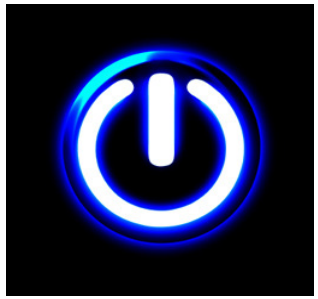
About OMICS Group

OMICS Group International is an amalgamation of Open Access publications and worldwide international science conferences and events. Established in the year 2007 with the sole aim of making the information on Sciences and technology 'Open Access', OMICS Group publishes 400 online open access scholarly journals in all aspects of Science, Engineering, Management and Technology journals. OMICS Group has been instrumental in taking the knowledge on Science & technology to the doorsteps of ordinary men and women. Research Scholars, Students, Libraries, Educational Institutions, Research centers and the industry are main stakeholders that benefitted greatly from this knowledge dissemination. OMICS Group also organizes 300 International conferences annually across the globe, where knowledge transfer takes place through debates, round table discussions, poster presentations, workshops, symposia and exhibitions.

About OMICS Group Conferences

OMICS Group International is a pioneer and leading science event organizer, which publishes around 400 open access journals and conducts over 300 Medical, Clinical, Engineering, Life Sciences, Phrama scientific conferences all over the globe annually with the support of more than 1000 scientific associations and 30,000 editorial board members and 3.5 million followers to its credit.

OMICS Group has organized 500 conferences, workshops and national symposiums across the major cities including San Francisco, Las Vegas, San Antonio, Omaha, Orlando, Raleigh, Santa Clara, Chicago, Philadelphia, Baltimore, United Kingdom, Valencia, Dubai, Beijing, Hyderabad, Bengaluru and Mumbai.




LEGAL FORENSIC

3rd International Conference on Forensic Research & Technology, October 06-08, 2014, San Antonio, USA

Cybercrime, criminal justice and the funnel effect: Challenges for forensic investigators, prosecutors and criminal justice officers

- Cameron Brown

Australian National University

Significance of subject matter

The seriousness of the 'funnel effect' in the case of cybercrime demands an inquiry into factors impeding the administration of criminal of justice to raise awareness, identify blockages, and find solutions.

- Identify the most commonly used investigative measures by police.
- Identify how cybercrime comes to the attention of police and what measures can be taken to increase reporting.
- Identify the main impediments to quantifying cybercrime incidents.
- Identify problems associated with obtaining electronic evidence.
- Identify the obstacles that impede successful adjudication and prosecution.

Digital forensics

LEGAL FORENSIC

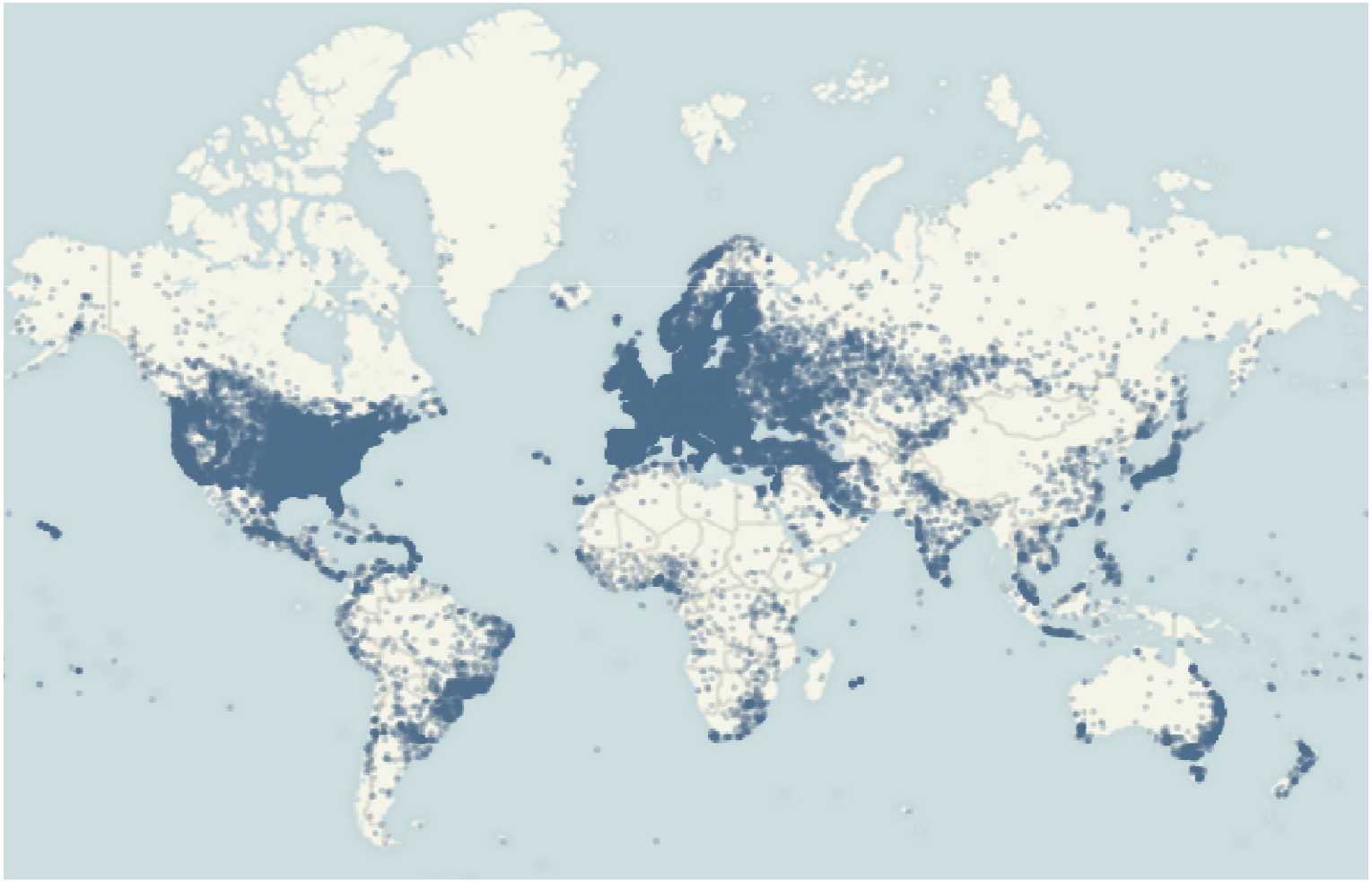
- Probative value for investigators and prosecutors in proving the 'mental aspect' / 'intent element' of various offences.

- Increasingly an integral element of high-tech investigations but also traditional civil and criminal investigations:

Unauthorized Data Duplication	Murder
Bankruptcy/Insolvency Investigation	Theft
Disloyal Employees	Assault
Industrial Espionage	Stalking
Breach of Contract	Phone 'Phreaking'
Breach of Corporate Policy	Child Exploitation Material
Private Investigations	Fraud
Due Diligence Investigations	Theft of IP
	Counterfeit/Forgery
	Insider Trading

The global challenge

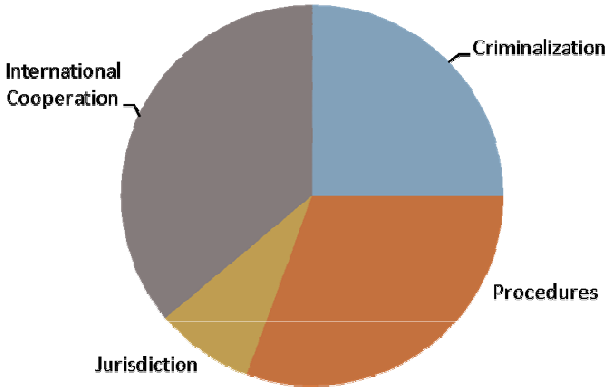
Geo-Location of Internet Protocol Addresses



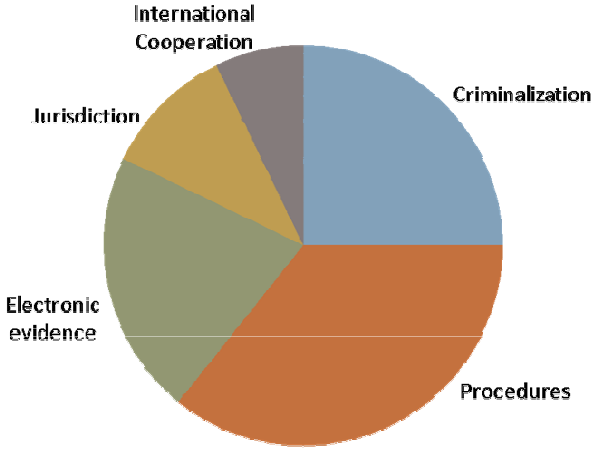
The challenge for the law

Binding	Non-binding
Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography (2000)	Commonwealth Model Laws on Computer and Computer-related Crime (2002) and Electronic Evidence (2002)
CIS Cooperation Agreement on Computer Crimes (2001)	Model Arab Law on Combating Information Technology Offences (2004)
Council of Europe Convention on Cybercrime (2001) and Additional Protocol (2003)	East African Community Draft Legal Framework for Cyberlaws (2008)
Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (2007)	HIPCAR (Caribbean) Model Legislative Texts on Cybercrime (2010)
(Draft) ECOWAS Directive on Fighting Cybercrime (2009)	COMESA Model Cybersecurity Bill (2011)
Arab Convention on Combating Information Technology Offences (2010)	SADC Model Law on Computer Crime and Cybercrime (2012)
Draft African Union Convention on Cybersecurity (2011)	
EU legislation including on e-Commerce (2000/31/EC), Personal Data (2002/58/EC as amended), Attacks against Information Systems (2005/222/JHA), and Proposal COM(2010) 517 final	

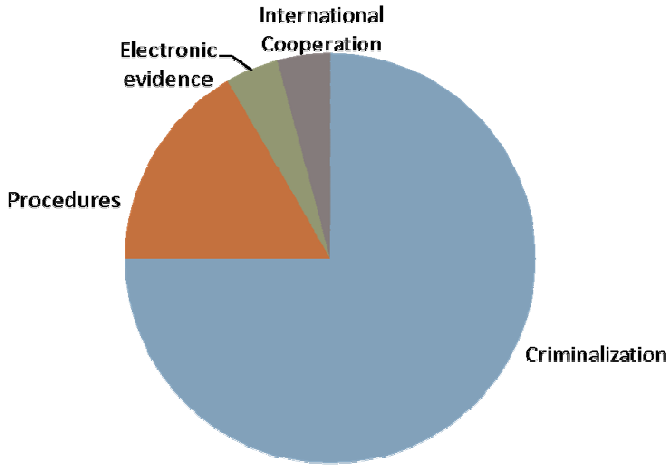
Diversity in legal approaches



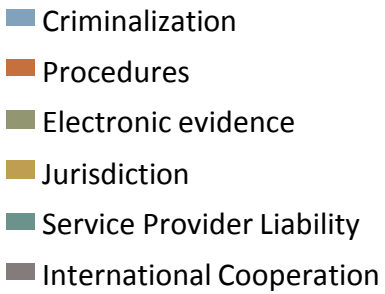
Council of Europe Convention on Cybercrime



Commonwealth Model Legislation



ECOWAS Directive on Cybercrime



Enhancing capacity

LEGAL FORENSIC

Capacity Building:

- Training for law enforcement investigators , lawyers, prosecutors and judges on investigative techniques
- Delivery of analysis tools

Prevention:

- Awareness raising
- Engagement of private sector solutions
- Research and analysis

Framework Support:

- Development of national cybercrime coordinating mechanisms
- Review and strengthening of legal frameworks

Cooperation:

- Development of public-private partnerships
- Strengthening of informal and formal international cooperation mechanisms

Technical Assistance Tools:

- Guides on comprehensive assessment, international cooperation, electronic evidence and trend monitoring

Underlying Standards:

- Respect for international human rights law
- Regional and international cyberlaw approaches

Tracing an IP - back in the day

LEGAL FORENSIC

INTERNET USER ATTEMPTS TO LOG ON VIA A MODEM

INTERNET SERVICE PROVICER

ISP HAS RIGHTS TO IP RANGE

203.64.125.0 TO

203.64.125.255

IP NUMBER

E.G. - 203.64.125.1

DYNAMICALLY SELECTED BY ISP SERVERS

IP NUMBER

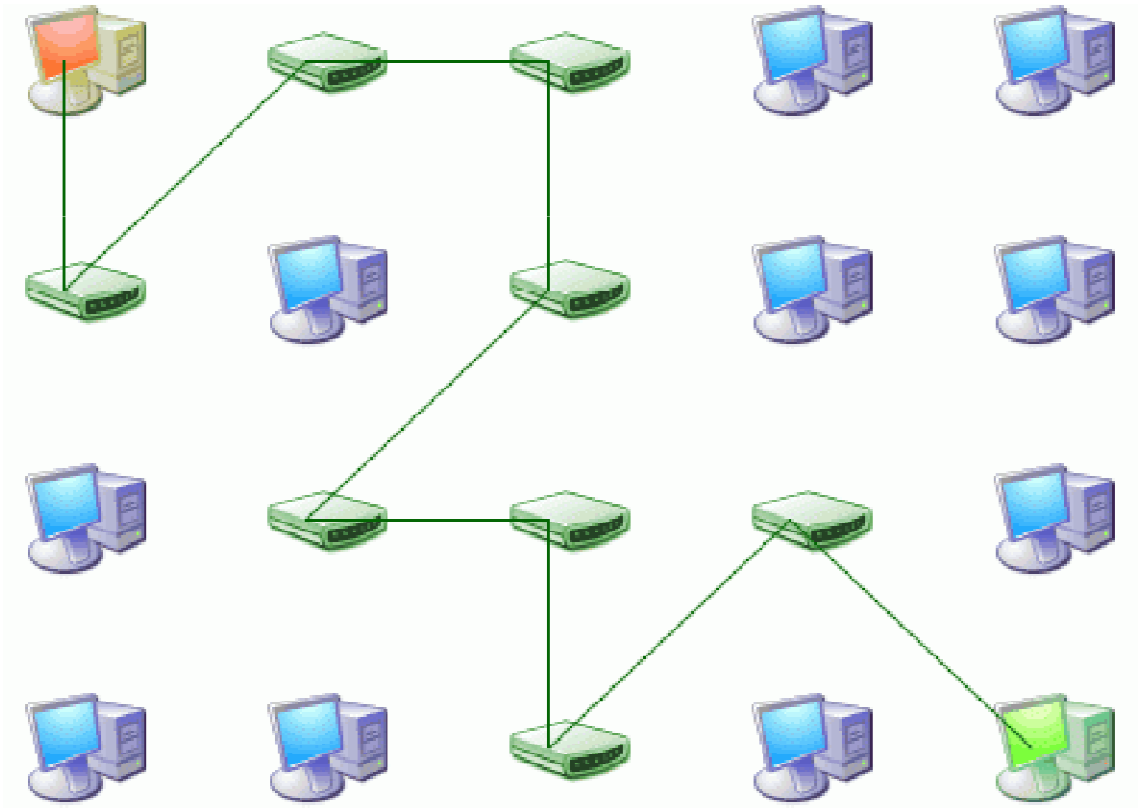
203.64.125.1 ASSIGNED TO USER on 08/11/12 at 10:15:19 CEST

INTERNET USER SENDS EMAIL OR SURFS THE INTENET AND CAN BE TRACED TO THE IP NUMBER

Evasive criminal techniques

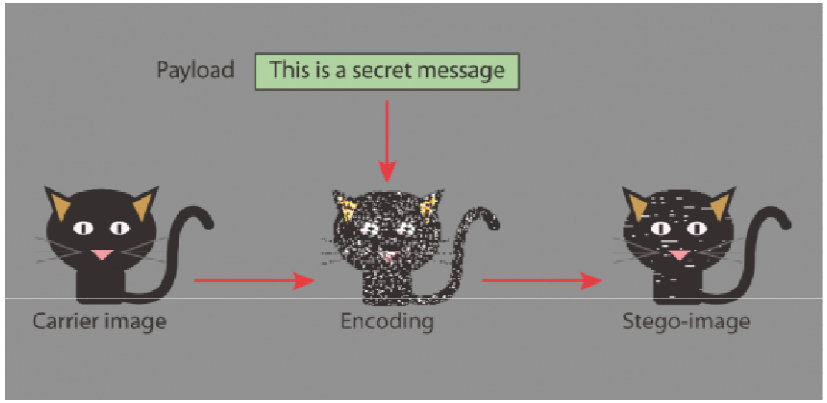
- Dead dropping
- Cryptography
- Use of codes / aliases for communication
- Anonymity networks and proxy services
- Steganography
- Compromised intermediaries
- Spoofing
- Hiding in safe jurisdictions

Anonymity networks

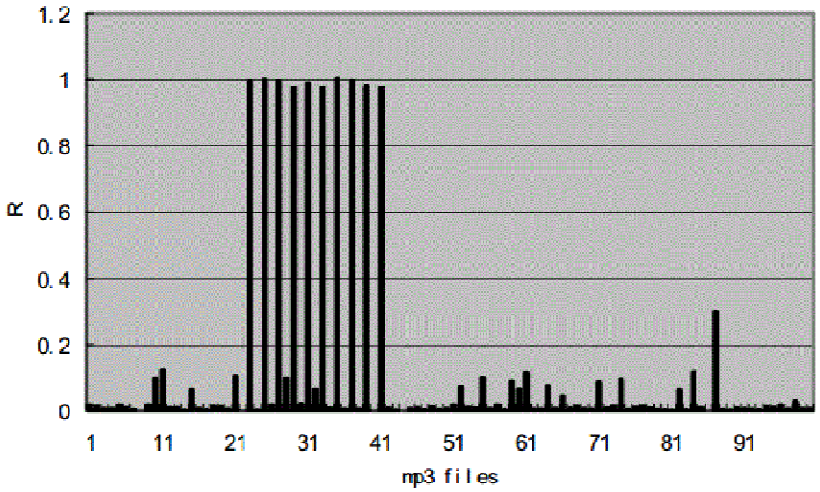


Steganography

Concealed in a graphic image file



Concealed in a sound file



Incentives
Cybercriminals

- Making money through fraud or from the sale of valuable information.
- Realising gains on the stock market by obtaining information prior to announcement of official transactions.
- Extorting money from private entities by holding data to ransom or interfering with online transactions of a commercial nature.
- Indulging in depravity by disseminating abusive material and satisfying predatory urges.

Incentives
Industrial competitors

- Stealing intellectual property and trade secrets.
- Gaining advantage in the marketplace by acquiring commercially sensitive data, such as key negotiating positions.
- Furthering privatization strategies by discrediting counterparties to a transaction.

Incentives
Foreign intelligence agencies

- Obtaining sensitive research and development information from leading manufacturers, governments, and defense contractors.
- Toppling hostile regimes.
- Sabotaging the technical developments of enemy states.

Incentives

State sponsored operatives

- Advancing homeland security through ubiquitous surveillance.
- Collaborating with likeminded nation-states to solve shared problems.
- Monitoring political speech online and silencing dissidents.
- Sabotaging international deals to safeguard and enhance domestic commercial interests, or to give local industries an economic advantage.

Incentives
Hackers

- Interfering with computer systems as an intellectual challenge or to earn respect among peers.
- Penetration testing to identify vulnerabilities.
- Reverse engineering systems to gain knowledge.

Incentives
Non-state actors

- Disrupting government services and impeding capacity of industry to function.
- Exploiting information security weaknesses to raise awareness, exact revenge or expose wrongdoing.
- Attacking critical infrastructure for political or ideological reasons.
- Circulating graphic material to traumatize adversaries and defacing digital resources to further a political agenda.

Incentives

Employees and end users

- Accidental or deliberate system misuse by users who have legitimate access or escalated privileges.
- Punishing an employer for perceived grievances.
- Monitoring or stalking a significant other.
- Planting insiders within a department to gain access to information.

Case study

- Initial Event
- Incident Report
- Police Response
- Investigation
- Jurisdictional Complexities
- Forensic Inquiry
- Legal Counsel
- Mandatory Disclosure
- Pre-trial
- Trial
- Evidence
- Experts
- Defence
- Adjudication

Challenges for administering justice
Identification

- Attributing ownership and authorship of electronically stored information (ESI) and identifying individuals in control computer systems.
- Expediently locating relevant information amongst voluminous sets of data.
- Tracing criminal activity where data anonymisation and obfuscation techniques are employed.
- Widespread availability of sanitisation and data wiping software leading to destruction of evidence.

Challenges for administering justice

Access

- Inability to obtain authorisation for search and seize of data stored remotely, particularly in relation to Cloud Service Providers.
- Bureaucracy causing delays in processing requests for mutual legal assistance.
- Lack of technical resources and absence of legal authority required to compel data production.
- Rapid advancements in strong consumer security on personal devices and ease of access to anti-forensics.

Challenges for administering justice
Human resources

- Lack of qualified digital forensic personnel required to operate equipment, discover evidence, and assist investigators and prosecutors in the preparation of reports, delivery of expert testimony, and the demystification of the technical underpinnings and probative value of ESI.

- Scarcity of law enforcement officers and prosecutors with technical expertise and mindset to investigate and prosecute cybercriminals.

Challenges for administering justice
Wellbeing

- Performance pressure and stressful working conditions for criminal justice officers.
- Prolonged exposure to obscene material throughout the course of an investigation.
- Inexperienced supervisors who lack capacity to provide for the welfare of first responders and technical personnel.

Challenges for administering justice
Liability

- Interruption of business operations during warrant activity.
- Disclosure of private or legally privileged information during the course of an investigation.
- Inadvertent damage to information systems whilst seizing exhibits and during forensic analysis, leading to criminal, civil, and/or administrative liability.

Challenges for administering justice
Internal policies

- Disinclination to commit time and money towards investigating cybercrime offending that is not congruent with existing policy preferences or public priorities.

- Absence of police standard operating procedures for handling electronic evidence.

Challenges for administering justice
Retrieval and retention

- Failure to collect ephemeral sources evidence from live systems.
- Failure of service providers to respond to authorised requests for production and preservation of data.
- Failure to action data retention and preservation requests in a timely manner, leading to loss of evidence.

Challenges for administering justice
Admissibility and fairness

- Failure to maintain chain-of-custody documentation or demonstrate evidence integrity.
- Inability to demonstrate the reliability or authenticity of computer generated and computer stored information.
- Defendants unable to afford to engage forensic services to test findings or challenge opinions.
- Analytical subject matter is predominately submitted by the prosecution, and evidence is produced almost exclusively on behalf of the prosecution.

Challenges for administering justice
Technical resources and funding

- Inadequate analytical tools for acquiring, processing and presenting electronic evidence, such as dedicated crime laboratories and forensic facilities.

- Court rooms not equipped with modern technology for presenting electronic evidence.

- Failure to maintain updated forensic equipment for gathering and extracting electronic evidence.

Challenges for administering justice
Underreporting and uncertainty

- Low proportion of cybercrime offending brought to the attention of police due to widespread underreporting.

- Problems for investigators and prosecutors in identifying and obtaining appropriate legal authority for gathering electronic evidence caused by gaps in legislation and administrative delays owing to judicial uncertainty vis-à-vis manifestations of cybercrime.

- Defence lawyers creating confusion with novel legal arguments and experts overstating or understating findings.

Challenges for administering justice
Privacy and privilege

- Investigative powers transgressing fundamental rights of suspects and accused persons.

- Doctrine of legal professional privilege delaying investigations and adding complexity to legal process and data analysis.

Challenges for administering justice
Cooperation

- Lack of cooperation by private sector entities in responding to requests for assistance from law enforcement.

- Delays attributable to strict formal cooperative mechanisms and ineffectual international instruments that impede capacity to combat cybercrime originating outside national borders.

Challenges for administering justice
Legal frameworks and due process

- Lack of harmony between legal frameworks.
- Data protection and privacy laws putting high value information beyond the reach of law enforcement.
- Failure of legislative provisions to keep pace with advancements in technology and practical realities of conducting cybercrime investigations.
- Unrealistic legislative time constraints related to processing electronic evidence with the consequence that a large volume of data is never analysed.

Challenges for administering justice
Training

- Insufficient understanding among investigators, prosecutors, and the judiciary concerning:

  - Trans-jurisdictional complexities
  - Diplomatic and legal processes
  - Conflicts between the laws of disparate nation- states
  - Sovereignty issues
  - Information communication technology (ICT)
  - Sources of electronic evidence

Thoughts and questions

"The justice system's inability to prosecute cybercrime cases is a sign that it is not functioning effectively in this area" – Susan Brenner, 2004.

Australian National University

LEGAL FORENSIC

Pursuing the root causes of crime will never cease because our understanding of the origins of criminality will have to be continuously revised as society evolves and technology marches forward.

Cameron Brown

Master of Policing Intelligence and Counter Terrorism
Master of International Security Studies
Grad.Cert. Computer Crime Investigation
LL.B., B.A. (Behavioural Science)
Technical: Certified Data Recovery Expert (CDRE)
A+, Network+, Security+
Creative: Ad.Dip. Music (Commercial) - Performance

Let Us Meet Again

We welcome you all to our future conferences of OMICS Group International

Please Visit:

www.omicsgroup.com
www.conferenceseries.com