# Postgraduate Diploma in IT Forensics

Week 8 of Module 5: Collecting Digital Evidence and Presentation in Court

*Hayson Tse, PhD (HK), Adjunct Lecturer, HKUSPACE*

*9 May 2019*

## Contents

# 1 Prologue

## 1.1 Help

- Blue means `"I am a link; please click me."`

## 1.2 Contact info

- Personal email
  - hayson.tse

## 1.3 Copyright




## 1.4 Disclaimer

- All materials come from the public domain. There are no government or trade secrets.
- Newspaper clippings may or may not contain the complete sets of allegations in relation to a case.
- A person who has been reported by newspaper clippings as being arrested or charged is presumed innocent until he is convicted or even until his appeal against conviction is dismissed.

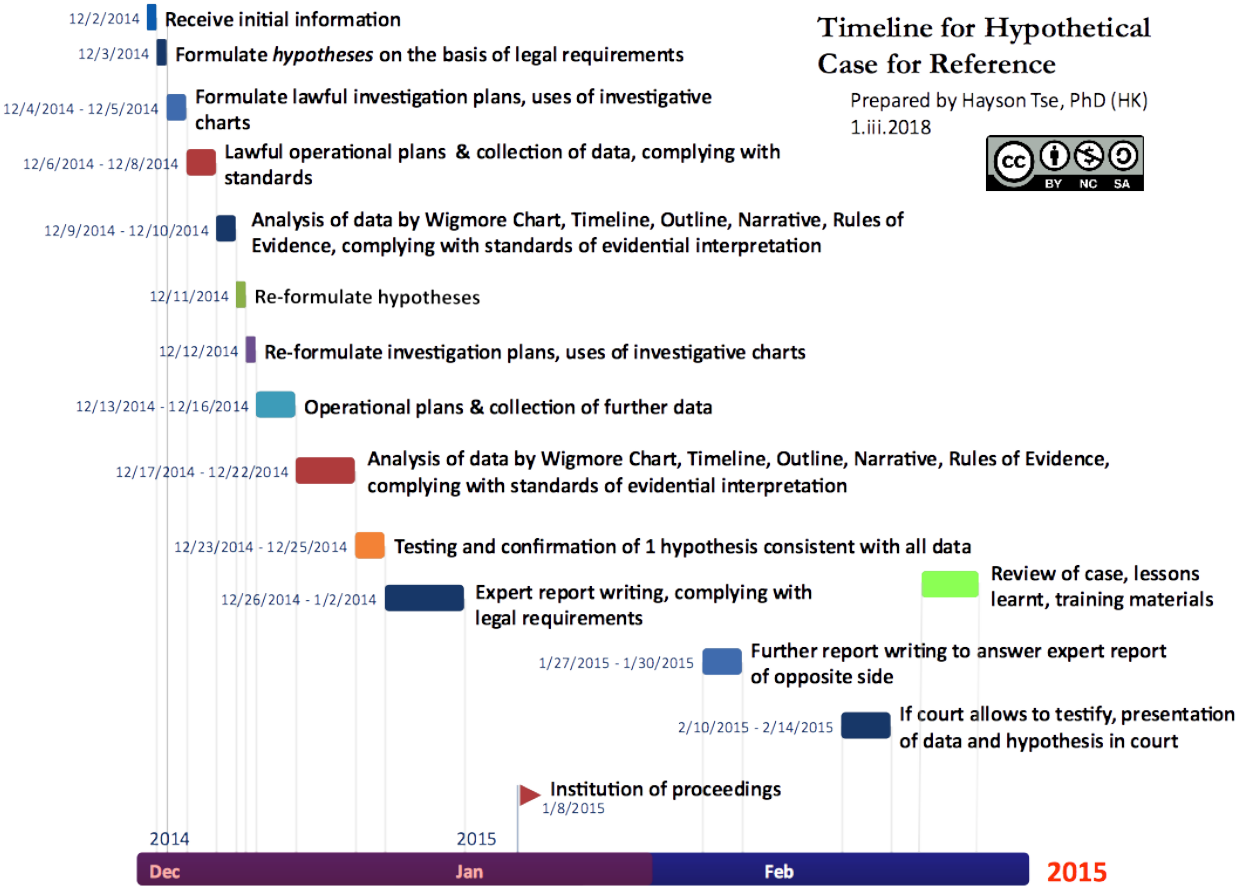
## 1.5 Classroom regulations

- HKU SPACE Handbook
  - No reservation of seats.
  - No eating or drinking.
  - Turn off all mobile phones and pagers.
  - No smoking at all HKU SPACE learning centres and the University campus.
  - *No video / audio recording, unless with the permission of the Programme Director / Manager*
  - The Programme Direction / Manager may impose any conditions when granting the permission.
  - No unattended personal belongings.

## 1.6 Important dates

- Assignment: 2 May 2019
- EXAMINATION: 6 June 2019

## 1.7 Overview of your work cycle



# 2 Mistakes and defence

## 2.1 A Case

- *HKSAR v.Kwok Po-lun* DCCC 64/2012; Reasons for Verdict
- Offences:-
  - one charge of possession of child pornography, contrary to section 3(3) of the Prevention of Child Pornography Ordinance (Chapter 579)
  - one charge of publishing child pornography, contrary to section 3(2) of the Prevention of Child Pornography Ordinance (Chapter 579)

## 2.2 Summary of allegations

- Police executed a search warrant at the defendant's home
- Police seized three computers, one from the bedroom of the defendant
- 62,284 images and 639 films suspected to be child pornography were stored on the computer
- Admitted in evidence at trial was that of these 40,954 images and 510 films were child pornography

## 2.3 Digital information

- Only valid user account of the computer was "Alan"
- Access was set as system administrator
- Child pornography was found in four different locations within D drive, the vast majority in folders named "eMule" and "My Pictures"
- 30,580 images and 624 films of suspected child pornography were found in "eMule"
- "eMule" was installed using the account "Alan" (How and why do you know?)
- The programme files of "eMule" belonged to the account "Alan" (How and why do you know?)
- The account "Alan" was last used to execute the programme "eMule" on the 14 April 2010, the day before arrest. (How and why do you know?)
- 31,704 suspected child pornographic images were stored in My Pictures
- 15 'link files' containing suspected child pornography in a folder of the account "Alan"
- Account "Alan" had, between the 12 January 2010 and the 15 April 2010, the day of arrest, been used to access the files to which the link files pointed
- The incoming file path where "eMule" was used to store downloaded and uploaded files was D:
- All files in this path were set to share via the internet thus permitting access by the public
- The file sharing status of "eMule" confirmed a total of 9 images and 501 films containing suspected child pornography had been shared via the internet
- In respect of one film 'ChildAmerica.avi' (child pornography) for which there had been 996 requests of which 30 had been accepted for uploading resulting in a total of 2.92 MB data from the file being uploaded and shared onto the internet

## 2.4 Prosecution expert

- No challenge to the expertise of PC 3379 (What was the expertise?)
- PC 3379 was put forward as 'computer expert' (Was this correct?)
- What should be the 'area of expertise'?
- PC 3379 had not prepared what can properly be called an expert report setting out all his findings
- PC 3379 only prepared a series of witness statements each addressing the specific requests made of him by the officer in charge of District Investigation Team 6 of Sau Mau Ping
- He was not requested specifically by the officer in charge of the case to consider whether the computer had been hacked. PC 3379 did not include his findings in any of his statements or disclose this information until he was asked in court.
- PC 3379 agreed he had never asked to look for signs of hacking and therefore had made no reference to hacking in any of his witness statements. In fact he had already analysed the chance of the computer being hacked. The details were recorded on his computer but because no one requested them.

## 2.5 Criticism by the trial judge

- His Honour Judge Dufton:

  "In my view a full report setting out all findings and not just limited to the specific requests should be prepared and this should also include the reply to any defence expert report. However it is right to say at no time was PC 3379 ever asked to prepare a full expert report whether by the officer in charge; the Department of Justice or anyone in the prosecution team."

  "I should add that in order that the court could fully understand all aspects of the expert evidence this necessitated repeated explanations by the experts and lengthy questioning by the court at the end of the evidence of each expert."

- (What if there were a good expert report?)

## 2.6 How defendant was linked to the files?

- DPC 33596 testified that after the father had let the police to go inside the flat, the defendant was seen to walk out of the bedroom where the computer was found
- DPC 33596 asked the father whose bedroom that was and to whom the computer belonged.
- The defendant and answered saying it was his bedroom and his computer. DPC 33596 however made no written record of this reply at the time in his notebook or at the police station in the investigation report. The first record was made five months later in his witness statement.

- PC 3379 found two valid user accounts "Alan" and "Guest", however only "Alan" was activated to accept password logon whereas "Guest" was not activated
- The defendant was employed by Yung Shiang International (HK) Limited and his work email was "alan . . . ."
- PC 3379 found two Microsoft word files; four Microsoft excel files and 74 email files which related to a male, Kwok Po Lun (the name of the defendant) and Alan (How this evidence was presented in court? What were the time …)
- Inside the flat was the defendant, his father and the step-mother

## 2.7 When the police seized the computer was the child pornography on the computer?

- On 15 April 2010, PC 58917 examined the computer found at the home of the defendant. He used the image search function of 'SPADA' no child pornographic images were found.
- PC 58917 told the court that although he was aware at the time of his examination of the shortcomings of 'SPADA' he made no record of this in his witness statement.
- On 23 April 2010, PC3379 performed the process of 'Forensic Image Acquisition' by using computer forensics software 'EnCase' and found the child pornography.
- After PC 58917 completed the preliminary examination of the computer DPC 33596 attached 'anti tamper' labels to the switches of the computer. Part of one of the labels AD 014391 was not covering a switch found on the side of the computer. The other label AD 014392 was found on the back of the computer just below a switch.
- The computers were then taken to the police station and kept under a desk in DPC 33596's office without being locked away.

## 2.8 The defence case

- HKSAR v. Kwok Po Lun [2015] 3 HKLRD 84
- The Court of Appeal summarise the defence case:

> "7. The applicant did not avail himself of his right to give evidence, but did call Dr Ajay Kumar to give evidence as an expert witness in respect of computer technology. However, Dr Kumar had not conducted a physical examination of the applicant's computer."

> "8. The defence case was that the evidence of the location of the computer at the time of its seizure was unreliable. It had not been proven that the room from which the computer was seized was the applicant's bedroom. Further, the possibility that others, such as the applicant's parents who also resided in the flat, might have accessed the computer for their own purpose could not be excluded. . . ."

> "8. . . . Also, third parties could have secretly caused the child pornography to

be stored in the computer either by entering the applicant's flat to gain physical access to the computer, or by remotely accessing it or by hacking into it. Finally, it was suggested that, given the poor level of security obtaining during the time that the computer was in the custody of the police following its seizure, the possibility was that the material could have been installed on the computer after its seizure by the police."

### 2.9 Outcome of the case

- The trial judge said:

"107. Taking into account the following matters:"

> "1. physical access was by password only and "Alan" is the only account which could access the computer;"
>
> "2. that the defendant is the "Alan" using the computer;"
>
> "3. access was set as system administrator which meant that the defendant had access to everything on the computer(see paragraph 11, exhibit P9);"
>
> "4. the vast majority of the child pornography was located in either "eMule" or "My Pictures", both commonly used sites;"
>
> "5. "eMule" was installed using the account "Alan", and"
>
> "6. the account "Alan" had been used to access the child pornographic files to which 15 link files pointed"

"I am satisfied so I am sure the only inference to draw is that the defendant controlled and knew of the existence of the child pornography on the computer. Further I am satisfied so I am sure the only inference to draw is that the defendant also knew the exact nature of the material was child pornography."

## 3 Purpose of cross-examination

### 3.1 Areas of cross examination

- Investigation with a view to negate defence; areas of cross examination of the State's computer forensic expert in a child pornography case by Messrs Garland, Samuel and

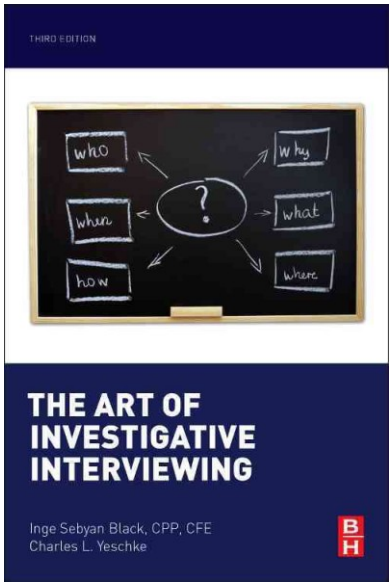
Loeb, Atlanta Trial Attorneys

- Exclusion of evidence
  - Search warrant obtained by false or misleading information
  - Search exceed the scope of warrant
  - Person giving consent did not have proper authority
- Forensic integrity destroyed
- Meta data unreliable due to fault of investigation
- Elements of offence not proved
  - Images not of child
  - Images not of pornography
- No reason to suspect
- Images "saved" automatically
- Images in cache never seen because images were located in lowest part of a webpage not displayed on the monitor
- Images seen but "saved" automatically as cache
- Images downloaded as part of larger download of non-illicit material
- Name of images did not describe child pornography and were never viewed after download
- Images placed by computer or another person unknown to defendant
- Virus downloaded the images
- Images embedded in emails (unknown to Defendant)
- cross-examination to show computer examiner does not understand the following issues
  - electronic file properties
  - allocated v. unallocated / slack space
  - file paths
  - ".link files"
  - windows history
  - Internet web page caching
  - global unique identifier of the images downloaded by officer before search
  - software used for examination
  - P2P file sharing program
  - timeline

# 4 Investigative plan

## 4.1 Book: The Art of Investigative Interviewing

- Black and Yeschke. The Art of Investigative Interviewing:




## 4.2 Names used in the book

- First Responder: a person who is first on the scene after an incident or the first Forensic Laboratory Foren- sic Analyst on the scene of an incident
- Forensic Analyst: a person responsible for performing forensic work on a case in the Forensic Laboratory
- Forensic Team: the Forensic Analysts deployed on a given case
- Incident Manager: the person managing an incident irrespective of what organization they are from
- Lead Forensic Analyst: the person who is in charge of a team of Forensic Analysts. Where there is only one Forensic Analyst in the Forensic Team, he or she is the Lead Forensic Analyst for the case.
- Officer in the Case also known as the Case Officer: the lead investigator in a case

## 4.3 Chapter 6

- Title: Public and private interviewing

> "Regardless of whether an offence is investigated by public or private detectives, the evidence needed to prosecute the case is the same. If a piece of evidence is to be (or, for that matter, to society), the methods used to it must meet the . This is true even when the collected evidence serves only to justify an employee's dismissal rather than prosecution in court. The case may turn ugly if the fired employee sues the company for wrongful termination and the company must produce the evidence on which it based the termination."

## 4.4 Chapter 12

- Title: Internal Controls: Issues to be considered
- What was the source that provided initial information and under what terms? (That is, informant, whistleblower, co-conspirator, witness, etc.)
- Determine who might be allowed into the knowledge of an ongoing investigation.
- Who will you want to interview and what information might they have?
- Determine whether the allegations fall under criminal conduct or an internal discipline matter.
- Address any conflicts of interest by anyone connected to the investigation.
- Be prepared to document everything related to this case.
- Who in the company needs to be notified of the investigation? (That is, human resources, legal department, auditing, financial department)
- What evidence will you need to gather to prosecute this case?
- Know and follow all relevant company policies.
- Consider all laws that might apply.

## 4.5 FBI: Functions of an investigation plan

- FBI Law Enforcement Bulletin, 68(6), 22 - 25
- Focus the investigative process to ensure that all litigation elements are addressed;
- Limit unnecessary procedures and step duplication;
- Coordinate the activities of numerous personnel on large cases;
- Provide stability to the investigation if staff changes occur
- Enhance communication with legal authorities:
  - by providing an outline of the investigation;
  - identifying strengths and weaknesses in the case;
- Provide a framework for the final report;
- Become a training aid for inexperienced staff members.

## 4.6 FBI: Law Enforcement Bulletin articles

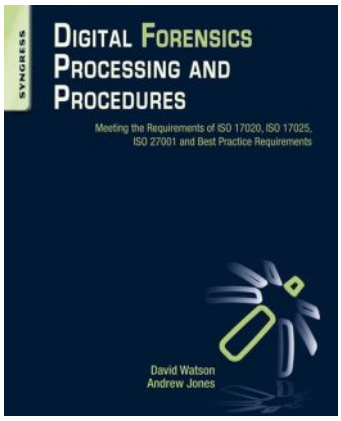
- Digital Forensic Examination: A Case Study (fingerprints shown in a digital image)
- Digital Evidence (ensuring suitability for presentation in court)
- Analysis of Digital Financial Data
- Virtual Currency: Investigative Challenges and Opportunities
- Searching Cell Phones Seized Incident to Arrest
- Searches Incident to Arrest in the Smartphone Age
- Executing Search Warrants in the Cloud

# 5 Forensic laboratory

## 5.1 Book

- Andrew Jones, David Lilburn Watson. Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements. Syngress; 1 edition (October 1, 2013).

  "This is the first digital forensics book that covers the complete lifecycle of digital evidence and the chain of custody. This comprehensive handbook includes international procedures, best practices, compliance, and a companion web site with downloadable forms. Written by world-renowned digital forensics experts, this book is a must for any digital forensics lab. It provides anyone who handles digital evidence with a guide to proper procedure throughout the chain of custody–from incident response through analysis in the lab."




## 5.2 Contents

- Introduction
- Forensic Laboratory Accommodation
- Setting up the Forensic Laboratory
- The Forensic Laboratory Integrated Management System
- Risk Management
- Quality in the Forensic Laboratory
- IT Infrastructure
- Incident response
- Case Processing
- Case Management
- Evidence Presentation
- Secure Working Practices
- Ensuring Continuity of Operations
- Managing Business Relationships

- Effective Records Management
- Performance Assessment

## 5.3 Chapter 3

- Setting up the Forensic Laboratory

## 5.4 Forensic Laboratory Terms of Reference

- stakeholders
  - owning organisation of the Forensic Laborary
  - the team
- basis of the relationship
- Terms of Reference (ToR)
- Created during the earliest stages of the project for the establishment of the Forensic Laboratory
- purpose and structure of the Forensic Laboratory
- define and verify the scope of the Forensic Laboratory
- measure success of the Forensic Laboratory
- basis for future decision
- common understanding of the scope among the stakeholders
- what needs to be achieved, by whom and when
- identifies the set of deliverables that satisfy the requirements and the scope
- identify the success factors, risks, and boundaries
- written in some detail and should include:
  - vision;
  - scope and objectives;
  - deliverables;
  - boundaries, risks, and limitations;
  - roles, responsibilities, authority, accountability, and reporting requirements;
  - stakeholders;
  - the regulatory framework;
  - resources available;
  - work breakdown structure and schedule;
  - success factors;
  - intervention strategies.

## 5.5 Contents of ToR

- Vision
  - a short statement, normally of one or two paragraphs
  - explains the mandate given to the team
  - defines the reason for the Forensic Laboratory's creation and its purpose
- Scope and objectives
  - define the scope of the work

  - specify the work to be undertaken
  - specify types of deliverables
  - Give timescales for the production of deliverables
  - Deliverables
  - Define deliverables include
    * outcome of investigation
    * internal deliverables such as accounts, audits, and test results and reports
- Boundaries, risks and limitations
  - describes where the process/system/operation starts and ends
  - authority delegated to the Forensic Laboratory to implement changes
  - powers given
  - mention systems, policies, procedures, relevant legislation, etc.,
  - give detail risks
- Roles, responsibilities, authority, accountability, and reporting requirements
  - policy defines:
    * roles, responsibilities, and functions of each employee working within the Forensic Laboratory
    * the authority that is associated with each of the roles
    * accountability associated with each of the roles
    * reporting requirements for each role and task
    * actions to be performed during both routine work activities and an incident
    * who is responsible for, and authorized to contact which internal teams and external organizations and under what circumstances
- Stakeholders
  - identify the main stakeholders and their interests, roles, and responsibilities
  - stakeholders
    * representatives of the owning organization
    * Forensic Laboratory employees
    * Clients
    * other parties who have an interest in the efficient running of the Forensic Laboratory
- Regulatory framework
  - framework for the operation of the Forensic Laboratory
    * legal
    * institutional
    * contractual
  - Regulations
    * European Union
    * Federal (National)
    * State (Provincial),
    * Municipal Governments
    * domestic legislation
  - policies and practices that pertain to parent corporations, partnerships, etc.
- Resources
  - real estate,

  - administrative support;
  - available budget;
  - employees;
  - materials and supplies;
  - other supporting functions (e.g., security);
  - resources available and how they are to be accessed;
  - information processing equipment (business and forensic);
  - training requirements and how this will be provided.
- Work breakdown structure and schedule
  - Work breakdown is a structure of a list of tasks that require action.
    * work broken down into smaller and smaller tasks
  - Schedule
    * individual tasks
    * relevant dependencies
    * timelines
      · task durations
- Success factors (SFs)
  - also known as Critical Success Factors
  - identify aspect of the company business that have targets to be reached and maintained
  - define
    * factors or activities required for ensuring the success
    * measurement of those factors
      · measurable and associated with a target goal
  - measurements examples
    * the number of jobs processed in the month
    * number of hours spent on each task
  - examples which need target
    * laboratory processes
    * staff
    * organization skills
    * tools
    * techniques
    * technologies
  - Intervention strategies
    * define what constitutes an emergency
    * contingency plans for any emergency
- Status of the forensic laboratory
- Give details of
  - the ownership
  - the services that it will offer
  - the structure of the laboratory
  - the standards that it will work to
  - the expected customers.

## 5.6 The forensic laboratory principles

- 23 principles
- Responsibilities
- Users of the Forensic Laboratory relies on:
  - reputation of the Forensic Laboratory
  - abilities of their Forensic Analysts
  - the standards of the profession
- Forensic Laboratory relies on Laboratory Manager to develop and maintain an efficient, high-quality forensic laboratory
- Roles of Laboratory Manager is making decisions and judgments in balancing:
  - scientific principles
  - requirements of the Criminal Justice System
  - effects on the lives of individuals that may be subject of an digital forensic investigation
- Integrity
- Forensic Team
  - honest and truthful with their
    * peers
    * supervisors
    * subordinates
  - trustworthy and honest in representing the Forensic Laborator
- Quality
- Forensic Team
  - implement quality assurance procedures
  - monitor and verify quality of work
  - compliance with ISO 9001 and ISO 17025
- Efficiency
- Forensic Team
  - provide products and services which maximizes organizational efficiency
  - ensures an economical expenditure of resources and personnel
- Productivity
- Laboratory Manager
  - establish reasonable goals for the production of forensic casework in a timely fashion
  - Give highest priority to cases which have a potentially productive outcome and have an effective impact on the enforcement or adjudication process
- Meet organizational expectations
- Laboratory Manager
  - implement and enforce the relevant organizational policies and procedures
  - establish additional internal procedures designed to meet ever-changing needs of forensic case processing
- Health and safety
- Laboratory Manager
  - aim: reasonably assure safety in the Laboratory and in the field

  - plan and maintain systems to achieve aim
  - systems include maintenance of records of injuries, and routine safety inspections
  - compliance with health and safety procedures prescribed by law and industry
- Information security
- Laboratory Manager
  - planning and maintaining the security of the Forensic Laboratory
  - control of access 24 x 7
  - compliance with ISO 27001
- Management information systems
- Laboratory Manager
  - developing management information systems
  - provide information in a timely manner
  - current and past work
- Qualifications
- The Laboratory Manager
  - hire employees sufficient academic qualifications or experience
  - provide employees with fundamental scientific principles
  - assure that they are honest, forthright, and ethical in their personal and professional life
- Training
- Laboratory Manager provides training:
  - principles and details of forensic science as applied to the work of Forensic Laboratory
  - handling and preserving the integrity of physical evidence
  - processes and procedures as well as for the specific tools to be utilized
  - develop a full training program for all Forensic Analysts and Investigators
- Maintaining employee competency
- Laboratory Manager
  - monitor the skills and proficiency
    * continuing basis
    * annual basis
  - maintain ongoing program of training, awareness, and competency
- Employee development
- Laboratory Manager
  - foster development of Forensic Analysts and Investigators for greater job responsibility
  - support internal and external training,
  - provide sufficient library resources
    * keep abreast of changing and emerging trends in forensic science
  - encouraging Forensic Analysts and Investigators
    * keep abreast of changing and emerging trends in forensic science
- Environment
- Laboratory Manager
  - ensure safe and functional work environment
    * adequate space to support all the work activities

        * adequate facilities to protect evidence from contamination, tampering, or theft
- Supervision
- Laboratory Manager
  - set up performance evaluation process
  - provide the Forensic Analysts and Investigators with adequate supervisory review
  - ensure quality of work product
  - accountable for
    * performance of the Forensic Analysts and Investigators
    * enforcement of processes, procedures and policies
  - ensure
    * realistic performance goals on account of reasonable workload standards
    * no unduly pressured to perform substandard work through case load pressure or outside influence
- Conflicts of interest
- All must avoid any activity, interest, or association that interferes or appears to interfere with their independent exercise of professional judgment.
- Laboratory Manager
  - set up Forensic Laboratory Conflict of Interest Policy
- Legal compliance
- Laboratory Manager
  - ensure operational procedures in compliance with legislative, good practice and procedural requirements
  - establish and publish operational procedures
- Accountability
- Laboratory Manager and the Lead Forensic Analyst
  - accountable for their decisions and actions
  - decisions and actions
    * supported by appropriate documentation
    * open to legitimate scrutiny
- Disclosure and discovery
- Forensic Laboratory records must be open for reasonable access when legitimate requests are made by Officers of the Court or other legitimate requesters.
- Work quality
- Laboratory Manager
  - establish a quality assurance program
- Forensic Analysts and Investigators
  - accept responsibility for evidence integrity and security; validated, reliable methods; and casework documentation and reporting
- Compliance with ISO 9001 and ISO 17025
- Accreditation and certification
- Laboratory Manager
  - achieve and maintain certifications and accreditation that the Top Management deemed necessary
- Membership of appropriate organizations
- Laboratory Manager

  - ensure Forensic Team joins appropriate professional organizations
  - encourage Forensic Team obtain the highest professional membership grade possible
- Obtain appropriate personal certifications
- Laboratory Manager
  - ensure Forensic Team achieves appropriate certifications of both generic and tool-specific types to demonstrate their skill levels
- Laboratory service level agreements
- A Service Level Agreement (SLA)
  - a "promise" containing a definition of the level of service service of the Forensic Laboratory
  - also known as (a description of) the quality of the work (usually called the "Turn Round Time")
  - provide in plain language using easily understood terms
  - provide standard of measurements that are measurable and tested on a regular basis
- A business contract normally include SLAs within the terms of agreement to to define the level of service
- The SLA forms an essential element of the legal contract between the Company and the customer

## 5.7 Impartiality and independence

- Compliance with ISO 17025
  - able to show evidence that its work and results are "free from undue influence or pressure from customers or other interested parties" and that "laboratories working within larger organizations where influence could be applied (such as police laboratories), are free from such influence and are producing objective and valid results."

## 5.8 Codes of practice and conduct

- In the United Kingdom, the Forensic Regulator has produced Codes of Practice and Conduct for forensic science, October 2017.
  - ISO 17025 is a mandatory standard for Digital Forensics laboratories in the United Kingdom (UK) as of October 2017. All laboratories that are not ISO 17025 certified must disclose their 'non-compliance' on every report produced.

## 5.9 Quality standard

- (What is forensic?)
- Supplier of forensic services
  - maintain highest possible standards
- Quality standards in forensic science are best attained through accreditation
  - ISO 17025, ISO 9001

## 5.10 Objectivity

- Measures to reduce threats to compliance with objectivity, such as:
  - advising the management of the Forensic Laboratory of the potential threat
  - Forensic Analyst or Investigator removing themselves from the case
  - Forensic Laboratory having in place suitable peer review and supervisory procedures
  - terminating the relationship that gives rise to the threat

## 5.11 Management requirements

- Implement Integrated Management System (IMS) based on the Publicly Available Specification 99:2012 (PAS 99:2012) (last updated by BSI/ISO) (discussed in Chapter 4 of the book)

## 5.12 Insurance

- regularly review its insurance coverage
  - jurisdiction
  - business undertaken
  - specific contractual requirements
  - number of employees

## 5.13 Policies

- Clear statements covering:
  - all of the major forensic issue, including
    - subcontracting
    - contacting law enforcement
    - carrying out monitoring
    - conducting regular reviews of forensic policies, guidelines, and procedures
  - only allow authorized personnel to carry out their tasks
  - special policy for incident handlers
- review and update at frequent intervals
- consistency with
  - right to privacy
  - general data protection principles and regulations
  - all applicable laws

## 5.14 Guidelines and procedures

- purpose
  - consistency in processing materials
  - consistency in same standard
  - admissibility in court

  - demonstrate integrity of data
- for all tasks relating to processing forensic cases and management systems
- for outsourcing (Chapter 14 of the book)
- consistent with
  - parent companies
  - all applicable laws
- guidelines include
  - step-by-step procedures for per- forming the routine tasks, such as imaging (cloning) of hard disk or capturing of volatile data from live systems

# 6 Standards

## 6.1 Standards in digital investigation

- Use of standards as a means to demonstrate suitability of scientific methods

## 6.2 HK Government Laboratory: ISO/IEC 17043:2010

Hong Kong Accreditation Service
香港認可處

**Certificate of Accreditation**
**認可證書**

*This is to certify that*
*特此證明*

**GOVERNMENT LABORATORY**
政府化驗所

**7/F., Homantin Government Offices, 88 Chung Hau Street, Kowloon, Hong Kong**
香港九龍何文田忠孝街八十八號何文田政府合署七樓

*has been accepted by the HKAS Executive, on the recommendation of the Accreditation Advisory Board, as a*
*為香港認可處執行機關根據認可諮詢委員會建議而接受的*

**HOKLAS Accredited Proficiency Testing Provider**
「香港實驗所認可計劃」認可能力驗證提供者

*This Proficiency Testing Provider meets the requirements of ISO/IEC 17043:2010 "Conformity assessment - General requirements for proficiency testing" and it has been accredited for providing proficiency testing schemes as listed in the HOKLAS Directory of Accredited Proficiency Testing Providers*
*此能力驗證提供者符合ISO/IEC 17043:2010《合格評定 – 能力驗證的通用規定》所訂的要求，獲認可提供載於香港實驗所認可計劃《認可能力驗證提供者名冊》內的指定能力驗證項目*

*The common seal of the Hong Kong Accreditation Service is affixed hereto by the authority of the HKAS Executive*
*香港認可處根據認可處執行機關的權限在此蓋上通用印章*

CHAN Sing Sing, Terence, Executive Administrator
執行幹事 陳成城
Issue Date : 23 December 2010
簽發日期：二零一零年十二月二十三日

Registration Number :
註冊號碼： PTP 001

Date of First Registration : 9 October 2009
首次註冊日期：二零零九年十月九日

*This certificate is issued subject to the terms and conditions laid down by HKAS*
*本證書按照香港認可處訂立的條款及條件發出*

L 000776

## 6.3 HK Government Laboratory: ISO/IEC 17025:2005

Hong Kong Accreditation Service
香港認可處

**Certificate of Accreditation**
認可證書

*This is to certify that*
*特此證明*

**GOVERNMENT LABORATORY** - Forensic Science Division
政府化驗所 - 法證事務部

**9/F and 10/F., Lai Chi Kok Government Offices, 19 Lai Wan Road, Lai Chi Kok, Kowloon, Hong Kong**
香港九龍荔枝角荔灣道十九號荔枝角政府合署九及十樓

*has been accepted by the HKAS Executive, on the recommendation of the Accreditation Advisory Board, as a*
*為香港認可處執行機關根據認可諮詢委員會建議而接受的*

**HOKLAS Accredited Laboratory**
「香港實驗所認可計劃」認可實驗所

*This laboratory meets the requirements of ISO / IEC 17025 : 2005 – General requirements for the competence of testing and calibration laboratories and it has been accredited for performing specific tests or calibrations as listed in the HOKLAS Directory of Accredited Laboratories within the test category of*
*此實驗所符合ISO / IEC 17025 : 2005 -《測試及校正實驗所能力的通用規定》所訂的要求，*
*獲認可進行載於香港實驗所認可計劃《認可實驗所名冊》內下述測試類別中的指定測試或校正工作*

**Forensic Testing**
科學鑑證

*This laboratory is accredited in accordance with the recognised International Standard ISO / IEC 17025 : 2005. This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality management system (see joint IAF-ILAC-ISO Communiqué).*
*本實驗所乃根據公認的國際標準 ISO / IEC 17025 : 2005 獲得認可。*
*這項認可資格表示在指定範疇所需的技術能力及實驗所質素管理體系的運作*
*(見國際認可論壇、國際實驗所認可合作組織及國際標準化組織的聯合公報)。*

*The common seal of the Hong Kong Accreditation Service is affixed hereto by the authority of the HKAS Executive*
*香港認可處根據認可處執行機關的權限在此蓋上通用印章*

CHAN Sing Sing, Terence, Executive Administrator
執行幹事 陳成城
Issue Date : 10 March 2011
簽發日期：二零一一年三月十日

Registration Number : HOKLAS 203
註冊號碼：

Date of First Registration : 10 March 2011
首次註冊日期：二零一一年三月十日

*This certificate is issued subject to the terms and conditions laid down by HKAS*
*本證書按照香港認可處訂立的條款及條件發出*

L 000831

## 6.4 China national standards 國家標準

- Can read most standards at this portal
- GB/T 29360-2012 電子物證數據恢復檢驗規程 Technical specification for data recovery of electronic forensic
- GB/T 29361-2012 電子物證文件一致性檢驗規程 Technical specification for file identification of electronic forensic
- GB/T 29362-2012 電子物證數據搜索檢驗規程 Technical specification for data search of electronic forensic
- GB/T 31500-2015 信息安全技術存儲介質數據恢復服務要求 Information security technology — Requirement of data recovery service for storage media

## 6.5 China public safety industrial standards 公共安全行業標準

- GA/T 754-2008 電子數據存儲介質複製工具要求及檢測方法
- GA/T 755-2008 電子數據存儲介質寫保護設備檢測方法
- GA/T 756-2008 數字化設備證據數據發現提取固定方法
- GA/T 757-2008 程序功能檢驗方法
- GA/T 825-2009 電子物證數據搜索檢驗技術規範（已作廢）
- GA/T 826-2009 電子物證數據恢復檢驗技術規範（已作廢）
- GA/T 827-2009 電子物證文件一致性檢驗技術規範（已作廢）

- GA/T 828-2009 電子物證軟件功能檢驗技術規範
- GA/T 829-2009 電子物證軟件一致性檢驗技術規範
- GA/T 976-2012 電子數據法庭科學鑑定通用方法
- GA/T 977-2012 取證與鑑定文書電子簽名
- GA/T 978-2012 網絡遊戲私服檢驗技術方法
- GA/T 1069-2013 法庭科學電子物證手機檢驗技術規範
- GA/T 1070-2013 法庭科學計算機開關機時間檢驗技術規範
- GA/T 1071-2013 法庭科學電子物證 Windows 操作系統日誌檢驗技術規範
- GA/T 1170-2014 移動終端取證檢驗方法
- GA/T 1171-2014 芯片相似性比對檢驗方法
- GA/T 1172-2014 電子郵件檢驗技術方法
- GA/T 1173-2014 即時通訊記錄檢驗技術方法
- GA/T 1174-2014 電子證據數據現場獲取通用方法
- GA/T 1175-2014 軟件相似性檢驗技術方法
- GA/T 1176-2014 網頁瀏覽器歷史數據檢驗技術方法
- GA/T 1772-2014 電子郵件檢驗技術方法
- GA/T 1773-2014 即時通訊記錄檢驗技術方法
- GA/T 1774-2014 電子證據數據現場獲取通用方法
- GA/T 1474-2018 法庭科學計算機系統用戶操作行為檢驗技術規範
- GA/T 1475-2018 法庭科學電子物證監控錄像機檢驗技術規範
- GA/T 1476-2018 法庭科學遠程主機數據獲取技術規範
- GA/T 1477-2018 法庭科學計算機系統接入外部設備使用痕跡檢驗技術規範
- GA/T 1478-2018 法庭科學網站數據獲取技術規範
- GA/T 1479-2018 法庭科學電子物證偽基站電子數據檢驗技術規範
- GA/T 1480-2018 法庭科學計算機操作系統仿真檢驗技術規範

## 6.6 司法部頒司法鑑定技術規範

- can download here
- SF/Z JD0400001-2014 電子數據司法鑑定通用實施規範
- SF/Z JD0401001-2014 電子數據複製設備鑑定實施規範
- SF/Z JD0403001-2014 軟件相似性檢驗實施規範
- SF/Z JD04020001-2014 電子郵件鑑定實施規範
- SF/Z JD0400002-2015 電子數據證據現場獲取通用規範
- SF/Z JD0402003-2015 即時通訊記錄檢驗操作規範
- SF/Z JD0403003-2015 計算機系統用戶操作行為檢驗規範
- SF/Z JD0403002-2015 破壞性程序檢驗操作規範
- SF/Z JD0401002-2015 手機電子數據提取操作規範
- SF/Z JD0402002-2015 數據庫數據真實性鑑定規範
- SF/Z JD0300002-2018 數字聲像資料提取與固定技術規範
- SF/Z JD0302003-2018 數字圖像修復技術規範
- SF/Z JD0303001-2018 照相設備鑑定技術規範
- SF/Z JD0304002-2018 錄像設備鑑定技術規範
- SF/Z JD0402004-2018 電子文檔真實性鑑定技術規範

- SF/Z JD0403004-2018 軟件功能鑑定技術規範
- SF/Z JD0404001-2018 偽基站檢驗操作規範

## 6.7 中國法律法規

- 《司法鑑定執業分類規定（試行）》2000 年 11 月 29 日
- 《司法鑑定機構登記管理辦法》2000 年 8 月 14 日（已廢止）
- 《司法鑑定人登記管理辦法》2000 年 8 月 14 日（已廢止）
- 《司法鑑定機構登記管理辦法》2005 年 9 月 30 日
- 《司法鑑定人登記管理辦法》2005 年 9 月 30 日
- 《司法鑑定程序通則》2007 年 10 月 1 日（2015 年 12 月 24 日修訂，2016 年 5 月 1 日起施行）
- 《司法鑑定許可證和司法鑑定人執業證管理辦法》的通知 2010 年 4 月 12 日
- 關於換發新版《司法鑑定許可證》和《司法鑑定人執業證》的通知

## 6.8 認證認可行業標準和規範

- RB/T 214-2017 檢驗檢測機構資質認定能力評價檢驗檢測機構通用要求
- RB/T 219-2017 檢驗檢測機構資質認定能力評價司法鑑定機構要求
- CNAS-CL08：2018 司法鑑定/法庭科學機構能力認可準則
- CNAS-CL08-A001：2018 司法鑑定/法庭科學機構能力認可準則在電子數據鑑定領域的應用說明

## 6.9 ISO

- ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories
- ISO/IEC 17043:2010 Conformity assessment – General requirements for proficiency testing
- ISO/IEC 27037:2016 Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO/IEC 27041:2016 Guidance on assuring suitability and adequacy of incident investigative method
- ISO/IEC 27042:2016 Guidelines for the analysis and interpretation of digital evidence (30 June 2015)
- ISO/IEC 27043:2016 Incident investigation principles and processes (31 March 2015)
- ISO/IEC 27050-1:2016 Electronic discovery - Part 1: Overview and concepts
- ISO/IEC 27050-2:2018 Electronic discovery - Part 2: Guidance for governance and management of electronic discovery
- ISO/IEC 27050-3:2017 Electronic discovery - Part 3: Code of practice for electronic discovery

## 6.10 Suitability of scientific methods within UK criminal justice system

- Angus M. Marshall. Standards, regulation and quality in digital investigations: The state we are in. Digital Investigation. Volume 8, Issue 2, November 2011, pages 141 - 144.
- Three factors to consider suitability
  - evidence derived from scientific techniques or theories
  - validity of new scientific techniques or theories, and the basis for their interpretation
  - four criteria for expert testimony
- Four criteria for expert testimony
  - Whether the theory or technique can be (and has been) tested
  - Whether the theory or technique has been subjected to peer review and publication
  - In the case of a particular technique, what the known or potential rate of error is or has been; and
  - Whether the evidence has gained widespread acceptance within the scientific community.

## 6.11 UK traditional forensic science adopted BS 10008:2014

- BS 10008:2014 Evidential weight and legal admissibility of electronic information.

## 6.12 UK traditional forensic science adopted ISO/IEC 17025:2017

- ISO/IEC 17025:2017 (General requirements for the competence of testing and calibration laboratories) requires evidence of:
  - Competence of staff
  - Validation of processes
  - Proficiency of the provider

## 6.13 Competence of staff

- Show that staff are not only properly qualified at the point of recruitment, but that their skills and knowledge are maintained and updated appropriately.

## 6.14 Validation of processes

- All processes should be subjected to proper validation to show that they are fit for purpose. This validation should be based on requirements agreed with the customer.

## 6.15 Proficiency of the provider

- Demonstrate that, given identical samples, their results should match those of other providers offering the same service regardless of the process used.

## 6.16 Standards in the context of presentation of evidence in court

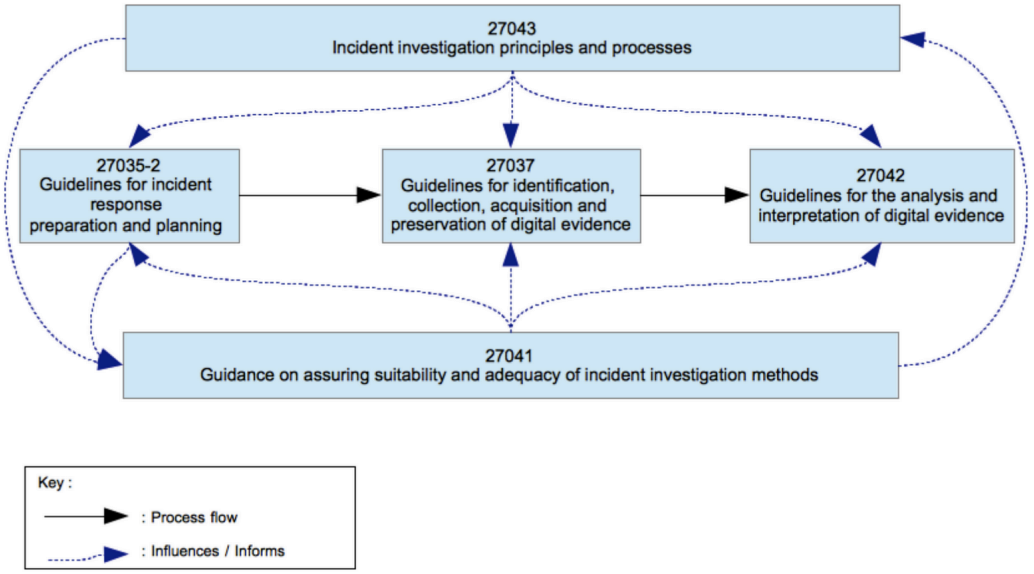
- ISO/IEC 27xxx standards:

### Legal evidence

1. 27037:2012 covers **digital evidence.**
2. 27038 will be a specification for **digital redaction.**
3. 27041 guideline on **assurance for digital evidence investigation methods.**
4. 27042 guideline on **analysis and interpretation of digital evidence.**
5. 27043 guideline on **digital evidence investigation principles and processes.**

## 6.17 Relationships of ISO/IEC 27xxx standards

- Angus M. Marshall. Standards, regulation & quality in digital investigations: The state we are in. Digital Investigation 8 (2011) pp. 141 - 144.




## 6.18 ISO 27037:2016

- ISO/IEC 27037:2016 Guidelines for identification, collection, acquisition, and preservation of digital evidence

- Scope and purpose

"The standard provides detailed guidance on the identification, collection and/or acquisition, marking, storage, transport and preservation of electronic evidence, particularly to maintain its integrity. It defines and describes the processes through which evidence is recognised and identified, documentation of the crime scene, collection and preservation of the evidence, and the packaging and transportation of evidence."

## 6.19 Parts of the chapters of ISO 27037:2016

- Key components of identification, collection, acquisition and preservation of digital evidence
- Instances of identification, collection, acquisition and preservation
- Annex A: Digital Evidence First Responder core skills and competency description
- Annex B: Minimum documentation requirements for evidence transfer

## 6.20 ISO 27041:2016

- ISO/IEC 27041:2016 Guidance on assuring suitability and adequacy of incident investigative methods
- Scope and purpose

". . . on assurance for the forensics processes relating to investigation of digital evidence. Credibility, trustworthiness and integrity are fundamental requirements …: this standard promotes the assurance aspects of investigating digital evidence. The standard will offer guidance on assuring the suitability and adequacy of the methods for investigating digital forensic evidence. It will describe methods through which all stages of the investigation process can be shown to be proper and suitable in themselves, and correctly performed. It will specify 'investigative requirements', essentially laying out the ground rules for digital forensics."

## 6.21 ISO/IEC 27042:2016

- ISO/IEC 27042:2016 Guidelines for the analysis and interpretation of digital evidence
- Scope and purpose

"The standard will provide guidelines for the analysis and interpretation of digital evidence …lay down certain fundamental principles which are intended to ensure that tools, techniques and methods can be selected appropriately and shown to be fit for purpose should the need arise. …inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organisations needing to protect, analyse and present potential digital evidence.

It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence."

## 6.22 ISO/IEC 27043:2016

- ISO/IEC 27043:2015 Incident investigation principles and processes
- Scope and purpose

"The standard concerns the principles behind, and the forensic processes involved in, investigating incidents. …provides guidelines that encapsulate idealised models for common incident investigation processes across various incident investigation scenarios involving digital evidence. This includes processes from pre-incident preparation up to and including returning evidence for storage or dissemination as well as any general advice and caveats on such processes. …describe processes and principles applicable to various kinds of investigations …a general overview of all incident investigation principles and processes . . ."

- Investigative process includes:
  - Incident management, including preparation and planning for investigations;
  - Handling of digital evidence;
  - Use of, and issues caused by, redaction (Some documents can contain information that must not be disclosed to some communities. Modified documents can be released to these communities after an appropriate processing of the original document. The process of removing information that is not to be disclosed is called "redaction".);
  - Intrusion prevention and detection systems, including information which can be obtained from these systems;
  - Security of storage, including sanitisation of storage;
  - Ensuring that investigative methods are fit for purpose;
  - Carrying out analysis and interpretation of digital evidence;
  - Understanding principles and processes of digital evidence investigations;
  - Security incident event management, including derivation of evidence from systems involved in security incident event management;
  - Relationship between electronic discovery and other investigative methods, as well as the use of electronic discovery techniques in other investigations;
  - Governance of investigations, including forensic investigations.
- Digital investigation is:

"Use of scientifically derived and proven methods towards the identification, collection, transportation, storage, analysis, interpretation, presentation, distribution, return, and/or destruction of digital evidence derived from digital sources, while obtaining proper authorisations for all activities, properly documenting all activities, interacting with the physical investigation, preserving digital evidence, and maintaining the chain of custody, for the purpose of facilitating or

furthering the reconstruction of events found to be incidents requiring a digital investigation, whether of criminal nature or no"

- Interpretation is:

  "Synthesis of an explanation, within agreed limits, for the factual information about evidence resulting from the set of examinations and analysis making up the investigation"

## 6.23 ISO/IEC 27050:2016 Electronic discovery

- Part 1: Overview and concepts
- Part 2: Guidance for governance and management of electronic discovery
- Part 3: Code of Practice for electronic discovery
- Part 4: ICT readiness for electronic discovery

## 6.24 ISO/IEC 17025:2017

- General requirements for the competence of testing and calibration laboratories (Publication date: November 2017)
  - specifies the general requirements for the competence, impartiality and consistent operation of laboratories.
  - applicable to all organizations performing laboratory activities, regardless of the number of personnel
  - The scope has been revised to cover all laboratory activities, including testing, calibration and the sampling associated with subsequent calibration and testing
  - The process approach now matches that of newer standards such as ISO 9001 (quality management), ISO 15189 (quality of medical laboratories) and the ISO/IEC 17000 series (standards for conformity assessment activities), putting the emphasis on the results of a process instead of the detailed description of its tasks and steps.
  - The standard has a stronger focus on information technologies.
  - It incorporates the use of computer systems, electronic records and the production of electronic results and reports.
  - A new section has been added introducing the concept of risk-based thinking and describes the commonalities with the new version of ISO 9001:2015, Quality management systems – Requirements.
- Comments about ISO 17025:2017
  - UK ISO 17025 Digital Forensics Survey
- Hong Kong SAR Innovation and Technologly Commission
  - Hong Kong Accreditation Service (HKAS) is part of ITC. The main role of HKAS is to promote conformity assessment services to underpin technological development and international trade.
  - Schedule for Implementation of ISO/IEC 17025:2017 in Accreditation of Testing

and Calibration Laboratories
    * The tentative deadline for laboratories to conform to ISO/IEC 17025:2017 is 30 November 2020
    * All HKAS accreditations to ISO/IEC 17025:2005 will become invalid after November 2020.

## 6.25 Other standards

- In addition to ISO, Chapter 9 by Watson and Jones mentioned other standards:
  - UK Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence
  - G8 (Group of 8) proposed principles for dealing with digital evidence
  - International Association of Computer Investigative Specialists (IACIS) requirements
  - International Organisation on Computer Evidence (IOCE) Standards
  - U.S. National Institute of Standards and Technology (NIST) criteria
  - UK College of Policing. Digital Investigation and Intelligence (April 2015)

## 6.26 ACPO Good Practice Guide for Computer-Based Electronic Evidence

- Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence

- ACPO Principle 1

  No action taken by Law Enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in Court.

- ACPO Principle 2

  In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

- ACPO Principle 3

  An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

- ACPO Principle 4

  The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

## 6.27 Group of Eight (G8)

- France, West Germany, Italy, Japan, the United Kingdom, United States, Canada, Russia
- G8 proposed principles for dealing with digital evidence:
- When dealing with digital evidence, all of the general forensic and procedural principles must be applied;
- Upon seizing digital evidence, actions taken should not change that evidence;
- When it is necessary for a person to access original digital evidence, that person should be trained for the purpose;
- G8 proposed principles for dealing with digital evidence:
- All activities relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review;
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession;
- Any agency, which is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

## 6.28 International Organisation on Computer Evidence (IOCE)

- Established in 1995 to provide international law enforcement agencies a forum for the exchange of information concerning computer crime investigation and other computer-related forensic issues
- In response to the G-8 Communique and Action plans of 1997, IOCE was tasked with the development of international standards for the exchange and recovery of electronic evidence.

## 6.29 Scientific Working Group on Digital Evidence (SWGDE)

- Established in February 1998 as the U.S.-based component of standardisation efforts conducted by IOCE
- home page
- SWGDE documents:
  - SWGDE Best Practices for Digital Audio Authentication
  - SWGDE Best Practices for Image Content Analysis
  - SWGDE Guidelines for Forensic Image Analysis
  - SWGDE Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis
  - SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs

  - SWGDE Digital and Multimedia Evidence Glossary
  - SWGDE-SWGIT Guidelines and Recommendations for Training
  - Guidelines & Recommendations for Training in Digital & Multimedia Evidence
- Guidelines & Recommendations for Training in Digital & Multimedia Evidence
- Job Categories (SWGDE)
  - Manager / Commander / Supervisor
  - Examiner / Analyst
  - Technician
  - First Responder
- Manager / Commander / Supervisor

  "[P]ersonnel who are responsible for setting agency policies and/or making budget decisions; supervise and/or direct personnel engaged in the field of digital and multimedia evidence"

- Examiner / Analyst

  "[P]ersonnel for whom examination, analysis and/or recovery of digital and multimedia evidence is a major component of their routine duties. The personnel may also be responsible for the collection of digital and multimedia evidence."

- Technician

  "[P]ersonnel whose primary responsibility is to collect and/or prepare digital and multimedia evidence for examination and analysis"

- First Responder

  "[P]ersonnel who are the first to secure, preserve and/or collect digital and multimedia evidence at the crime scene."

## 6.30 IOCE International principles

- Standardised recovery of computer-based evidence are governed by the following attributes:-
  - Consistency with all legal systems;
  - Allowance for the use of a common language;
  - Durability;
  - Ability to cross international boundaries;
  - Ability to instil confidence in the integrity of evidence;
  - Applicability to all forensic evidence; and
  - Applicability at every level, including that of individual, agency, and country.

## 6.31 IOCE Standards for Exchange of Digital Evidence

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access the original evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

## 6.32 NISTT Standards

- U.S. National Institute of Standards and Technology. Computer Forensics Tool Testing Program
- Disk imaging tools criteria:
  - The tool shall make a bit-stream duplicate or an image of the original disk or partition;
  - The tool shall not alter the original disk;
  - The tool shall be able to verify the integrity of a disk image file;
  - The tool shall provide a bit-stream image or a qualified bit steam image if I/O errors are present;
  - The tool shall log I/O errors;
  - The tool's documentation shall be correct;
  - The tool shall copy a source to a destination drive that is bigger than the source and document the parts of the disk that are not part of the copy;
  - The tool shall advise the user of a source larger than the destination.

## 6.33 Other documents

- US Department of Homeland Security. U.S. Secret Service 'Best Practices for Seizing Electronic Evidence Pocket Guide'
- Sedona Principles for Electronic Document Production, October 2017
- National Institute of Justice Electronic Crime Program
- United Nation

## 6.34 Sedona principles

- The Sedona Conference is a research and educational institute composed of leading judges, lawyers, experts and academics who are committed to developing the law.
- 14 Principles provide guidance for:
  - handling all aspects of e-discovery
    - provide important guidance on how parties to litigation should handle e-discovery

    * set forth best practices related to proportionality, specificity of requests
  - cooperation with opposing counsel
  - scope of preservation and relevance
  - form of production
  - safeguarding privilege and confidentiality, and sanctions for failure to preserve ESI.

## 6.35 National Institute of Justice Electronic Crime Program

- National Institute of Justice Electronic Crime Program, which includes the Electronic Crime Center of Excellence, supports the development of tools to assist state and local law enforcement agencies in combating electronic crime and collecting digital evidence.
- Website
- Documents available including:
  - Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors
  - Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition
  - Forensic Examination of Digital Evidence: A Guide for Law Enforcement
  - Investigations Involving the Internet and Computer Networks
  - Investigative Uses of Technology: Devices, Tools, and Techniques

## 6.36 Other references

- United Nations Office on Drugs and Crime. Staff Skill Requirements and Equipment Recommendations for Forensic Science Laboratories. United Nations, New York, 2011.
  - Specific skills requirements for digital and multimedia evidence (pages 15 - 19)
  - Minimum equipment requirements for digital and multimedia evidence (page 38)
  - Specific techniques for digital and multimedia evidence (pages 51 - 59)
- Lyle, et al. Ten years of computer forensic tool testing. Digital Evidence and Electronic Signature Law Review, Volume 8.
- Maria Angela Biasiotti. A proposed electronic evidence exchange across the European Union. Digital Evidence and Electronic Signature Law Review, 14 (2017).
- Peter Sommer. Certification, registration and assessment of digital forensic experts: The UK experience. Digital Investigation 8 (2011) pp. 98 - 105.
- Ballou and Gilliland. Emerging paper standards in computer forensics. Digital Investigation 8 (2011) pp. 96 - 97.
- Beckett and Slay. Scientific underpinnings and background to standards and accreditation in digital forensics. Digital Investigation 8 (2011) pp. 114 - 121.
- Amann and James. Designing robustness and resilience in digital investigation laboratories. Digital Investigation 12 (2015) pp. 5111 - 5120.
- Linzi Wilson-Wilde. The International Development of Forensic Science Standards — A Review. Forensic Science International (In Press, Accepted Manuscript; available online 16 April 2018).

# 7 Epilogue

## 7.1 Summary

- Mistakes and defence
- Purpose of cross-examination
- Investigative plan
- Forensic laboratory
- Standards