The image features a central graphic of a fingerprint, where the ridges are represented by white circuit traces on a blue background. The background is filled with faint binary code (0s and 1s).

The Evolution of Electronic Evidence under Maltese Law

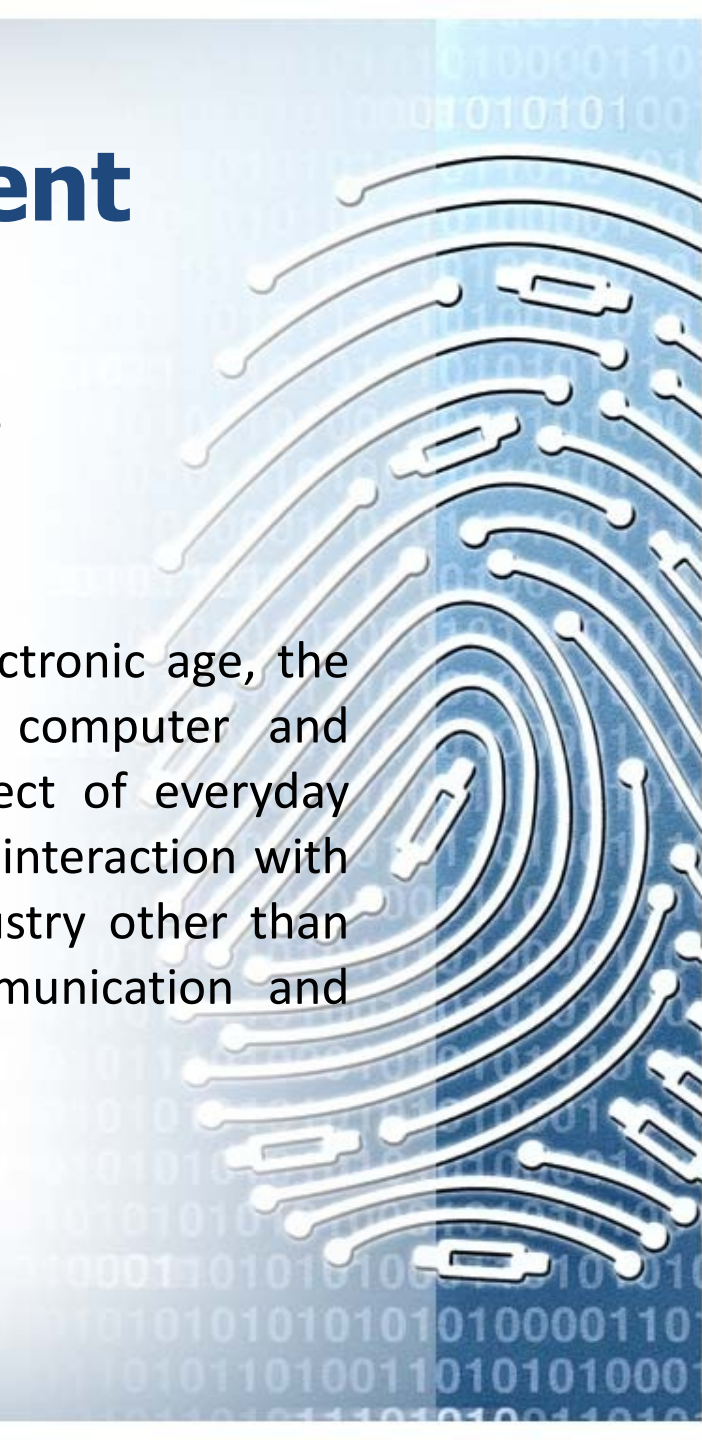
**What a
first responder
needs to know**

Opening Statement

Vincit Omnia Veritas

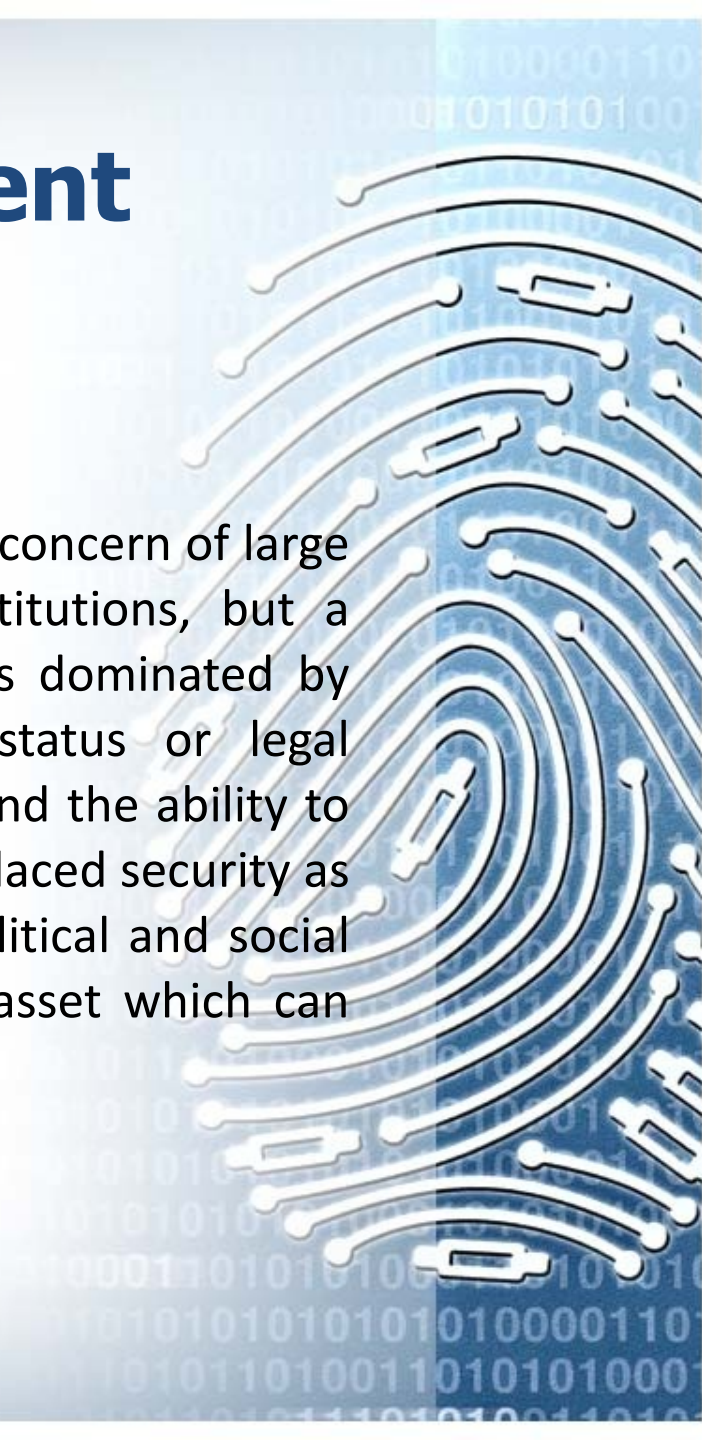
TRUTH CONQUERS ALL THINGS

- We live in what has been termed as the electronic age, the result of proliferation and integration of computer and communication technologies into every aspect of everyday life. As a result it is very difficult to conceive interaction with any government institution, business or industry other than through the generation of electronic communication and electronic interaction.



Opening Statement

- Computer and network security is no longer a concern of large organisations and military and financial institutions, but a concern for all those who use technology as dominated by computing devices, irrespective of class, status or legal personality. The dependence on technology and the ability to connect devices into one global network has placed security as a critical core issue. In today's economic, political and social context information has become a valuable asset which can have serious repercussions if compromised.



The electronic evidence evolution



- 1977
- The United States of America attempts to legislate computer misuse on a federal basis through the Ribicoff Bill
- This bill was not adopted but proves that as early as 1970, members of the United States Congress were contemplating the dangers of computer crime
- The Computer Fraud Abuse Act of 1986 was a federal legislation of significance



Computer Crime

- 1980
- John Draper a former United States Air Force engineer became known as Captain Crunch.
- Draper used his engineering knowledge and a whistle as a means of exploiting phone systems.
- This form of tampering became known as PHREAKING the ancestor of what later became known as HACKING.
- In 1986 United States federal legislation made **unauthorized access** a criminal offence even if no damage is caused.

The relevance of unauthorized access



- As a legal principle any criminal offence requires two important elements, *Mens Rea* and *Actus Reus* (guilty mind and criminal act)
- Of equal importance is the onus of proof which rest with the prosecution.
- Early legislators realized that through such intrusion (unauthorized access) it was possible that the intruder may have **accidentally** caused damage, even without malicious intent or actual intent.
- The personal computer and the internet further complicated unauthorized access as a result jurisdiction issues or **CYBERSPACE**

Europe

- In 1985 the European Union was closely looking at international and local developments setting up a European Committee on Crime Problems (CDPC).
- The Council of Europe set up a Committee of Experts on Crime in Cyber-space (PC-CY) which met in secret for several years drafting an international treaty.
- The Convention on Cybercrime which was released in final form in June 2001.
- This convention set out the framework proposals for Member States and Non-Member States to transpose these into their respective domestic legislation.

Convention on Cybercrime



The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.

It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention is divided into 48 articles in 4 chapters.



The United Kingdom

- The first Computer Misuse laws enacted originated from recommendations of the Scottish and English Law Commissions.
- However it soon became clear that a number of scenarios still created significant problems most significantly the issue of jurisdiction.
- The Computer Misuse Act of 1990 attempted to resolve these issues encompassing three main offence categories;

The United Kingdom continued

- Unauthorized access to computer material
(*Ellis v DPP [2001]*)
- *Unauthorized access with the intent to commit or facilitate or the commission of a further offence*
(*R v Delamare [2003]*)
- *Unauthorised modification of computer material by the introduction of viruses, corruption of programs or data.*
(*R v Vallor [2003]*)



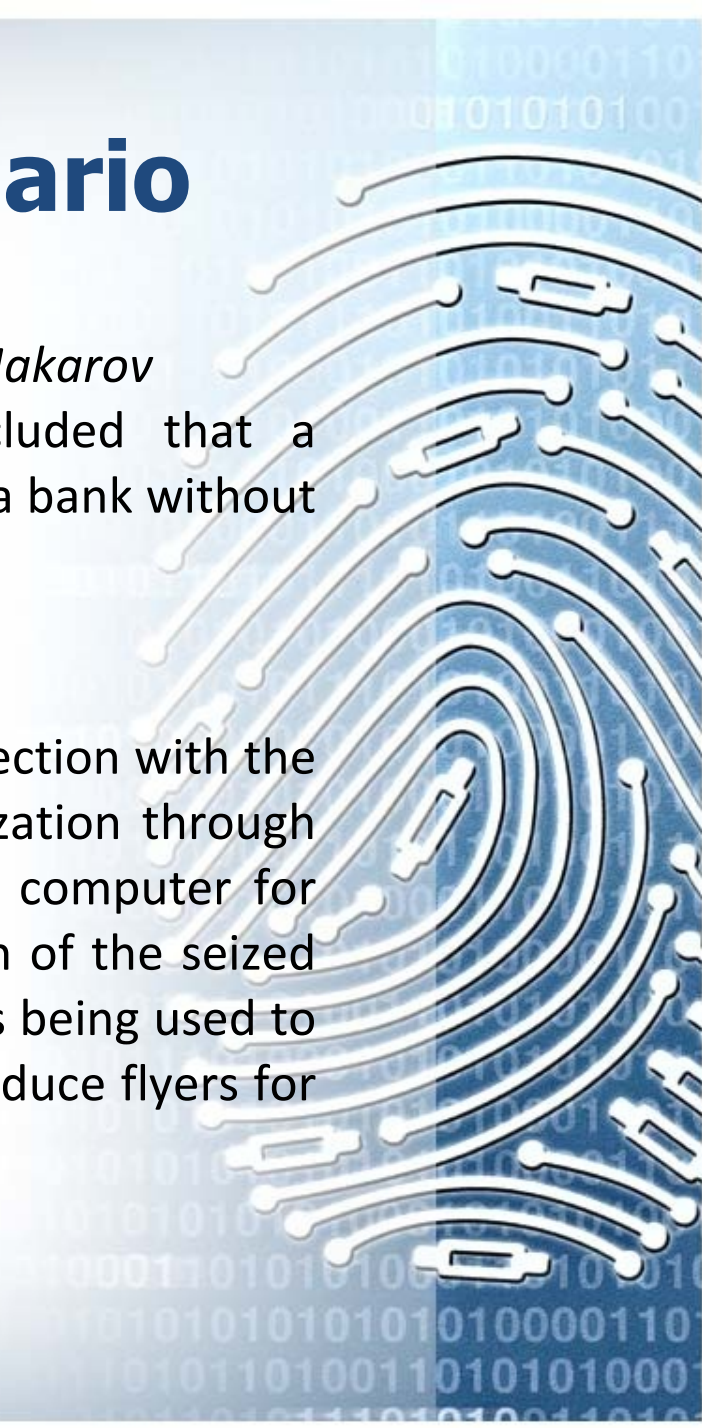


The United Kingdom continued

- The 1990 amendments did not provide a complete solution to all problems relating to unauthorized access.
- In *R v Bedworth* the British legal system still required the prosecution to prove intent. The defendant used his drug addiction as a defence claiming that the influence of drugs prevented him from forming any intent.
- In *R v Cropp* the judge acquitted the defendant due to lack of specialist knowledge on the subject of computers.
- In *DPP v Bibnell* a police officer who accessed the Police National Computer to obtain information for his own use could not be prosecuted under the definition of the Act.

The Maltese Scenario

- *Police vs Vitaliy Platanov and Police vs Alexei Makarov*
In both cases forensic investigations concluded that a computer network was being used to operate a bank without a licence.
- *Police vs Carmen Spiteri*
Spiteri was investigated and arraigned in connection with the setting up of a fictitious philanthropic organization through which she collected donations to purchase a computer for administration purposes. Forensic examination of the seized computer revealed that the said computer was being used to surf the internet and to play games and to produce flyers for private parties.





The Maltese Scenario continued

- Also of interest was the additional comment, regarding the proposed bills:
- *“These three bills, when enacted, will not only position Malta as a leading hub for electronic commerce, but they will also afford a competitive edge in a fast-evolving global economy. In addition, these laws will permit for a quality leap in all government services as they establish a critical foundation for the attainment of e-Government”.*
- This multi facet approach was a clear message of the Government’s intention to place Malta on the map as a leader in e-commerce, a position it clearly holds in relation to the e-gaming and online gaming services.

Legislative Milestones



- 1977 - Attempt to legislate through the Ribicoff Bill [USA]
- 1986 - The Computer Fraud Abuse Act [USA]
- 1990 - The Computer Misuse Act [UK]
- 2001 - The Convention on Cyber Crime [Treaty]

The Treaty was released in final form in Budapest in June 2001. It took another three to four years to be introduced within the major Council of Europe member states.

Malta introduced major technology relevant legislation before signing up to the Treaty and ahead of other major EU Member States and years before becoming a EU Member State.



Major IT related legislation

- The Electronic Commerce Bill - Chapter 399 (10-May-01)
 - Introduced for the purpose of setting the mechanism for conducting e-commerce and the processing of electronic transactions.
 - Originates from the Electronic Signature Directive (1999/93/EC) and the Electronic Commerce Directive (2000/31/EC).
 - The basis of this law is founded on the Australian Electronic Transactions Act which is in turn based on Article 6 of the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures.
 - The main definitions of which have been taken from the Irish Electronic Commerce Act, which are in turn taken from the Electronic Signature Directive (1999/93/EC).



Major IT related legislation

- The Data Protection Bill - Chapter 440 (22-March-02)
 - introduced for the purpose of covering all automatic processing of personal data and it also includes provisions on certain manual processing. The bill originates from the Data Protection Directive (95/46/EC).
 - A noteworthy Change is LN 198 of 2008 introducing data retention requirements in relation to telephony and internet.
- The Computer Misuse Bill - Never materialised
 - Instead on the 10th May 2002 the provisions of the bill had been transposed into the Chapter 9 – The Criminal Code under Article 337B *et seq.*
 - An extensive list of definitions precede the provisions of the Law.

Definitions and Differences



- Elements of Computer and Data:

computer, computer data, computer network, computer output, computer software, computer supplies computer systems, function and support documentation

- The term *computer* in our legislation is a misnomer since the law provides the following definition:

“... an electronic device that performs logical, arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, software and communication facilities that are connected or related to a computer system or network”

Definitions and Differences



- The main differences between the Convention and Maltese Legislation:
 - i. The quality of the device
 - ii. The distinction between any device as opposed to an electronic device
 - iii. The performance of the device
- Under Maltese Law the relevance of the medium is its integrity and not the data it stores
- Furthermore the Maltese Legislator ensure to give *data* and *output* the widest possible interpretation – irrespective of whether it is in in human readable form



Classification of Offences

- Computer Related Offences
 - Fraud, Forgery and Misappropriation which in essence could be defined as economic crimes
- Computer Content Offences
 - Crimes which fall under the heading of those against the Peace and Honour of the Families and against Morals, such as child pornography
- Computer Integrity Offences
 - offences against the confidentiality, integrity and availability of computer data and systems



Classification of Offences

- Computer Integrity Offences *continued...*

The Maltese law provisions also included specific provisions on the commission of an offence outside Malta. Article 337E, and the burden of proof, article 337F(6). The legislator ensured that:

- i. If any act is committed outside Malta which act had it been committed in Malta, would have constituted an offence, then such act is to be deemed as have been committed in Malta.
- ii. It shall not be necessary for the prosecution to negate by evidence any authorisation. The burden of proving any such authorisation shall lie with the person alleging such authorisation, the mere uncorroborated testimony of the person charged is not sufficient to discharge this liability.

Maltese Judgments

- Since 2002, judgements on infringements of Articles 337B to 337H amounted to (34) judgements
- twenty-nine (29) have been admitted upon arraignment
- four (4) cases have been disputed
 - two (2) of which have been adjudged guilty
 - while the remaining two (2) have been acquitted. In one case the complainant (the wife of the accused) withdrew the charges.



Maltese Judgments



In the cases where an admission of guilt had been registered during arraignment, the defendants were first time offenders and the defence seems to have opted for an early admission rather than a defence.

In one case the Magistrates' Court concluded that the accused was an Internet Service Provider (ISP) drawing the definition of an ISP from Wikipedia.

Question Time





First Responders



Search and Seizure

- The original intentions on the legislative framework proposed that Computer Misuse would be an Act in its own right. This Act would have been cited as the Computer Misuse Act 2000. The proposed provisions regarding Search and Seizure found in the White Paper were more detailed than the provisions found in the Criminal Code.

“337G. The Minister may, for the purpose of this Sub-title by regulations prescribed:

- the manner in which the Police may search computers, computer systems or computer supplies and seize data software stored therein;*
- procedures and methods for handling evidence that is in an electronic form”.*



Search and Seizure

- The seizure and handling is not regulated.
- Hence the strict adherence to the chain of custody principles must be upheld at all times.
- However, besides setting their own standards, the police and court experts tend to follow some form of procedure or guidance set by reputable organisations,.
- Two of these sources are ;
 - “The Good Practice Guide for Computer-Based Electronic Evidence” published by the Association of Chief of Police Officer (ACPO)
 - “The Best Practices for Seizing Electronic Evidence, A Pocket Guide for First Responders” published by the U.S. Department of Homeland Security, United States Secret Service



Search and Seizure

- Handlers of electronic evidence must observe four principles:
- Any device under custody which is to be subsequently to be relied upon as evidence, must have no changes in its structure or data.
- If circumstances warrant that access is made to the original data on the device in question, then this should be carried out by a competent person legally recognised and capable of explaining the relevance and implications of his/her actions.
- A detailed audit trail of all processes applied in the process of the examination of the electronic evidence should be retained, such that an independent third party may be capable of replicating the processes and achieving the same result.
- At all times during the process and examination of the electronic evidence, the principles of chain of custody and the law are upheld.



Search and Seizure

- The relevance of the above mentioned principles are of paramount importance under Maltese Law since all evidence is admissible as long as it is relevant which is contrary to the theory of the fruit of the poisonous tree.
- Hence, whilst evidence, irrespective of its source, is admissible as long as it is relevant under Maltese procedural law, the only way to effectively exclude or create sufficient doubt on the probative value of the electronic evidence is to attack it in terms of chain of custody and contamination.

Rules on Electronic Evidence



- The prosecution will present evidence in order to prove beyond any reasonable doubt the probative value of the evidence.
- The defence will attach such evidence by contradicting or claiming that it has been contaminated with the objective to raise sufficient doubt on the probative value of the evidence produced.
- Traditional evidence is given probative value on the basis its biological link to the victim or suspect.
- Electronic evidence gains probative value when considered in relation to human ingenuity in light of its specific character and nature
- A defence counsel mindful of these differences will endeavour to disassociate the accused from the electronic device.

Rules on Electronic Evidence



- It is relevant to note the following in relation to the digital world.
- That the digital world is nothing more than the processing of human manual interaction in electronic format is correct
- While that the digital world is the electronic interaction or association between a human and the process is incorrect.
- A clear example of this arises in cases where the generation of an electronic signature occurs. Unlike a handwritten signature, where the manuscript signature links the document to a person, a digital signature links the document to a device.

Traditional trace evidence

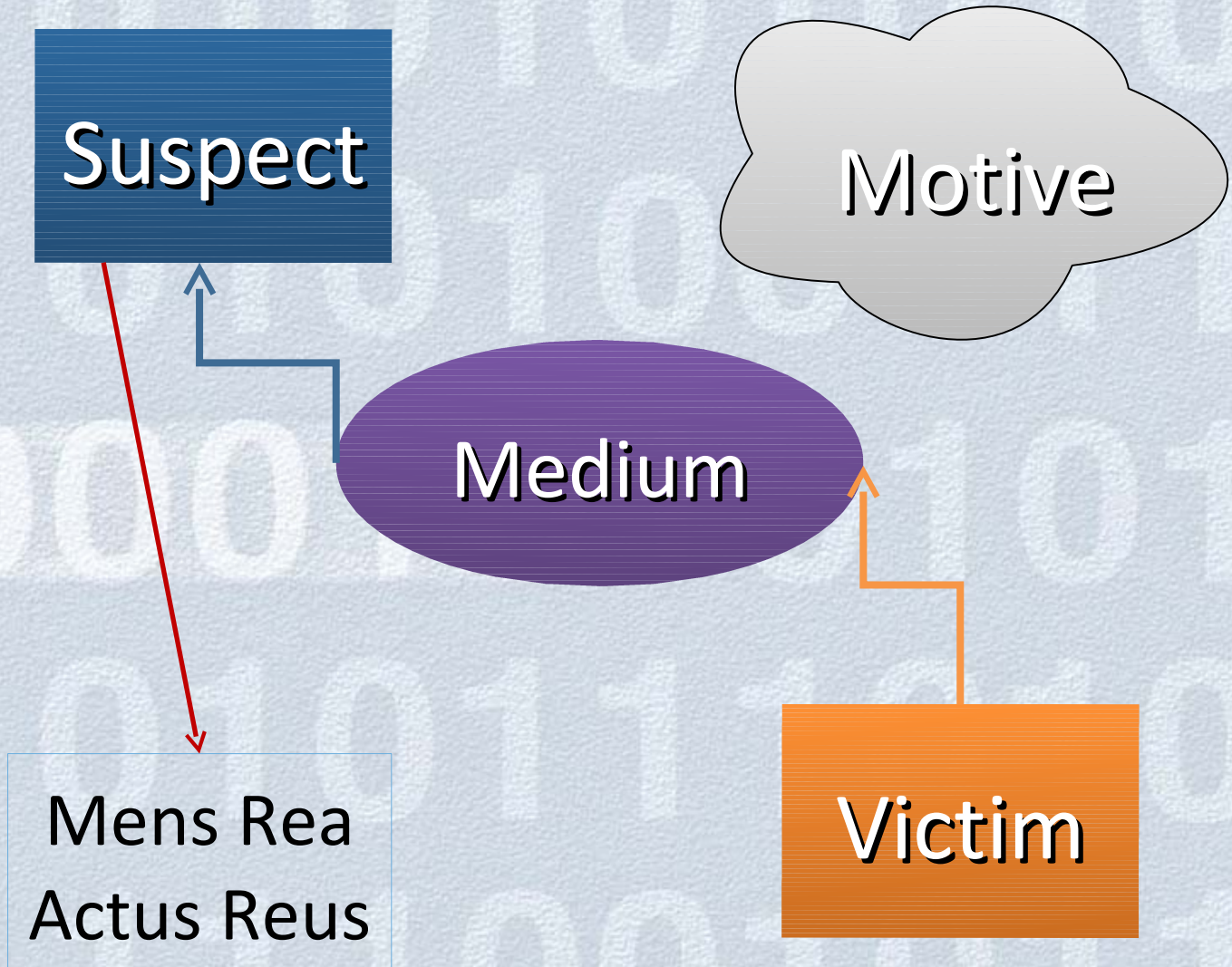
Suspect

Motive

Medium

Mens Rea
Actus Reus

Victim



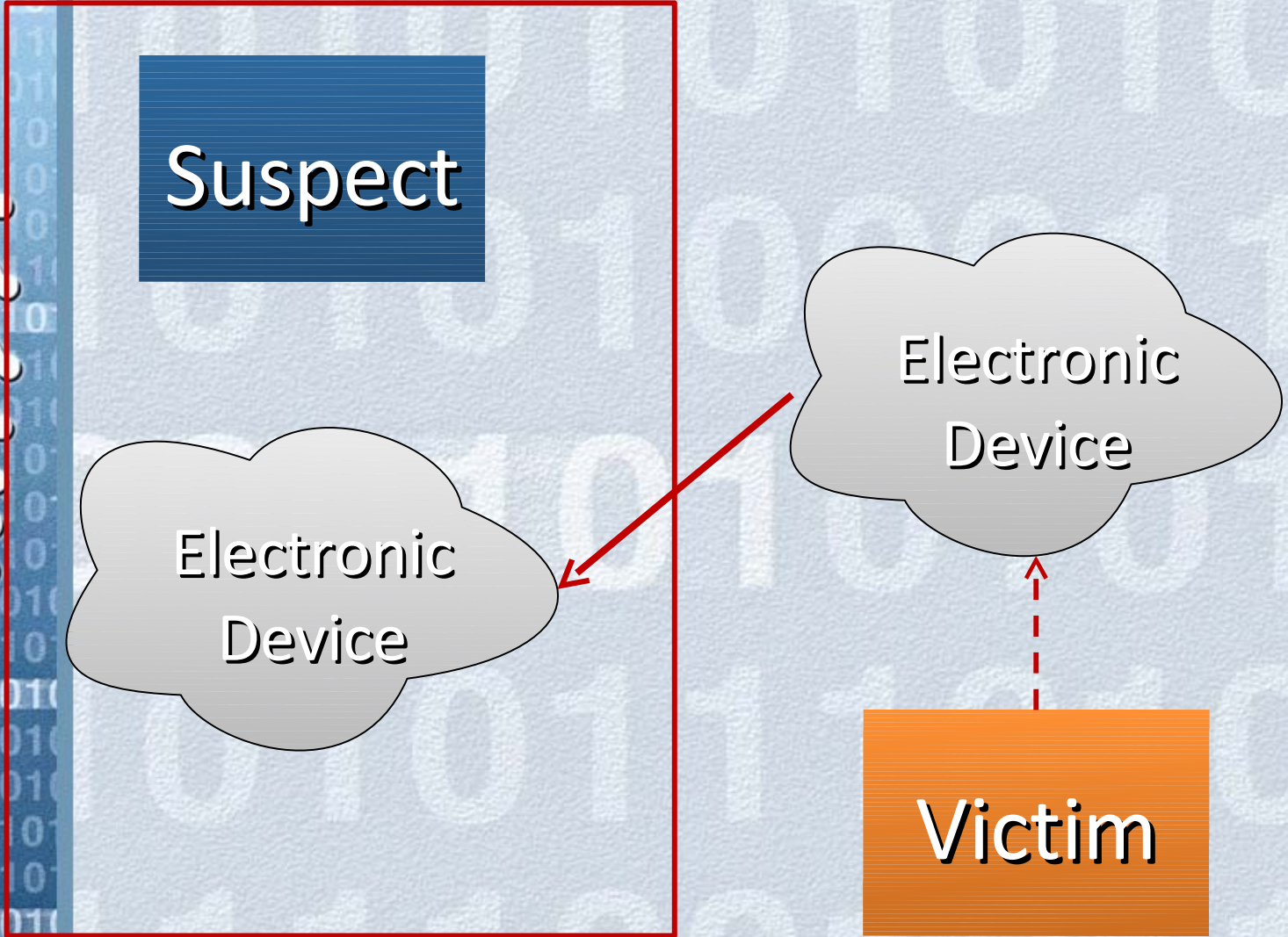
Electronic trace evidence

Suspect

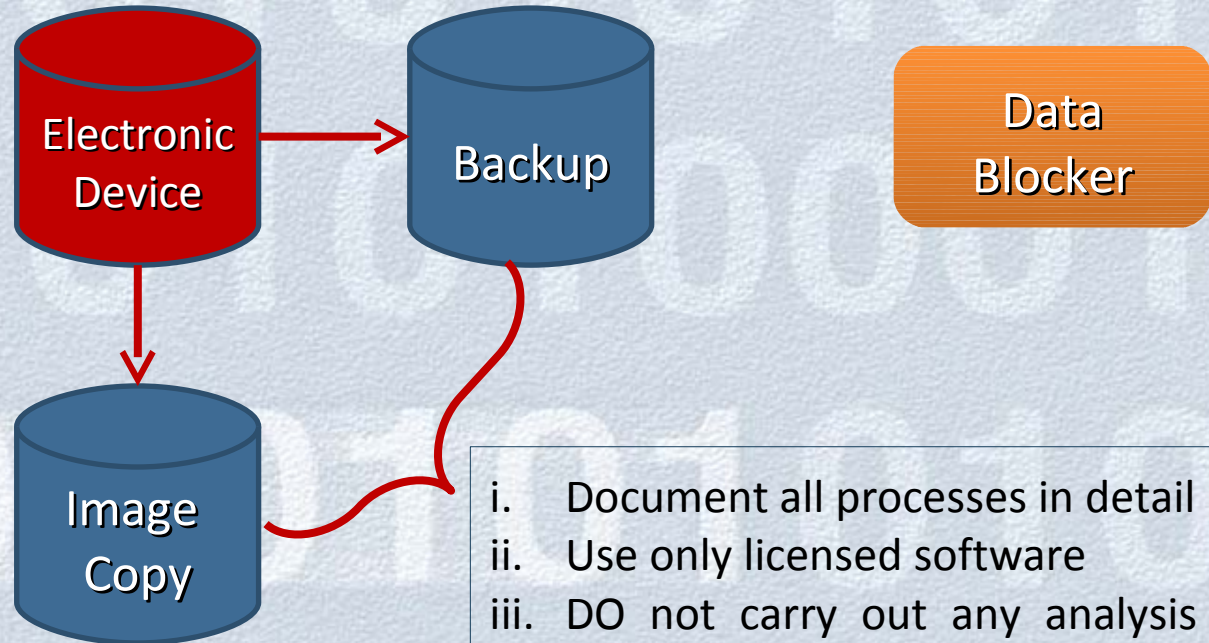
Electronic Device

Electronic Device

Victim



Examination



- i. Document all processes in detail
- ii. Use only licensed software
- iii. DO not carry out any analysis on a trial and error basis
- iv. Conclude on the evidence but do not forward any opinion
- v. If possible work in pairs and both sign off the documentation
- vi. Once you have established the facts do not attempt further analysis.

Chain of Custody

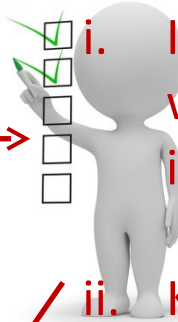
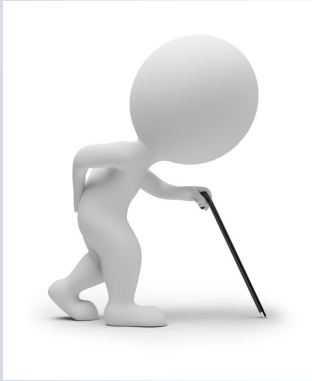
- The relevance of the chain of custody principle has tremendous importance under Maltese Law. If the defence prove that at any given time whoever had custody lost absolute control over the exhibit or that the exhibit could have been subject to an external or third party influence, than reasonable doubt to it having been contaminated could arise.
- Contamination and reasonable doubt are elements which erode the probative value of electronic evidence.



Evidence Presentation

- In any investigative proving the facts is on the ultimate objective.
- Evidence needs to be understood by lay persons who will adjudicate its probative value.
 - Always use the simple methods of analysis.
 - Always use software which lay users are familiar with, this facilitates their cognitive value of the evidence.
 - Always be concise and objective in any report you draw up.
 - If you are unable to prove a point or fact do not use suppositions, and never assume any event or fact.
 - Remember that in a Criminal Court the probative value of any evidence must be on a basis of beyond any reasonable doubt.

Environment



7 FT	2.13 M
6 FT	1.83 M
5 FT	1.52 M
4 FT	1.22 M
3 FT	0.91 M



i. Insist to be present when their complaint and investigation is interviewed and investigation

i. If you find it

i. If you identify a

ii. Keep minutes of the meeting and conduct your complaint investigation same. you

suspect remember

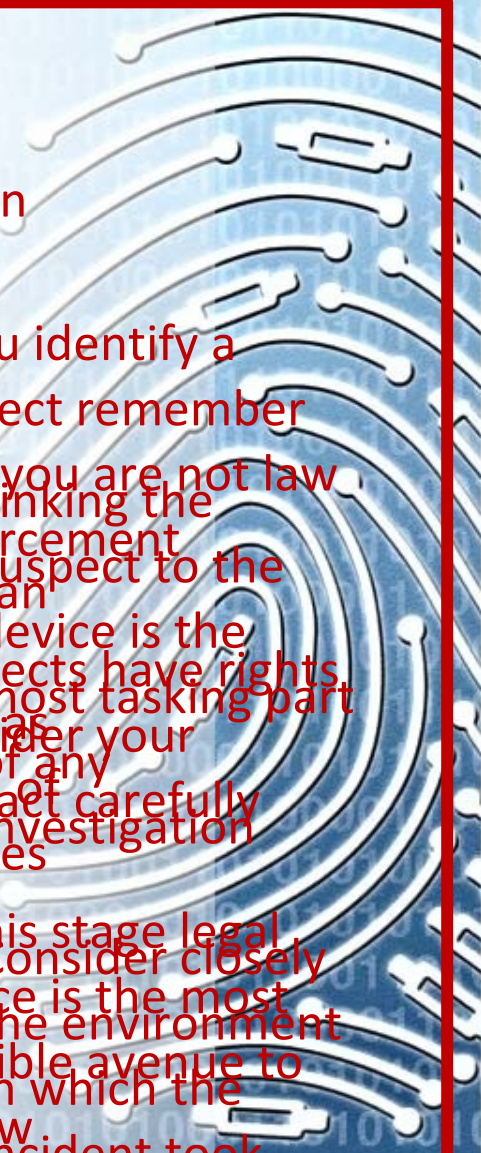
that you are not law enforcement suspect to the device is the most tasking part of any investigation

iii. Collect and update your any related documents to your meeting report

ii. Suspects have rights consider your contact of carefully investigation

iii. Report objectively your findings

iii. At this stage legal advice is the most sensible avenue to follow in which the incident took place





First Responders Objectives

- Collect details on the incident reported.
- Immediately ensuring that chain of custody is guarantee once incident has been reported.
- If analysis of the electronic evidence is necessary before a complaint with law enforcement is made, ensure that this analysis is fully documented.
- If you are unable to conduct such an investigation get expert help.
- Do not rely on hearsay evidence, also ensure that you verify the information with the original source.
- The most tasking part is to factually link a suspect to an electronic device, consider the environment this may provide the link.
- Never assume or suppose anything.
- Protect against possible contaminates such as lack of chain of custody and cross contamination.



Question Time



THE END

Thank you for your attendance time and patience

Dr. Martin Bajada FIAP., LL.B., LL.D.
19 'Gazebo'
Triq Guzè Mercer Street
Qormi – QRM 2686

Tel: 2144 3820

Mbl: 7940 3144

Email: mbajada@mbajada.com