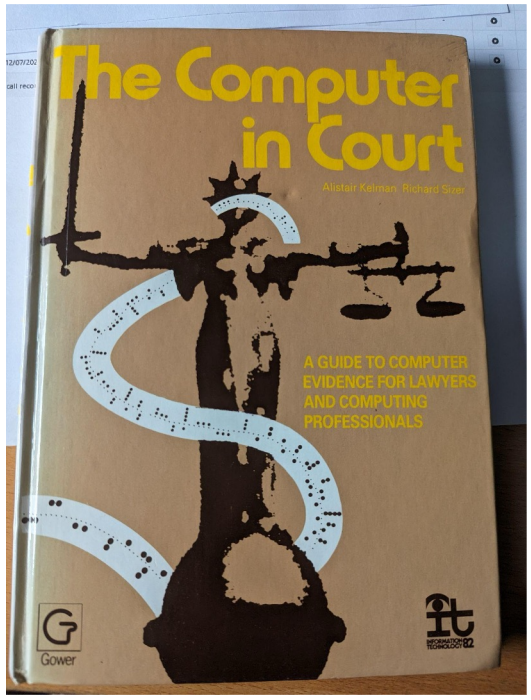
Computer Evidence Workshop

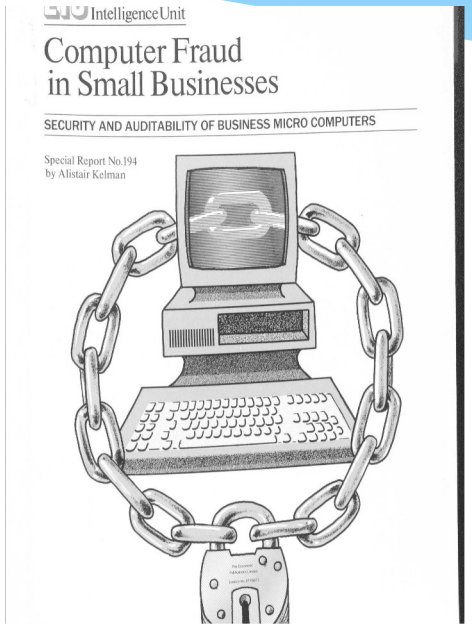
A potential solution to the computer evidence problem

Alistair KELMAN

2 May 2025

A long long time ago …





The Concept

* **Dr Stephen Castell:** *"A trial relying **on** computer evidence should start with a trial **of** the computer evidence"*
* But: *Lawyers who can turn a grown man into a quivering pulp under vicious cross-examination do not know how to highlight latent errors in computer evidence*
* **Solution:** Give lawyers a resource which identifies all the potential sources of error in the computer evidence so that they can cross-examine the evidence and enable the court (and jury) to determine the correct weight to apply to the computer evidence.
* The original **Seven Statement Test** from Kelman and Sizer

The draft Affidavit or deposition

* My view, back in 1982, was that a new form of affidavit or deposition should be used to produce computer evidence in both criminal and civil cases so that the question of reliability of computer evidence could be adequately argued in court.
* "*A document containing the Seven Statements would be extremely lengthy but much of it could and, we believe, should, be prepared by an organisation using computers prior to any incident requiring the organisation to go to law or to assist in a prosecution. The first six of the Seven Statements could be kept in draft form on file. It would then be a simple and inexpensive process to finally add the Seventh Statement and engross the document attaching any relevant computer printouts to it as exhibits.*"

The original Seven Statements

1	The qualifications and experience of the person in charge of the computer system. This is to establish that he is capable of swearing such a document.
2	A description of the computer system with reference to each of the components in the system by brand and model number, e.g. a Kamikaze DDB7 with the Asthma 2.6 operating system running custom written payroll programs.
3	A long statement, should deal with the quality of the individual components by reference to the development time involved in their creation. For example reference could be made here to any technical literature or manuals which were used, giving the number of man hours involved in their original development. Manufacturers of quality products would gladly assist in producing technical evidence of this kind.
4	The testing and documentation standards applied to any custom written software. If the software had been bought-in, the software house, if reputable, should be willing to provide information on its testing and documentation standards.

The original Seven Statements

5	The procedures for logging updates to the software and the qualifications of the subordinate staff involved in the computer system.
6	The physical and electronic security features of the installation.
7	How the particular computer printout came into existence and what it purports to show. In this section the person in charge can say that *no faults manifested themselves during the material time which would indicate to him that the computer evidence could not be relied upon.*

Bringing the SST up to date #1

Update the Seven Statement requirements to cater for modern systems:

1. A Board Member with explicit responsibility for ensuring that the business maintains accurate records
2. “Wiki” of the key components that make up the computer system by brand, model number and configuration
3. Quality of the individual components in a fully hypertext reference document which would identify the exact sources of information on the components assisted by A.I
4. The Testing and documentation standards applied to any custom written software e.g. DITA (Darwin Information Typing Architecture) which is an XML-based standard that enables the creation of modular, reusable, and adaptable content.

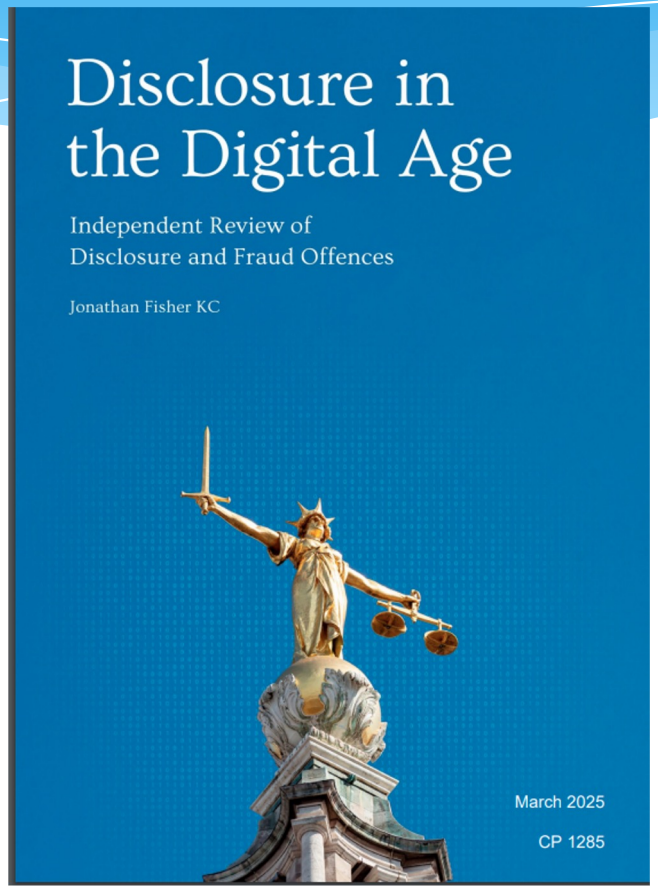
Bringing the SST up to date #2

Update the Seven Statement requirements to cater for modern systems:

5. How software is updated and maintained. This today would deal with overnight security updates and patches plus hashing and end to end encryption
6. The physical and electronic security features of the installation now also considering how computers could be remotely accessed both legitimately (by support staff working with an operator) and illegitimately.
7. How the particular computer printout came into existence and what it purports to show. In this section the person in charge can say that no faults manifested themselves during the material time which would indicate to him that the computer evidence could not be relied upon.

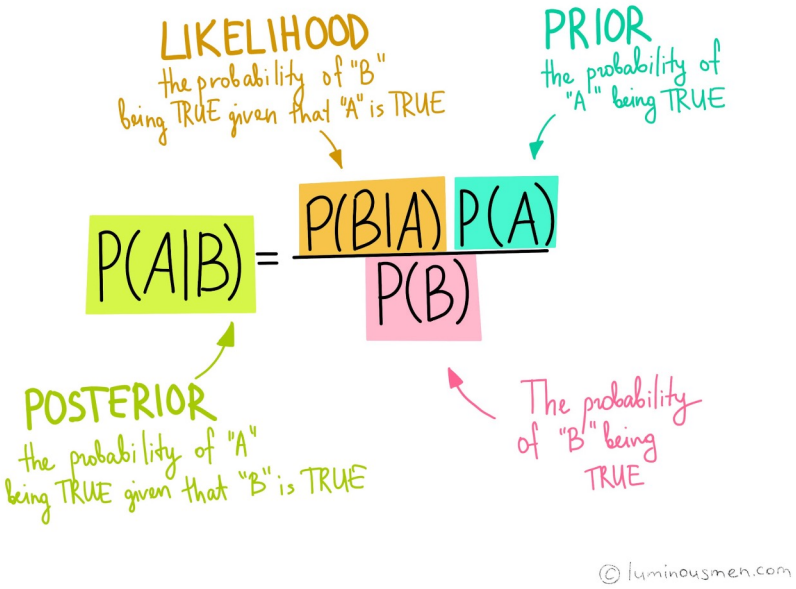
Make it Future Proof

* Update the law in line with Sir Jonathan Fraser KC's "*Disclosure in the Digital Age*"
* Only need to have a trial of computer evidence (*Voir Dire*) if the reliability of the evidence falls below a "threshold" set by Parliament
* Lawyers automatically get funded to dispute reliability if the reliability of the evidence falls below a "threshold" set by Parliament
* Establish the "threshold" by Bayesian Analysis
* Use D&O Insurance policies to drive the market and create a virtuous circle



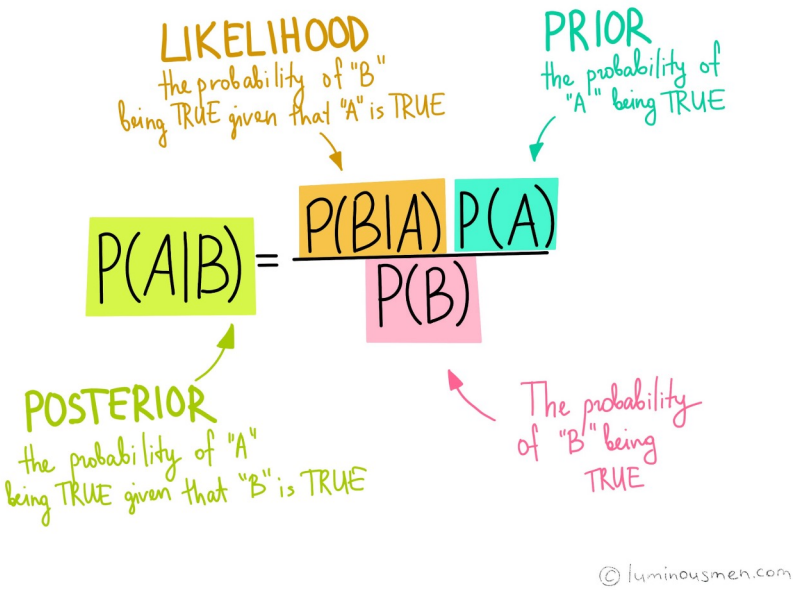
Bayesian Analysis #1

* Thomas Bayes two hundred and fifty years ago devised a mathematical means of combining the probability of certain events so that risk could be determined.
* It can be powerfully deployed to establish whether someone is guilty of a crime or otherwise by combining different pieces of evidence e.g. what weight to give to evidence of a DNA match when combined with the failure to identify the defendant in an identity parade.



Bayesian Analysis #2

* To apply it involves complex calculations which are only realistically possible through the use of computers - for most of the past two hundred years Bayes Theorem was ignored for this reason
* Applying Bayes Theorem today is done through the use of Bayesian Networks and there are mathematical tools which enable this to be done
* Used to eliminate spam mail, valuation of anything, solve crimes, prove facts



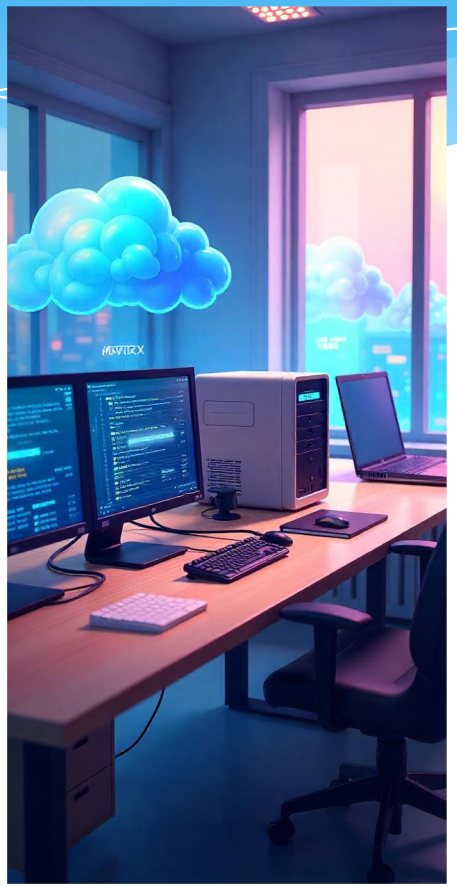
Bayesian Analysis issues

Start with a little company keeping its accounts on a computer system

* Hardware: e.g. **Dell Workstation running Windows 11 Pro**
* Application Software: e.g. **ZoHo Books**
* Cloud Service; e.g **Google Workspace**

Bayesian Analysis of :

* **Firewall, Updates, Remote Access, Cryptography, Backups, logging, chain of custody of records, physical security, documentation standards, testing et al …**
* **BYOD issues**
* **Litigation hold**



A bigger company - called “BullionTrader”

Company has custom written software

* Hardware: e.g. 100 **Lenovo ThinkCentre m70qGen5Tiny workstations running Ubunto Desktop 24.10**
* Application Software: e.g. **BullionTrader V23.43**
* Cloud Service; e.g **AWS from Amazon**

Bayesian Analysis of :

* **Firewall, Updates, Remote Access, Cryptography, Backups, logging, chain of custody of records, physical security, documentation standards, testing et al …**
* **BYOD issues**
* **Litigation hold**

aws

An Agency - called "*RatsNest*"

A tax and benefits systems for citizens WFH

Agency has custom written software under PFI agreement

* Hardware: e.g. 10,000 **F-Off Rodent workstations running Microsoft Windows Me in an emulation environment**
* Application Software: e.g. ***Kpbica* V0.43**
* Cloud Service; e.g **AWS China**

Bayesian Analysis of :

* **Firewall, Updates, Remote Access, Cryptography, Backups, logging, chain of custody of records, physical security, documentation standards, testing et al …**
* **BYOD issues**
* **Emulation issues**
* **Litigation hold**

AWS China