there is the generally accepted science concerning the Subscriber module, cell site analysis, communication triage etc. Extracting and preserving evidence from mobile phones is a complex issue and must not be attempted by someone without the requisite forensic training.

As a legal technology firm, with lawyers who are trained forensic engineers, our combined legal and technical skills, cover the life circle of mobile phone evidence.

How can we help?

From pre seizure considerations, extraction of evidence, preservation, evidence analysis, review and presentation, we are well positioned to serve your needs and advice on strategic considerations for the presentation of mobile phone evidence in court or tribunal.

Because we are involved from pre trial proceedings, directions hearing to court room advocacy, we have a broad and specific view of the relevance or otherwise of mobile phone evidence to your case.

We undertake the review of forensic expert reports and where relevant, conduct the direct or cross examination of expert witnesses and laboratory technicians.



Electronic document discovery

Are you prepared for potential litigation?

The term document, now includes digital and electronic data extracted from computers and other digital devices like mobile phones and PDA's - these extracted data include, emails, video files, music files, application files e.g. Microsoft word, voice mail, chat room sessions, mobile phone data, internet surfing records, GPS tracking data, databases, computer logs and volatile computer data.

Electronic evidence is now an entrenched component in most legal jurisdictions. The courts now encourage parties to confer and agree on the scope and method of electronic discovery before and during trial. It is important to get it right at these conferences or when responding to a court imposed directions.

Failure to identify relevant document custodians, determine the scope and relevance of keywords for search purposes or prescribe the format in which responsive data needs to be produced, may irretrievably jeopardise your case and lead to attendant prohibitive cost.

Issues of electronic document discovery will arise at pre trial and during trial. Attorneys and their clients must adopt a proactive role when it comes to dealing with electronic evidence. This is one area of litigation or arbitration that cannot be addressed spontaneously when a disclosure or interrogatory request is served from the other side.

Document Management

Electronic documents unlike traditional documentary evidence are not located in file cabinets to be pulled out promptly when required. There must be adequate and functional strategy in place to confront issues dealing with electronic document discovery and archiving. Adequate planning, time, capacity and secure access are fundamental to any electronic management strategy.

IT Managers often do not possess the necessary equipment and are not specifically trained to understand and fully appreciate the legal nuances involved in electronic evidence gathering, analysis, the formulation of search terms and keywords, and automating ways of redacting privileged documents. These stages require the use of expensive, professional hardware and proprietary software – which are not found in the typical IT department.

How can we help?

We prepare and implement customised in house and trial protocols for identifying and presenting relevant digital and electronic evidence, establish a chain of custody, prepare or respond to motions for discovery and interrogatories of electronic data and initiate strategies on cost saving measures and shifting of e-discovery. Resist ill conceived and burdensome electronic document discovery request.

We maintain a secure online repository for all your electronic documents. They are scanned into the appropriate format for achieving and potential discovery. They are made securely available only to your legal team online 24/7. We work on a strictly client Attorney confidentiality with your documents.



Demonstrative evidence

Every picture tells a story – Leverage your position.

As the old adage says, “A picture is worth a thousand words.” Visual imagery transcends language, jargon, scientific description and technical terminology. Harnessing the power of visual communications gives you a distinct advantage over just spoken or written words alone.

Demonstrative evidence can take various forms - Power point presentation slides, 2D and 3D graphic images, computer animation, crime scene reconstruction, accident reconstruction, product liability, flowcharts, Timeline mappings and Medical Illustrations.

Due to the presence of procedural rules with respect to the admissibility of evidence in court, the mere possession of or the ability to produce demonstrative or illustrative evidence will not make it acceptable by the court. Arguments about admissibility and weight to be given to demonstrative evidence will often arise. How do you cross this hurdle?

The party who wishes to rely on demonstrative evidence will need to prove certain essential ingredients to assure the court amongst other grounds, that the demonstrative evidence will not be prejudicial to the merits of the case and that it is relevant. Because Demonstrative evidence on its own, does not provide any independent probative value ,it is used generally :

- ✚ to educate the Judge and Jury;
- ✚ to explain a technical and complex point
- ✚ to persuade your audience of something
- ✚ to dissuade your audience of something
- ✚ to reinforce something your audience already believes

The above objectives cannot be met, without a comprehensive legal analysis of the facts of a case, combined with the relevant law and the applicable procedural rules of court.

How can we help?

Because, we are lawyers with the requisite technical background, we are able to provide an end-end service with the use of demonstrative evidence in court or Arbitration.

Prior to the production of demonstrative evidence, we carry out the essential legal analysis based on the facts of the case and the relevant law. Thereafter, we advice on whether or not it is prudent to incorporate demonstrative evidence; if yes, in what form, scope and the required protocol for its presentation in court.

We integrate with the digital production team at every stage and ensure compliance with the facts of the case and the stated objectives We conduct arguments in pre trial hearings and case management conference to allow or resist the use of demonstrative evidence. More importantly we present the final demonstrative evidence as expert witnesses in court. From initial conception to court room delivery, you will be dealing with one team with respect to the use and presentation of demonstrative evidence in court or arbitration.



Training and Seminars

Evidence! Evidence!! Evidence!!! This is the essential ingredient that determines whether or not you win or lose in Court or arbitration; to extend the theme further, not just evidence but the quality of evidence.

A couple of factors come to the fore when the Courts determine what constitutes admissible and relevant evidence and the quality or probative value to attach to a piece of evidence. Lawyers by training are comfortable with these parameters.

It is however, a matter of regret that professional legal training has not kept pace with the rapid advancement of technology. Given, that about 90% of Business documentation and communication now passes through computers and digital devices but never make it to the paper format. Legal training institutions, lawyers, Judges and litigants must appreciate the need and relevance for digital evidence training. A nodding acquaintance with the subject will not suffice.

Given, the highly technical and volatile nature of computer evidence, professional training in identifying, extracting, analysing and presenting computer evidence is not only imperative but mandatory. It is no longer fashionable for a lawyer to say he or she is ignorant about computers- this mind set is a sure way to attract a professional negligence suit.

While the initial goal is not aimed at making every lawyer a computer forensic expert, or an IT manager a legal forensic specialist within every organisation, at a minimum, the legal department, Human resource department and the IT department must have a resource person who has had some meaningful training on digital evidence. The alternative is to retain the services of a digital evidence consultant who is able to respond promptly when the need arises.

How can we help?

We run relevant courses and seminars that cover the essentials of digital evidence. The courses are organised in specific modules thus allowing delegates to choose their areas of interest. These courses can be held at your office or at our Classroom in London. Find below a list of some of the courses we presently offer. Visit our web site for an exhaustive list.

- ✚ Introduction to Computer Evidence
- ✚ Computer Evidence – Intermediate
- ✚ Computer Evidence – Advanced
- ✚ mobile phone evidence – Introduction
- ✚ IT law for IT Managers
- ✚ Electronic Document Discovery
- ✚ Digital evidence for Lawyers.
- ✚ Digital evidence for the Judiciary
- ✚ Prosecuting Computer crimes

Legal Practice Software training

- ✚ Trial Director – Court room case presentation
- ✚ Sanction – Court room case presentation
- ✚ Case Map – Total case management
- ✚ Doculex – Digital Document Management.



Expert Evidence

In litigation or arbitration, it's increasingly probable that digital evidence will be an integral part of your legal arguments. The need to present proof of file transfers, the existence of incriminating emails, Internet use, software defects, IP theft etc. has moved into our world and our courtrooms.

It is not just about producing evidence. It is about producing and presenting quality and probative evidence. Computer evidence is easily tainted if the appropriate measures are not taken during its life cycle. Many types of criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialist:

Criminal Prosecutors use computer evidence in a variety of crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.

Civil litigations can readily make use of personal and business records found on computer systems that bear on: contracts, divorce, discrimination, and harassment cases.

Insurance Companies are able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.

Corporations often hire computer forensics specialists to ascertain evidence relating to: sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information.

Individuals sometimes hire computer forensics specialists to investigate private issues concerning cyber stalking, computer hacking, email tracing and domain disputes.

Consequently, the forensic expert will investigate, analyse and present his findings. Very often, these findings end up in court in the form of testimony. The forensic investigator in presenting his findings in a court of law or tribunal will be acting as an expert.

The rules concerning expert evidence will without exception apply to the computer forensic expert. It is important therefore, that the forensic expert be familiar with the peculiar nuances of the legal environment while giving evidence. Be able to communicate technical and complex scientific findings in a way that the court, Judge and jury can fully understand the relevance or otherwise of computer evidence.

How can we Help?

Because we are lawyers who also qualify as computer forensic experts, we have a unique advantage in acting as your computer forensic expert. We understand the law and the technology.

In order to sustain or contest the findings of other forensic experts, we provide computer expert witness testimony in Criminal and Civil cases on issues dealing with computer and mobile phone evidence. We carry out independent review of forensic evidence in our own laboratories. We verify, and where necessary contest the procedures, protocols and findings of forensic investigators based on reports from our own independent investigations and forensic laboratory reviews.



Incident Response

Bad things are happening on computers and to computers; ranging from fraud, security breach (Hacking), corporate espionage, internal sabotage, missing files. All of these instances may lead to civil, criminal and arbitration issues followed by request for discovery and interrogatories. An incident response protocol prepares a company to respond proactively to a potential crisis or respond adequately to a crisis and be litigation ready.

An otherwise probative source of electronic evidence may be tampered with and irreparably destroyed due to poor handling of electronic evidence by a non specialist staff.

Business organisations may open themselves up to expensive litigation because there is no digital evidence incident response protocol in place. How do you implement a protocol within an organisation? How does the presence of a protocol help with e-discovery? We specialise in setting up incident response and crisis management protocol for corporate organisations.

The events surrounding Enron and WorldCom corporate scandal and the attendant Banking system financial disaster have now made it imperative for corporations in the US, UK and elsewhere around the world, to have an incident response protocol in place.

Corporate Attorneys and medium to large firms must appreciate the need for a functional incident response protocol for their information technology infrastructure; implementing an incident response protocol is the right thing to do. Acceptable Incident response requires a proactive approach not a response after the fact of an incident.

The prohibitive penalties associated with not having a protocol in place may lead to accusations of tampering with potential evidence and create logistic difficulties when responding to a litigation Hold request arising from an impending litigation.

Regulatory compliance and business practices now require evidence of IT audit protocol concerning the IT infrastructure of companies particularly, publicly listed companies. The credit card multi billion industries now insist on certain defined measures of IT security protocol from its agent.

A company with a lax security and incident response protocol does not leave much in its defence of culpability when the issue of negligence is in issue especially as it relates to data loss, corporate espionage or unregulated access to company intellectual property assets and shared network resources.

How can we help?

We assist in the formulation and implementation of incident response protocols that are audited on an annual basis or as regularly as the client desires. Very often, taking the auditing task from internal control ensures better compliance and audit of relevant protocols. Having a protocol in place ensures prompt and inexpensive response to motions for interrogatories and disclosures. On the contrary, not having a protocol in place creates a dangerous void. This void may lead to so many unforeseen legal consequences down the road. Play safe and be proactive with computer incident response. Contact us for more details.



Internet law

The Internet (cyberspace) and its associated technologies, processes and services have resulted in the revolution of commerce. Apart from affecting our understanding of local and international commerce, it has also broadened our understanding of traditional areas of law like defamation, libel, contract, copyright, intellectual property, patents and commercial law, and the scope of criminal activities that needs attention.

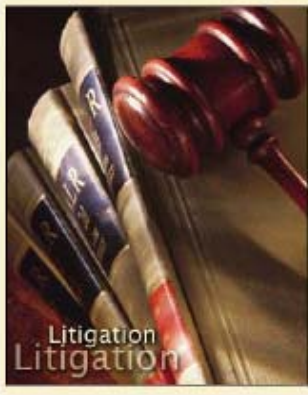
The pervading influence of the internet in our private and corporate dealings makes it imperative to develop and implement relevant strategies to protect our interests when using this medium (internet) for trade, information dissemination or establishing a corporate presence.

There is an evolving body of international law, case law, and national statutes that dictate what, how and when internet relationships are formed. However, there are a lot of legal pits falls arising from conflict of law issues and the relevant law to apply to a set of facts.

This is further complicated by the unique nature of evidence required to prove or disprove computer evidence especially when the facts exist across national borders. Computer evidence in its native form is made up of binary numbers- (1 and 0) it needs to be traced, extracted, and preserved. This is not a task easily accomplished without the help of an expert. This is where we come in to the picture. We offer services in the following areas.

- ✚ Domain Name Disputes
- ✚ Domain and Email tracing
- ✚ Patent and Copy Right Infringement
- ✚ Intellectual Property
- ✚ Service provider Contracts
- ✚ Online fraud
- ✚ Defamation
- ✚ Web Site Hacking

A thorough knowledge of internet law and strategising is required to effectively deal with any dispute that may arise from the above subjects. Your traditional understanding of the law of defamation (for example) may not aid your appreciation of defamation in cyberspace. The scope of facts, source and nature of evidence is different; the evidential rules required to ground proof are often different. Contact us for further information.

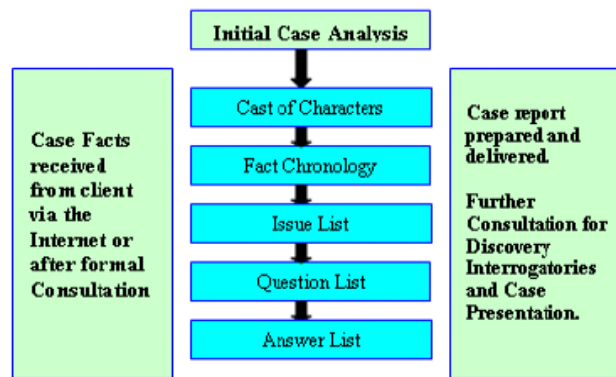


Litigation Strategy

A good case can be lost due to poor strategy or lack of it. Relevant facts particularly those dealing with computer evidence may not be apparent on the surface consequently, they get ignored. If your case has a connection with the use of a computer or mobile phone chances are, there is a case component that may be relevant in the formulation of your legal theory.

“What you don’t know may hurt you”

We adopt a sound forensic approach that clearly identifies the real technological issues and marry them with the facts. Depending on which side of the "V" you find yourself, our job is not only to prepare and evaluate the case in your favour, but we are also candid enough, based on our findings, to advise on potential problem areas or inherent weakness in your case. The illustration below depicts our case handling process.



Digital discovery and disclosure request can be very expensive to comply with. Your adversary may employ the use of digital document discovery to intimidate and complicate your case. Let us show you how to respond and shift the cost.

Digital discovery strategies, interrogatories and Timeline mappings improve the drafting and scope of pleadings. We advise on what Discovery request are necessary, how to respond to discovery request, what preliminary motions are necessary before and during the substantive case.

If required, we advise and participate in court room presentation conducting advocacy and undertaking the direct and cross examination of expert witnesses and document custodians.



**computer evidence
mobile phone evidence
digital document discovery**

iTevidence
Office 12, The Generator
95, Miles Road, Mitcham
Surrey. CR4 3FH
London