



ISO/IEC JTC 1/SC 27 N7934

ISO/IEC JTC 1/SC 27/WG 4 N7934

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Disposition of comments

TITLE: Disposition of National Body comments and Liaison Body comments on SC 27 N7570

SOURCE: Co-editors (Marthie Gobler and Sivanathan Subramaniam)

DATE : 2009-11-11

PROJECT: 27037

STATUS:

ACTION:

DUE DATE:

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice Chair
T. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenber, WG-Conveners
M. Grobler, S. Subramaniam, Project Co-editors

MEDIUM: Livelink-server

NO. OF PAGES:

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: SC 27 N7570

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

[AU]1A			Ed	There are numerous grammatical errors in the working draft. The Australian comment does not seek to identify these. In some cases, specific commentary has been made.	Grammatical errors throughout the working draft are identified and corrected	Noted.
[AU] 1.1A			Ge	The phrase “collection and/or acquisition” appear in the title and throughout the standard. However as defined these two processes are independent of each other. One relates to physical devices while the other deals with the data stored on a physical device. There is no need to link these processes with “and/or” they are independent of each other.	Replace “collection and/or acquisition” with “collection and acquisition” or “collection or acquisition” as appropriate throughout the text.	Accepted – The new text necessitates a title change to 'Guidelines for identification, collection, acquisition and preservation of digital evidence'. Changed to either 'and' or ',', depending on the context.
[AU] 1B			Ge	The standard seems to be written from the perspective of a person involved in technical incident response. It does little to inform about the “forensic” perspective, especially the needs/requirements of the Courts. Australia fears that, in its current context, the standard will not be an acceptable basis for the cross-border transfer of evidence which Australia believes was a primary driver for the standard. The comments provided below improve the draft, but in Australia’s opinion, it requires substantial change.	The draft requires considerable re-work with specific input from a forensic and legal perspective.	Noted.
[AU]1C			Ge	The standard creates numerous requirements that are “nice-to-have” but are not necessary for admissibility or to increase evidential weighting. It is not the role of a standard to create new requirements, rather to collate, synthesise and articulate a consensus set of existing requirements.	Identify items that are actually requirements and for the others, either remove them or qualify them.	Accepted in principle – Addressed in UK 18.
[AU]1D	1	Paragraph 1	Ge	The standard should not attempt to provide guidance on the various physical forms that digital devices could take	Replace with: “This international standard provides guidance on the	Accepted – Replace with: “This international standard provides

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				(i.e. recognition) – we could never do it justice.	management of digital evidence management. It describes the processes of identification, collection, acquisition and preservation of digital data which may be of evidentiary value.	guidance on digital evidence management. It describes the processes of identification, collection, acquisition and preservation of digital data which may be of evidentiary value.
[AU]2	1	Paragraph 2	Ge	The role of the standard is to provide guidance to people needing to protect digital evidence. It does not matter why they need to do this and is so much more than computer incidents.	Replace existing paragraph with: “It is applicable to organisations needing to protect, analyse and present digital evidence. It is also applicable to policy making bodies that create procedures relating to digital evidence and decision making bodies need to evaluate digital evidence, often as part of a larger body of evidence”	Accepted.
[AU] 3	1	Paragraph 2	Ge	The scope needs to clarify what is meant by “digital”.	Add: “This standard applies to data that is already in a digital format and makes no attempt to cover the conversion of analog data into a digital format.”	Accepted. This sentence is added to Section 1, Scope.
[AU]3.1	1	Paragraph 3	Ge	This paragraph can be consolidated and clarified and should not be limit the standard to any specific sources of digital evidence.	Replace paragraph with: “This standard applies to data sourced from any type of media.”	Accepted.
[AU]4	1.1	Paragraph 1	Ge	The term digital evidence first responder is misleading. The person who is responsible for dealing with the digital evidence may not be the first person on the scene. A better term would be “digital evidence specialist” Not only is this document intended for the people on the ground it is also of just to those setting policies and standard operating procedures. Judiciary, lawyers and managers are also an important audience.	Replace digital evidence first responder with digital evidence specialist. Reword paragraph: “This standard is intended to provide guidance to those responsible for the identification, collection, acquisition and preservation of digital evidence. This includes incident response specialists, digital evidence specialists and forensic laboratory managers.”	Accepted with modification - Content of ZA 25, ZA 27 and AU 5.1 are combined and incorporated in existing clause 1. These comments and suggested rewording will be addressed in the new text.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					Add: "This standard is also intended to inform decision-makers who need make a determination regarding the reliability of any digital evidence presented to them"	
[AU]5	1.1	Para 1, last sentence	Ge	This is a defining sentence: "This standard deals with common situations encountered throughout the whole process" and sets the (wrong) scene. The editors need to consider whether they are trying to describe "common" situations or trying to provide guidance to be used more generally – we suggest that the latter could be the objective of an ISO standard. Our understanding is that a standard is trying to achieve technical neutrality. If it is the intent, then the standard needs to specify what the "common situations" are.	Move the sentence into 1.2 and consider if it actually is the objective.	Accepted with modification - Content of ZA 25, ZA 27 and AU 5.1 are combined and incorporated in existing clause 1. These comments and suggested rewording will be addressed in the new text.
[AU]5.1	1.2	Para	Ge	The objective and background of the first draft indicated that the primary objective was to allow inter-jurisdictional transfer of evidence. This objective is now relegated to the third position after guiding the process and assisting in disciplinary action!	Replace paragraph with: The objective of this standard is to outline the minimum requirements necessary for enabling transfer of digital evidence between jurisdictions. It will provide a framework for the development of processes and procedures for the identification, collection, acquisition and preservation of digital evidence.	Accepted with modification - Content of ZA 25, ZA 27 and AU 5.1 are combined and incorporated in existing clause 1. These comments and suggested rewording will be addressed in the new text.
[AU] 5.2	3.1	All	Te	Acquisition can occur anywhere, not just at the 'incident scene'. The words 'leaving the original evidence is performed' is superfluous and limiting There forensic imaging is a field of forensic science only vaguely related to digital forensics. It has nothing to do	Reword to: A process of creating a copy of all data within a defined set. The product of an acquisition is a digital evidence copy.	Accepted with modification – Remove last part of the definition (see US 7). Include note in text regarding exceptions when it is not possible to leave evidence in tact. Remove restriction of incident scene, acquisition

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				with creating a copy of data. The term imaging should not be used for this purpose as it is confusion to anyone from outside the profession, ESPECIALLY the courts.		may be done remotely.
[AU] 5.3	3.2	All	Ed	The words 'and taking the items away from the incident scene for further investigation' are superfluous and limiting the definition	Remove: and taking the items away from the incident scene for further investigation	Accepted.
[AU]6	3.3		Te	A "blob" refers to any Binary Large Object and does not have to be a multi-media file. It is an abbreviation already included in 4.	Remove.	Accepted.
[AU]7	3.4		Te	It is an incorrect definition. Also, it is an abbreviation already included in 4.	Remove	Accepted.
[AU]8	3.6		Te	An "evidence copy" does not need to be created in a forensically sound manner, merely a (legally) reliable manner.	Replace with: "a copy of the digital evidence that has been produced in a legally reliable manner and includes both the digital evidence and a means of verifying it".	Accept with modification – Change to 'an evidentially reliable manner'. 3.6 is renumbered to 2.5.
[AU]8.1	3.7		Te	The term digital evidence first responder implies the 'first' person on the scene is the only one responsible for the identification collection etc of the evidence. This is not consistent with the definition provided.	Replace Digital Evidence First Responder with: Digital Evidence Specialist	Rejected – Both DEFR and Digital Evidence Specialist will be used in the standard. SE and AU to provide definition for Digital Evidence Specialist. Digital Evidence Specialist will be written out in full to avoid confusion with encryption DES. 3.7 is renumbered to 2.6.
[AU]8.2	3.8		Te	The terms "Hash Code" and "Hash Value" have the same definition. Why use different terms to say the same thing? This has the potential to create confusion.	Remove	Accepted – Remove the definition for hash code.
[AU]8.3	3.9		Te	What two properties?		Noted – Addressed in US 12.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

[AU]9	3.11		Te	This is a bad definition open to interpretation.	Preference is to use the term “create forensic copy” rather than imaging. Alternatively, replace with: “another term for <u>copying</u> , commonly adopted by computer forensic practitioners.”	Accepted in principle.
[AU]10	3.12		Te	This is a bad definition open to interpretation (for example DaVinci’s mirror). Also, in many jurisdictions, the term “image” has a specific interpretation that relates to pictorial content, specifically the science of “Forensic Imaging” which relates to the manipulation and creation of pictures.	Replace with: “another term for <u>copy</u> , commonly adopted by computer forensic practitioners.”	Accepted in principle.
[AU] 10.1	3.15		Te	A system clock may also be found in a PDA or mobile phone, or any other digital device. This term is self explanatory and does not need definition	Remove	Accepted.
[AU] 10.2	3.17		Te	Spoilage may occur as the result of an intentional or unintentional act.	Change to: Intentional or unintentional changes to digital evidence that may diminish its evidential value.	Rejected – Replace the word 'accidental' with 'unintentional'. Add the word 'unavoidable'.
[AU]11	3.17		Ed		Remove: “or allowing”	Duplicate – Addressed in AU 10.2.
[AU]12	3.18		Ed		Remove: “or allowing”	Duplicate – Addressed in AU 10.2.
[AU]13	4		Ed		Add: “PED Personal Electronic Device”	Accepted.
[AU]14	4		Ed		Add: “DES Digital Evidence Specialist” (instead of “DEFR Digital Electronic First Responder”)	Rejected – Digital Evidence Specialist will be written out in full to avoid confusion with encryption DES according to AU 8.1.
[AU]15	3	??	Ed	It would be useful to have a consistent term for referring to digital devices.	Add: “Digital Device any electronic equipment used to process or store digital data”	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

[AU] 15.1	5	Entire section	Te	<p>The challenges presented by the forensic examination of digital devices are no greater than the challenges presented by any other forensic examination. For example it can be strongly argued that electronic evidence is far less fragile than biological evidence. Electronic evidence will not be contaminated by simply having a person walk into in a crime scene. Also in the majority of cases the accuracy and reliability of digital evidence can be verified absolutely, it is either accurate or it is not. Biological evidence on the other hand is measured in terms of probabilities.</p> <p>The introduction should be presenting the principles which will be applied throughout the process. They are consistent with principles published by a number of authors and organisations. These relate to the principles proposed for section 6. I suggest that section 6 is re-titled to core requirements.</p> <p>There is crossover between the principles and requirements. However they serve two separate purposes. The principles describe how the DES should approach the process. The requirements set out what they should do. A new section 5.1 should be created expanding upon the core principles.</p>	<p>Reword entire section: “Digital evidence is by its very nature fragile. It can be altered, damaged or destroyed through improper handling or examination. Handlers of digital evidence must be appropriately trained to identify the risks and consequences of potential courses of action when dealing with digital evidence. Failure to handle digital devices in an appropriate manner may render the potential evidence contained on them unusable.</p> <p>The fundamental principles of handling potential sources of digital evidence are:</p> <ol style="list-style-type: none"> 1. Minimise handling of the original 2. Account for any change 3. Comply with the local rules of evidence 4. The digital evidence specialist must not exceed their knowledge. 	<p>Accepted in principle – Editor will include text on the Locard principle to extend explanation of volatile nature of digital data.</p> <p>New structure according to JP 18 may require the incorporation of some parts of this section into Section 5.</p>
[AU]16	5.1	Para 1	Ed	Badly written.	<p>Replace 1st sentence with: “Digital evidence is presented in physical and logical form. Physical refers to the construction and resultant appearance of the digital device and logical refers to the format used to arrange and store the data within the digital device”.</p> <p>Rewrite 2nd sentence.</p>	<p>Accepted. Section 5.1 is renumbered to 4.3.1.</p>
[AU]17	5.2		Te	This section ignores “collection” even though it is in the	Add: “ <u>Collection</u> is the removal of the	Accepted with modification - Addressed

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				title.	digital device for later analysis".	in ZA 48. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition..
[AU]18	5.3	2 nd sentence	Ed	Badly written.	Replace with: "There should be no modification to the data itself or any metadata associated with it (e.g. date and time stamps)".	Accepted. Section 5.3 is renumbered to 4.3.4.
[AU]19	5.4		Te	In most common law jurisdictions, only "expert evidence" needs to be scientifically proven. Digital evidence may be admitted as another class of evidence (e.g. business record) with differing requirements.	Remove: "scientifically proven" and replace with "evidentially reliable" or "legally defensible".	Not applicable since section is deleted – JP 15.
[AU]20	5.5		Te	Interpretation is part of Analysis.	Replace with: "This is the process of persuading decision-makers that (i) the digital evidence is reliable and (ii) its meaning in the context of the matter at hand. Presentation can take many forms, including checklists, written reports, multimedia presentations and witness box orations"	Not applicable since section is deleted – JP 15.
[AU]21	3		Ed	Include a definition for "legally defensible"	Add: "Legally defensible - conducted in according to the laws in the relevant jurisdiction and will withstand legal scrutiny, usually by an adversary"	Rejected – Suggest inclusion of definition for evidentially reliable. See AU19.
[AU]22	6.1		Te	There is no legal requirement for "methodical". Rather the measure is "reliable" and while "methodical" should lead to "reliable" it does not follow that other methods (e.g. intuitive) are not "reliable". The concepts presented here relate to a principle not a requirement are inconstant with the other headings within this section.	Rename to "Least intrusive" Remove this section. (move content to new 5.1.1).	Accepted - Move this section to a new paragraph in clause 5.1 in the new structure proposed by JP 18. Methodical is only one approach, common law countries experts have a role in evidence management process where expertise is more important than methodology.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

						Section 6.1 is renumbered to 5.2.1.
[AU]23	6		Te	See comments regarding this section in 5. The topics of auditable, repeatable and defensible are not principles, they are requirements. In order for the evidence to be accepted in court these points must be addressed. The heading of methodical is a principle; the content of this heading is addressed by the new section 5.1.1.	Change heading of this section to: “Requirements for the identification, collection, acquisition and preservation of digital evidence. Delete the existing paragraph and add Add: “In most jurisdictions, there are three fundamental requirements for evidence, including digital evidence. Evidence must be (i) relevant (ii) reliable and (iii) sufficient. Relevance depends on the matter under consideration and in the context of this standard, reliability and sufficiency can be explained using a number of overarching principles. The scope of this guide is limited to addressing point (ii) the reliability of the evidence. This topic can be addressed by ensuring that all actions taken are auditable, repeatable and defensible.”	Accepted in principle. Section 6 is renumbered and split into 4.1 and 4.2.
[AU]24	6.1	3 rd para	Te	In clause (b), the issue is “verification” as opposed to accuracy. An accurate process is of little use if it cannot be verified.	Replace the 2 nd sentence with: “The DES should first consider using methods that are readily verified, such as....”	Accepted with modification - Digital Evidence Specialist will be written out in full to avoid confusion with encryption DES according to AU 8.1. Section 6.1 is renumbered to 5.2.1.
[AU] 24.1	6.2	1 st para	Te	What are the highest possible standards? The standard adopted should meet the requirements of the investigation at hand. The clause at the end of this section should not be necessary. The steps taken should follow the core principles with respect to the evidence to be collected.	Remove existing section and replace with: It should be possible for an independent assessor to evaluate the steps taken by the DES. This will be made possible by appropriately documenting all actions	Accepted in principle - Digital Evidence Specialist will be written out in full to avoid confusion with encryption DES according to AU 8.1. Section 6.2 is renumbered to 4.1.1.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				For example: If the device being examined is a 100TB RAID it is not going to be feasible to create a forensic copy of the entire RAID. More likely the target of the process will be a few files contained on the RAID. These may be located using a laptop connected to the RAID, without any write-blocking method in place. This will cause changes to the file system, but not to the files that are the target of the search. The relevant files can then be acquired. The files themselves are the evidence, not the file-system metadata relating to them which may have been altered.	taken. The DES should also be able to justify the decision making process in selecting a given course of action.	
[AU]25	6.3	2 nd para	Te	“Similar” is not the “same” and is not good enough in this context.	Replace “similar” with “same”	Accepted. Section 6.3 is renumbered to 4.1.2.
[AU]26	6.3	3 rd para, clause (b),(c) and (d)	Te	The whole idea is that a different (perhaps but not necessarily independent) party perform the repeat test, using instruments that may or not be the same but are always suitable to the task.	Remove (b) Replace (c) with: “Using instruments and conditions that are comparable to the original test” Remove (d)	Accepted – Addressed in ZA 60. Accepted. Accepted. Section 6.3 is renumbered to 4.1.2.
[AU]27	6.3	3 rd para clause (e)	Te	The repeat test may need to be conducted months or years after the original test, especially where statute of limitations and for appeal is lengthy. Note however, there are instances where a repeat test is not possible e.g. when a drive has been copied and the original returned into use.	Replace (e) with: “Can be repeated at any time after the original test” Add a new clause: “The DEFR should be aware that there will be circumstances where it would not be possible to repeat the test e.g. when a drive has been copied and the original returned into use. In this case, the DEFR must be able to properly justify the reliability of the copying process.”	Accepted with modification – Include new content on different storage media’s data retention capabilities (e.g. limitation similar to those applied for auditing purposes and biological evidence). Section 6.3 is renumbered to 4.1.2.
[AU]28	6.4	1 st para	Te	The term “defend” has a specific context	Replace “defend” with “justify” Replace “Defense” with “justification”	Accept with modification - New structure according to JP 18.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					Change body of this section to: “The DEFR must be able to justify their actions in terms of the core principles outline in section 5.1.1.”	Section 6.4 is renumbered to 4.1.4. The principles are changed to requirements.
[AU]29	6		Te	The requirement of SUFFICIENT has not been addressed. Australia notes that the requirement is not COMPLETE which is quite (legally) different to SUFFICIENT.	Include a sub-section titled “Sufficiency”	Accepted in principle – AU to provide content.
[AU]30	7	1 st para, 2 nd sentence	Te	It does not always follow that “evidentiary weightage” is diminished.	Replace “will be” with “could be”	Accepted. Section 7 is renumbered to 5.1.
[AU]31	7	1 st para, 2 nd sentence	Ed	The correct term is “evidential weight” or “evidential weighting”. Australia accepts that this is country specific	Replace “evidentiary weightage” with “evidential weighting”	Accepted. Section 7 is renumbered to 5.1.
[AU]32	7	2 nd para	Te	Chain of Custody is only relevant up to the point where there is an evidentially reliable mechanism to determine if the evidence has been spoiled (i.e. up to the creation of the evidence copy). An advantage of making an evidence copy, as opposed to collecting the media, is that chain of custody is no longer required (but might be nice to have). In jurisdictions where cost is a consideration (see Civil Procedure Act §56) this is an important distinction.	Consider an alternate wording.	Accepted with modification – Chain of custody is to be maintained throughout the entire acquisition and collection process. Chain of custody is necessary to maintain evidentially reliable criteria, but the requirements may differ between jurisdictions. Section 7 is renumbered to 5.1.
[AU]33	8.1	1 st para	Te	The DEFR will most certainly have to provide some form of report, albeit a checklist.	Remove: “and development of the report”.	Rejected – DEFR should not be involved with the report of the analysis, but need to provide a report on acquisition and collection. Content will be enhanced accordingly.
[AU]34	8.1		Ge	At this point, it may be appropriate to introduce a concept of the “product” of the DEFR. This would include the collected digital device or an evidence copy and some	Include a paragraph that covers this point.	Accepted in principle – AU to provide content. Section 8.1 is renumbered to 5.3.1.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				sort of report. The “product” concept would then become useful for subsequent text.		
[AU]35	8.1	2 nd para, 1 st dot point	Te	The DEFR only needs knowledge of the digital devices that he/she is collecting or acquiring.	Replace with: “They should be properly and adequately trained to handle the digital devices which from which they intend to create their product”	Accepted – Incorporate with FIRST 30. Section 8.1 is renumbered to 5.3.1.
[AU]36	8.1	2 nd para, 2 nd dot point and Note	Te	The standard should not create requirements that diverge from law. Competency testing is only one way of establishing expertise. Australian law does not recognise competency testing (if competency testing is the only demonstration of skill) and recognises other ways of demonstrating skills including academic qualification, training and experience as alternatives. Australia feels that this clause would unfairly discriminate against a DEFR who chooses not to undertake what is Australia is an expensive vendor-provided competency test and is not in law enforcement. Alternative demonstrations of skill need to be recognised.	Rewrite the dot point recognising other appropriate means of demonstrating skill.	Accepted in principle – AU to provide content. Incorporate with FIRST 30 and UK 9. Section 8.1 is renumbered to 5.3.1.
[AU]37	8.3		Ge	The stated requirements are not usually a consideration for the DEFR. In Australia, the DEFR would not enter a crime scene until it was declared safe – almost always by someone else (e.g. Police). The Risk Assessment should focus on identifying the considerations impacting: <ul style="list-style-type: none"> • The information the investigator wants; • The choice of collection/acquisition methods; • The equipment that may be needed on-site; • What happens if data/equipment is damaged; • etc 	Consider the objective of the Risk Assessment and craft an appropriate paragraph.	Accepted – AU to provide content. The new text need to consider the corporate environment. Section 8.3 is renumbered to 5.2.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				The risk assessment is not a requirement of the DEFR, it is part of the initial assessment.		
[AU]38	9		Te	The DEFR needs to be aware of the risk of inherent bias. The briefing needs to be crafted so the DEFR can properly challenge any such allegation.	Write an appropriate paragraph.	Accepted in principle – AU to provide content. The DEFR should be completely objective. This section needs to include generic guidelines on briefing. Section 9 is renumbered to 5.4.
[AU] 38.1	10.3	2nd para	Te	The final sentence is redundant. This has already been addressed in 5 & 6.	Delete final sentence	Rejected – Unclear which sentence are referred to.
[AU] 38.2	10.3	2 nd para	Te	Time settings should be compared with a reliable time source, it does not hav to the the atomic clock.	Change ‘atomic clock’ to ‘reliable time source’	Accept with modification – Reliable time source, such as atomic clock or system clock. Section 10.3 is renumbered to 5.3.3.3.
[AU]39	10.2	3 rd para	Te	This paragraph reads as though “Collection” is the preferred approach and “Acquisition” should only be used if a digital device cannot be collected.	Replace with: “There are some circumstances when digital devices should not be collected. The DEFR should consider the following:”	Accepted. Section 10.2 is renumbered to 5.3.3.2.
[AU]40	10.2	(a)-(d)	Te	The most important condition is missing.	Insert as (a): “There is no legal entitlement to collect the digital device or there is an obligation to use other methods (e.g. to avoid interrupting a business)”	Accepted. Section 10.2 is renumbered to 5.3.3.2.
[AU]41	11	(a)-(l)	Ed	The examples are already provided as Annexure B	Remove (a)-(l) and insert: “Examples of devices that may contain digital evidence are provided in Annexure B”.	Accepted – Combine with SE 17. Section 11 is renumbered to 5.8.
[AU]42	11	3 rd para	Ed	Due care must be applied, not “implied”.	Replace: “due care to protect the data is not implied” with “due care to protect the data is not applied”	Accepted. Section 11 is renumbered to 5.8.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

[AU]43	11		Te	<p>The section uses “volatility” as the only measure for prioritising collection/acquisition. The concept of <u>evidential significance</u> (also called evidential value or litigical significance) is as important, perhaps more so. Evidential significance uses measures including relevance and weighting to measure the importance of documents to a case (remembering that digital evidence is, in law, a form of document).</p> <p>The problem here is that it implies the DEFR has knowledge of the case. This needs to be balanced against a criticism of running out of time to properly collect/acquire a evidentially significant document merely because it was not volatile and thus prioritised lowly (according to the draft text).</p> <p>Part of the prioritisation process is conducting a risk assessment. Rather than prioritising by volatility prioritise by evidence at most risk of being lost, spoiled or tampered with.</p>	<p>Re-work the section.</p> <p>Select a method for the assessment of evidential significance and provide guidance for its application and use.</p>	<p>Accepted in principle – To combine with UK 15. If time is critical during an acquisition, preference should be given to important data, not volatile data. A warning needs to be included regarding this.</p> <p>Section 11 is renumbered to 5.8.</p>
[AU]44	11	Note 1	Te	<p>Volatile data may change due to a number of triggers not just location.</p>	<p>Replace with: “Be aware that some volatile data may change due to factors including location, time and changes to the surrounding digital devices”.</p>	<p>Accept with modification – ‘...Including but not limited to’.</p> <p>Section 11 is renumbered to 5.8.</p>
[AU]45	12.1	1 st para	Ed	<p>The definition of “computer” relates to this section and not the whole standard.</p>	<p>Replace: “In the context of this standard” with “In the context of this section....”</p>	<p>Accepted.</p> <p>Section 12.1 is renumbered to 6.1.1.</p>
[AU]46	12.1	1 st para	Te	<p>Need to clarify the whether a computer capable of being connected to a network, but not connected at the time of the search, is covered in this section.</p>	<p>Add: “A computer that has network connectivity, but is not connected at the time of collection/acquisition, should be considered (for the proposes of this standard) as a standalone computer.”</p>	<p>Accepted.</p> <p>Section 12.1 is renumbered to 6.1.1.</p>

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

[AU]47	12.1.1	(a)	Te	This is not the role of a DEFR. Further, a non-Police DEFR has no authority to do this.	Remove	Accepted. Section 12.1.1 is renumbered to 6.1.1.1.
[AU]48	12.1	All	Ed	Need to be consistent in referring to a “digital device”. “Electronic device” incorporates a broader category of machines/instruments that are not within the scope of this standard.	Change “electronic device” to “digital device” Change “computer” to “digital device” where appropriate.	Accepted. Section 12.1.1 is renumbered to 6.1.1.1.
[AU]49	12.1.1	(c)	Te	What is a proprietary system in one country may well be mainstream in another and visa-versa.	Replace “of any proprietary systems” with “any digital devices...”	Accepted. Section 12.1.1 is renumbered to 6.1.1.1.
[AU]50	12.1.1	(d) (f)	Te	Use of wrong term	Replace “particles” with “particulates”	Reject – Meaning of terms are closely related.
[AU]50.1	12.1.1	(f)	Te	This is a generic precaution it should be part of the risk assessment	Move this point to section 11	Accept with modification - New structure according to JP 18. Section 12.1.1 is renumbered to 6.1.1.1.
[AU]51	12.1.2		Te	The actions described in this section may not be admissible. If conducted by the DEFR or unless conducted in a particular manner.	Add: “The DEFR must conduct non-electronic evidence collection according to procedural laws to ensure that any evidence is admissible. This is especially important if the non-electronic evidence is used to interpret electronic evidence, for example, a pass-phrase that is required to unlock encryption”	Accepted. Section 12.2.2 is renumbered and split into 6.1.2.2 and 6.1.3.2.
[AU]52	12.2	1st para	Te	There is a clear (legal) distinction between seizure and collection. A digital device can be collected without being seized (e.g. by consent) and an acquisition may also be a seizure.	Remove “(seize)”	Accepted. Section 12.2.2 is renumbered and split into 6.1.2.2 and 6.1.3.2.
[AU]53	12.2	All	Ge	Collection and acquisition are two different functions. They should be in separate sections.	Create a new section for acquisition	Accepted. The section is rewritten to allow for this new section. Section 12.2.2 is renumbered and split

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

						into 6.1.2.2 and 6.1.3.2.
[AU]54	12.2.1		Ge	Make clear that the steps are in order	Change (a), (b), etc to Step1, Step2, etc	Rejected – Refer to SE 21. The order of the steps depends on the situation. Editor to provide flow diagrams to present sequence correlation.
[AU]55	12.2.1	(e)	Te	This assumes the digital device is to be removed.	Pre-pend with: “If the digital device is to be collected,....”	Accepted with modification. Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.
[AU]56	12.2.1	(f) and (h)	Te	These are not requirements, rather nice-to-haves.	Remove	Duplicate – Addressed in SE 18.
[AU]56.1	12.2.1	(i)	Te	The hard drive should not be removed from the computer system until it is going to be acquired. Removing it from the case increases the risk of damage or mixing it up with another exhibit.	Remove	Accepted Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.
[AU]57	12.2.1	(j)	Te	Depending on the copying method, the sanitization of the target disk is not a requirement, rather a nice-to-have. Where there is an obligation to minimise cost, sanitizing a disk would be contrary to this obligation.	Remove the 2nd sentence.	Accepted - Admissibility may be a concern in some countries – sanitization is necessary when target disk sizes differ (include as qualifier). See IOCE 5. Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.
[AU]58	12.2.2			See comments for 12.2.1	See comments for 12.2.2.1	Refer to AU 54 – 57.
[AU]59	12.2.3	1st para	Ed	Over-emphasis	Change “many” to “some”	Accepted. Section 12.2.3 is renumbered to 6.1.3.3.
[AU]60	12.2.3	1st para	Te	It does not always follow that a military system can't be turned off.	Remove “military systems”	Accepted. Section 12.2.3 is renumbered to 6.1.3.3.
[AU]61	12.2.3	(c)	Te	See comment for 12.2.2.1 (j)	See comment for 12.2.2.1 (j)	Accepted – see comment on sanitization in IOCE 5.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

						Section 12.2.3 is renumbered to 6.1.3.3.
[AU]62	12.2.4	(c)	Te	Collection and acquisition are alternatives (remembering that collection also allows for subsequent acquisition).	Replace “and” with “or”	Accepted. Section 12.2.4 is renumbered to 6.1.3.4.
[AU]63	12.3	1st para	Te	Incorrect usage of terms	Replace: “All collected and/or acquired digital data must be protected from potential loss, damage or spoilage” with “All collected and/or acquired digital data must be protected from loss or tampering or spoilage”.	Accepted in principle – use the term spoliation, US 17. Section 12.3 is incorporated into 5.7.
[AU]64	12.3	(a)	Te	“Seal” has a specific legal meaning. The application of a legal seal will not suffice in this context. The objective is to create a means of verifying the reliability of the copy.	Reword	Accepted in principle – AU to provide content. Section 12.3 is incorporated into 5.7.
[AU] 64.1	12.3	(a)	Te	Very few existing forensic copying tools hash the original after the forensic copy has been made. The tools hash the data as it is read. If this section is left as is a number of vendors are going to have to rewrite their tools, and the imaging process will take twice as long as it currently does. Also reading the device twice is in violation of the first principle of minimal handling of the exhibit. The confirmation that a copy is identical to the data read from the device is a function of the acquisition process, not the preservation process (as preservation is defined within this standard). The points raised in this section should be moved to the new section on acquisition.	Move the relevant sections of this to new section on acquisition. Leave out any reference to biometric seals. (this is part of chain of custody anyway)	Accepted with modification – Hashing generally occurs during the acquisition process and not only after. This section will be moved accordingly in the standard's new structure. Accept with modification – biometric references will be modified and presented as a desirable, see UK 18. Section 12.3 is incorporated into 5.7.
[AU]65	12.3	(a)	Te	The use of biometric provides little value, since it binds a DEFR to the evidence (which solves a different problem)	Remove “or biometric features”	Duplicate – Addressed in AU 64.1.
[AU] 65.1	12.3	(b)	Te	Shrink wrap plastic is a bad move if static electricity or preserving biological evidence is of concern.	Remove “such as shrink wrap plastic”	Duplicate – Addressed in SE 22.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

[AU]66	12.3	(d)	Te	A nice-to-have. Also, there are evidence labels that require pencil to be used (because of tamperproof features).	Remove	Superseded by SE 27. Section 12.3 is incorporated into 5.7.
[AU]67	12.3	(f)	Ge	Should provide guidance on these requirements	Author some practical guidance or refer to an appropriate standard. For example AS2834 – Computer Accommodation.	Accepted with modification - generic discussion should be included. Section 12.3 is incorporated into 5.7.
[AU]68	13	All	Ed	Same comments as for 12	Same comments as for 12	Noted and addressed as in section 12.
[AU]69	13.1.1	(e) and (f)	Ge	These are educational statements, not requirements. Given that the DEFR is required to be proficient with the digital devices he/she is collecting, these are unnecessary here.	Remove.	Duplicate – Addressed in SE 25.
[AU]70	13.1.1	(g)	Ed	Cost and time may need to be considered in all the DES's actions.	Remove "If cost and time permit"	Accepted.
[AU]71	13.1.1	(h)	Ed	This has already been said.	Remove	Accepted.
[AU]72	13.1.2		Ed	This has already been said at 12.1.1	Remove	Accepted.
[AU]73	13.2		Ed	The considerations for collecting or acquiring are the same for standalone and network devices. There should be a separate section for this.	Create a separate section "Considerations for determining collection or acquisition of data"	Superseded by JP 18.
[AU]74	13.3		Te	Networked devices may have the ability to remotely wipe data.	Include a copy of 14.3 (a)	Accepted.
[AU]74.1	13.3		Te & Ge	This is a repeat of 12.3 see previous comments.	Remove	Superseded by JP 18.
[AU]75	13.2		Te	Networked devices may be multipath and DEFR needs to recognise and all paths (e.g. a desktop with a GSM card)	Add: "A device may have more than one communications method. For example a computer may have a wired LAN, a wireless modem and a mobile phone card. The DEFR should identify all	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					communication methods and take appropriate steps to protect against their improper use".	
[AU]76	14		Ge	Mobile devices are either stand-alone and network devices. There is no need to have a separate section. If there is to be a separate section, need to be clear on how to classify devices to minimise confusion. For example, what is a netbook that does not have a hard disk? What is a desktop that has GSM phone card?	Remove. Take clauses (e.g. faraday cage) into the relevant section of networked devices.	Accepted.
[AU]77	15		Ge	A CCTV is no different (from acquisition point of view) from a standalone or networked device. The critical difference is in the analysis phase which is beyond the scope of this standard. A DEFR who changes the video file format, has not acquired the digital data properly. Rather he/she has interpreted the data and thus now need to establish themselves as an expert.	Remove. Take clauses (e.g. number and placement of cameras) into the relevant section of standalone devices.	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.
[AU] 77.1	15.1			See previous comments. (12.1)		Noted and addressed as in section 12.
[AU] 77.2	15.2			See previous comments (12.2)		Noted and addressed as in section 12.
[AU]78	15.3		Te	There are special requirements for photographs and video in most Australian jurisdictions.	Add: "Some jurisdictions may have special requirements for the admission of photographs and video evidence. Even though the format is digital, the DEFR must adhere to those requirements."	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices. This section is added to clause 6.3.3.1.
[AU] 78.1	16		Ge	There is considerable overlap between the preservation sections and packaging. Suggest removing all preservation sections from 12, 13, 14, and 15 and consolidation then under 16.		Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

[AU]79	16.1	1st para	Te	Bad choice of language. The scientific term for “Bit rot” is “magnetic degradation” or “magnetic flux degradation”.	Replace 2nd sentence with: “The phenomena of magnetic flux degradation causes hard disks, tapes and other low volatility magnetic media to lose data over time.”	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
[AU]80	16.1	(d)	Te	Incorrect information	Replace with: “Magnetic media should be stored in packaging that is magnetically inert, anti-static and free of particulates.”	Accepted – Incorporate with SE 22. Use term 'particles' as decided in AU 50. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
[AU]81	16.1	(f)	Ed	Too much information. Interesting but not necessary.	Replace with: “Protect the digital devices from the influence of magnetic sources (e.g.....)”	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
[AU]82	16.1	(l)	Te	Some tamper-proof evidence labels require pencil.	Replace with: “If using pencil to mark labels, the DEFR must take care not to allow graphite powder to fall onto magnetic media.”	Superseded – addressed in SE 35.
[AU]83	16.1	(m)	Ge	Different jurisdictions have different requirements. We need to agree on a minimal set, but “client name” and “attorney’s office” are not it. In Australia, the marking of a suspect’s name onto evidence could cause the evidence to become inadmissible. Anonymous markings, such as a job code are usually used. In the Federal Court, there is a specified format for the markings in civil matters.	Create a section on “Labelling”. Agree a minimal set of markings that are required on the label and provide guidance on how to use them. Include: “Some jurisdictions have specific requirements regarding the format of labelling evidential material. The DEFR should be familiar with, and conform to, the requirements applicable in the matter at hand.”	Accepted in principle – Combine with SE 36. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
[AU]84	Annexe A			It is Australia’s view that this Annex does not add value to the standard. If it does remain, it is inaccurate with numerous examples for any of those offences where it is	Remove Annex. Alternately correct inaccuracies.	Accepted to correct inaccuracies – Editors and UK to review Annex A.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				wrong.		
[AU]85	Annexe B			It is Australia's view that this Annex does not add value to the standard . If the committee really wants to go do this path, they have a look at the forensic computing ontology. An example is at http://www.unisanet.unisa.edu.au/staff/Homepage.asp?Name=Jill.Slay	Remove Annex. Alternately, rework using the Computer Forensic Ontology	Accepted to rework the Annex or to link to existing external site for further information.
[AU]86	Annexe C			Any information included in the standard is going to be out of date before the standard is published.	Replace with a reference to the NIST CFTT website.	Not applicable since annex is deleted – SE 45.

FIRST-1	Intro	Para 1	Ed	"the right procedure" - reads like an opinion	"...a repeatable methodology..."	Accepted with modification – Change the content to 'legally acceptable methodology'.
FIRST-2	Intro	Para1	Ed	Admissibility	Admissibility	Accepted.
FIRST-3	Intro	Paragraph 3	Ed	Occurred	Occurred	Not applicable since sentence is deleted – US 3.
FIRST-4	1		Ed	Clauses 12 13 & 14 refer to hardware, there is no mention of identification, collection and preservation of <i>data or digital evidence</i>		Noted – FIRST to provide suggested changed content.
FIRST-5	1.1		Ed	responsible in	responsible for	Accepted with modification - Content of ZA 25, ZA 27 and AU 5.1 are combined and incorporated in existing clause 1. These comments and suggested rewording will be addressed in the new text.
FIRST-6	1.2		Ed	Colleccting	Collecting	Duplicate - Addressed in ZA 26.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

FIRST-7	Intro	Paragraph 3	Ge	Occurred	Occurred	Not applicable since sentence is deleted – US 3.
FIRST-8	5.1		Te	does not mention any off site network storage or local wireless storage identification		Accept in principle - FIRST to provide content. Section 5.1 is renumbered to 4.3.1.
FIRST-9	5.2	E)	Ed	Document the collection and any issues in the collection. Media collection efforts can be limited by size, threat, volatility...	e) Partial Acquisition In the event that the full media or partition is not available, a partial acquisition with accompanying documentation and hashed as available.	Accepted. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition.
FIRST-10	5.2	F)	Ed	Volatile data collection. Similar justification to a partial	f) Volatile Data Acquisition In the event that the full media or partition is not available, volatile data (e.g. memory, processes, active connections...) acquisition with accompanying documentation and hashed as available.	Accepted – Addressed in UK 7. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition.
FIRST-11	5.2		Te	Any old hash function	Consider adding MD5 and /or SHA1, 256	Accept with modification – Incorporate with IT 2, rewrite sentences to include 'proven hash function, for example MD5 and/or SHA1, 256'. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition.
FIRST-12	5.2	Paragraph 2 Sentence 2	Ed	The word “approach” should probably be plural.	Due to these different conditions, different approaches and tools are required.	Accepted. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition.
FIRST-13	5.3	Para 1	Ge	Admissible	Admissible	Not applicable since sentence is changed – US 26.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

FIRST-14	5.3		Te	<i>Spoilage</i>	Consider using “ <i>Modification or destruction</i> ”	Rejected – US 17 accepted to change the term 'spoilage' to 'spoliation'. Section 5.3 is renumbered to 4.3.4.
FIRST-15	5.4	Para 1	Ed	Process must be documented and repeatable	“...is to have a repeatable, documented process to preserve the integrity of the digital data.”	Not applicable since section is deleted – JP 15.
FIRST-16	5.4		Ge	To state that the analysis process involves the use of scientifically proven methods can be challenged on the basis that there aren't any. Scientific proof is rigorous, lengthy and above all expensive;	Consider instead “accepted” rather than proven. Given that this is a standard for acquisition and preservation, is there any need from analysis in this document at all?	Not applicable since section is deleted – JP 15.
FIRST-17	5.5		Ed	Replace “interpreted”	“presented”	Not applicable since section is deleted – JP 15.
FIRST-18	5.5		Ed	Does this item need to present if this is written for First Responders?		Not applicable since section is deleted – JP 15.
FIRST-19	6		Ed digital devices that <i>may</i> contain...		Accepted. Section 6 is renumbered and split into 4.1 and 4.2.
FIRST-20	6		Te	... must use scientifically derived and proven methods.... Again, this is setting the bar extremely high, impossibly so	Consider instead “ensure practitioners adhere to de facto methods that are repeatable defensible etc”	Accepted – incorporate with US 29. Section 6 is renumbered and split into 4.1 and 4.2.
FIRST-21	6.1	Para 2	Ed	Threat is an issue	“...cost, time, and threat.”	Rejected – The recommendation in FIRST 22 to include circumstances are understood to include threats as well.
FIRST-22	6.1	Paragraph 2 Sentence 1	Ge	Suggest rewording of “but this needs to be balanced with circumstances of cost and time.” Because circumstances need to be considered as well as cost and time.	but this needs to be balanced against circumstances, cost and time.”	Accepted. Section 6.1 is renumbered to 5.2.1.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

FIRST-23	6.1	Paragraph 3 Sentence 5	Ed	Suggest rewording of “determine and apply a method for establishing the accuracy and a copy has to the original source and its reliability.”	determine and apply a method for establishing the accuracy and reliability of a copy compared to the original source.	Accepted. Section 6.1 is renumbered to 5.2.1.
FIRST-24	6.1	Paragraph 3 Sentence 7	Ed	Suggest rewording of “However, this has to be balanced with circumstances of cost and time.” Because circumstances need to be considered as well as cost and time.	However, this has to be balanced against circumstances, cost and time.”	Accepted. Section 6.1 is renumbered to 5.2.1.
FIRST-25	6.2	Paragraph 1 Sentence 3	Ed	Past tense should be applied	The DEFR was capable of undertaking the processes and of making any conclusions;	Accepted. Section 6.2 is renumbered to 4.1.1.
FIRST-26	6.2a		Te	<i>Aren't DEFRs supposed to present evidence not form conclusions?</i>		Noted – Remove bullet c. Section 6.2 is renumbered to 4.1.1.
FIRST-27	6.4	Paragraph 1 Sentence 2	Te	I have to disagree with this statement. In corporate environments, we face so many different incident response and forensic tools for so many different types of situations that is quite impossible to have been trained on everything, let alone find some means of taking competency tests. I would strongly suggest a different statement. Something along the lines of showing that the DEFR continues their education in the field.	The defence should be achieved by demonstrating that he/she has taken training relative to the tasks performed.	Accepted in principle – Incorporate with UK 9. FIRST to provide a standard level of training for incorporation into the document. Include an editor's note: NBs to comment on a standard level of training for the DEFR. Section 6.4 is renumbered to 4.1.4.
FIRST-28	7		Ed	<i>“...who is responsible.... “</i>	<i>“who has handled digital devices.....”</i>	Accepted. Section 7 is renumbered to 5.1.
FIRST-29	8.1	Para 1	Ed	DEFR may or may not be involved in the report	Clarify “...may or may not...”	Accepted – Addressed in SE 16. Section 8.1 is renumbered to 5.3.1.
FIRST-30	8.1	Para 2	Ed	Acceptability of formal or internal training programs	“...properly and adequately trained (formally or internally) to handle...”	Accept in principle – FIRST to provide content on what training is considered to be adequate.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

						Include an editor's note: NBs to comment on a standard level of training for the DEFR. Section 8.1 is renumbered to 5.3.1.
FIRST-31	8.1		Ed	"A DEFR may not be involved in the analysis and development of the report of the analysis"	"to A DEFR may not be involved in the analysis and production of the report"	Duplicate - Addressed in SE 16.
FIRST-32	8.1	Paragraph 2 Sentence 4	Te	I have to disagree with the statement "They should be properly and adequately trained to handle digital devices which may contain potential digital evidence" because people providing "technical assistance" in a corporate environment may indeed be necessary due to their technical expertise, however, they are not likely to have received any training in incident response or forensics.	The DEFR should be properly and adequately trained to handle digital devices which may contain potential digital evidence and should provide guidance to anyone providing technical assistance.	Duplicate - Addressed in FIRST 30.
FIRST-33	8.1	Paragraph 2 Sentence 5	Te	I have to disagree with this statement. In corporate environments, we face so many different incident response and forensic tools for so many different types of situations that is quite impossible to have been trained on everything, let alone find some means of taking competency tests. I would strongly suggest a different statement. Something along the lines of showing that the DEFR continues their education in the field.	The DEFR should maintain their skills through continued training.	Duplicate - Addressed in FIRST 30.
FIRST-34	8.2	Paragraph 2 Sentence 1	Te	I have to disagree with this statement. In corporate environments, we face so many different incident response and forensic tools for so many different types of situations that is quite impossible to have been trained on everything. I would strongly suggest a different statement.	When required, the DEFRs should be able to demonstrate the he/she is formally trained to handle digital evidence and understands the underlying operation of the tools used to perform the tasks.	Duplicate - Addressed in FIRST 27.
FIRST-35	8.3		Te	Should EM effects be considered, e.g. will the mobile phones need to be RF shielded at seizure?		Rejected – Consensus that the standard should not cover this topic.
FIRST-36	9		Ed	Briefing	Briefing	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

						Section 9 is renumbered to 5.4.
FIRST-37	10.1g		Ed	Delete word 'eyeball'		Accepted. Section 10.1 is renumbered to 5.3.3.1.
FIRST-38	10.2		Ed	spoilage	damage	Rejected – US 17 accepted to change the term 'spoilage' to 'spoliation'.
FIRST-39	11	Para 1 pg 11	Ge	prioritze	Prioritize	Accepted. Section 11 is renumbered to 5.8.
FIRST-40	11	Note 2 pg 11	Ge	pyhsical	Physical	Accepted. Section 11 is renumbered to 5.8.
FIRST-41	11	Paragraph 3 Sentence 5	Te	If your definition of “cache memory” is L1 and L2 internal CPU cache, then I have an issue with this statement. The CPU cache is not typically obtained through standard forensic tools.	Collect and/or acquire the most volatile digital data first such as RAM, swap space, network connections, and running process, etc.	Accepted. Section 11 is renumbered to 5.8.
FIRST-42	12.2	Paragraph 1 Sentence 2	Te	Suggest rewording of “The choice needs to be balanced with circumstances of cost and time and available resources.” Because circumstances need to be considered as well as cost and time.	The choice needs to be balanced against circumstances, cost, time and available resources.”	Accepted. Section 12.2.2 is renumbered and split into 6.1.2.2 and 6.1.3.2.
FIRST-43	12.2	Paragraph 1 Sentence 4	Te	To allow for cases where a hard drive or partition can not be imaged, I suggest a additional sentence.	In all three scenarios, the DEFR is required to make an accurate image copy of the computers’ storage media which is suspected to contain potential digital evidence. If an image cannot be obtained, accurate copies of specific files suspected to contain potential digital evidence shall be acquired.	Accepted. Section 12.2.2 is renumbered and split into 6.1.2.2 and 6.1.3.2.
FIRST-44	12.2	Para 1	Ed	Threat is a factor in this acquisition process	“...cost, time, threat, and available...”	Rejected – Threat is incorporated into circumstances.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

FIRST-45	12.2	i)	Ed	Field conditions may not allow for drive removal	"If field conditions allow, remove..."	Accepted. Section 12.2 is renumbered to 6.1.3.
FIRST-46	12.2.1	(b)	Ge	Uninterruptible	Uninterruptible	Accepted. Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.
FIRST-47	12.2.3	d)	Ed	Additional documentation is required for a partial or limited collection	d) Document collection methodology and need for the partial collection	Accepted. Section 12.2.3 is renumbered to 6.1.3.3.
FIRST-48	12.2.3	Paragraph 4 Sentence 1	Te	The wording that suggests that only a validated tool can be used for imaging is quite impractical. At least, in most corporate environments, we use much more recent versions of Encase and FTK because we need the enhanced functionality.	Execute the imaging process by using validated or otherwise well established imaging tool to create an image of the identified partition, directory or file.	Accepted. Section 12.2.3 is renumbered to 6.1.3.3.
FIRST-49	12.3	Paragraph 2 Sentence 11	Te	How many people really have biometric mechanisms to protect evidence? What is wrong with just saying keep it secure? This just opens up arguments against proper security by requiring such high standards.		Duplicate – Addressed in AU 64.1.
FIRST-50	12.2.4	(c)	Ge	identified	Identified	Accepted. Section 12.2.4 is renumbered to 6.1.3.4.
FIRST-51	13.1.1	f)	Ed	Clarification of terms	"flavours" replaced with types "usually" replaced with may be	Not applicable since sentence is deleted – AU69
FIRST-52	13.1.2	Paragraph 2 Sentence 2&3	Te	Instead of using the word "employees" use "individuals"	He/she may talk to individuals who are directly or indirectly involved with the potential digital evidence or devices to be collected. These individuals may include the system administrator, the owner of the device and users of the computer and network devices.	Superseded by AU 72. This has been applied to Clause 6.1.1.2.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

FIRST-53	13.3	(a) Para 3	Ge	involces	Involves	Accepted.
FIRST-54	14.1		Ed	"It works similar"	"they work in a similar fashion to"	Not applicable since section has been deleted – AU 76.
FIRST-55	14.1.1		Ge	craddles	Cradles	Accepted.
FIRST-56	14.1.1	Para1	Ed	Serial number and identifying features should be recorded	"...scene, their associated serial numbers and any identifying features must be recorded."	Accepted.
FIRST-57	14.2		Ed	Alter	Alters	Accepted.
FIRST-58	14.2	Para 2	Ge	evironment	Environment	Duplicate – Addressed in ZA 88.
FIRST-59	14.2	Para 3	Ge	spoilling	Spoiling	Duplicate – Addressed in ZA 89.
FIRST-60	14.2.1.	B	Ed	"it is highly recommended that..."	"immediate delivery of the device is highly recommended"	Not applicable since section has been deleted – AU 76.
FIRST-61	14.2.2	B	Ge	craddle	Cradle	Duplicate – Addressed in FIRST 55.
FIRST-62	14.3	(d)	Ge	shilded	Shielded	Accepted.
FIRST-63	15.1	Para 1	Ge	neccessary	Necessary	Accepted.
FIRST-64	15.2	(k)	Ge	circumtsances	Circumstances	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.
FIRST-65	15.2	f)	Ed	Threat is a factor in all cases	"...cost, time, and threat."	Not applicable since section has been deleted – AU 76.
FIRST-66	16.1	(f)	Ge	electricy	Electricity	Duplicate – Addressed in ZA 98.
FIRST-67	16.1	(h)	Ge	Stiffies	Clarify stiffies and consider alternate wording	Not applicable since bullet is deleted – SE 32.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

FIRST-68	Annex C	9 (FTK Imager)	Ge	Foresnic	Forensic	Not applicable since annex is deleted – SE 45.
----------	---------	----------------	----	----------	----------	--

IOCE 1	Section 3		GE	The use of the term “digital evidence” has already been defined, and its definition accepted, on an international basis by the IOCE (see www.ioce.org). IOCE defined numerous definitions at the request of the G8 and four were refined and ultimately accepted and promoted by the G8 as internationally recognized and have been in use for years. Rather than develop new definitions we request that the SC27 either incorporate the existing IOCE/G8 definitions or contact the IOCE to possibly request modification of the existing definitions.		Accepted in principle – 'Information stored or transmitted in binary form that may be relied upon in court'. Editors will follow up regarding the copyright of the definition and act accordingly. AU, JP: 'in court' may become a problem but this will be addressed in the next WD. 3.5 is renumbered to 2.4.
IOCE 2.	6.1		TE	Clarification is required over what the term Independent Digital Forensic Experts mean in the context of validation. Is this an person external to the organisation using the tool. If so this is not appropriate as there will be internal tools developed for computer examination which have been validated internally and demonstrated as fit for purpose.	Suggested change. “All tools used by the DEFR must have been validated prior to use. This validation can be carried out externally or internally but the evidence must be available upon any challenge of the technique.”	Duplicate – Addressed in UK 8.
IOCE 3	6.2		GE	The note in this section mentions that direct cost needs to be considered to carry out the standard (usually for civil matters) because in general the highest possible standards are also the most expensive. What actually needs to be considered is what quality level is required for the specific examination. Therefore costs should consider to be proportional to the quality level required and the evidence weight of potential evidence found.	Suggest.” NB Direct costs need to be consider in relation to evidential significance of the potential data stored on the device and the required quality level of the examination”	Accepted. Section 6.2 is renumbered to 4.1.1.
IOCE 4	6.4		TE	In the following sections it mentions that DEFR should	Suggested Changes “DEFR should	Duplicate – Addressed in UK 9.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				demonstrate competency before carrying out an examination. However, there is no mention of ongoing competency assessment. How do we know someone is still competent 2-3 years down the line?	undergo initial tests to ensure he/she is capable of performing the examination reliably. In addition the DEFR should be regularly reviewed to ensure ongoing competency.”	
IOCE 4.1	8.1		TE	In the following sections it mentions that DEFR should demonstrate competency before carrying out an examination. However, there is no mention of ongoing competency assessment. How do we know someone is still competent 2-3 years down the line?	Suggested Changes “DEFR should undergo initial tests to ensure he/she is capable of performing the examination reliably. In addition the DEFR should be regularly reviewed to ensure ongoing competency.”	Duplicate – Addressed in UK 9.
IOCE 4.2	8.2		TE	In the following sections it mentions that DEFR should demonstrate competency before carrying out an examination. However, there is no mention of ongoing competency assessment. How do we know someone is still competent 2-3 years down the line?	Suggested Changes “DEFR should undergo initial tests to ensure he/she is capable of performing the examination reliably. In addition the DEFR should be regularly reviewed to ensure ongoing competency.”	Duplicate – Addressed in UK 9.
IOCE 5.	12.2.1 12.2.2 12.2.3		TE	The WD refers the method of sanitizing data in accordance with the US DoD 5220.22-M National Industrial Security Program Operating Manual. Although I admit that the manual developed by US DoS is excellent, it seems to be inappropriate to refer the specific document developed by one specific organization in the WD without reviewing in ISO. In addition, there may be other solution which are appropriate which do not fall into this criteria. The main fact is to be sure that the hard disk is clean before it is used.	Suggested “The image copy will be stored on a target disk which has been sanitized of any previous data. The sanitization process must have been validated to ensure that previous data remains. One possible solution is the follow the NISPOM requirements.”	Accepted – Some challenges may exist regarding admissibility if disk sizes do not correlate. Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1. Section 12.2.2 is renumbered and split into 6.1.2.2 and 6.1.3.2. Section 12.2.3 is renumbered to 6.1.3.3.
IOCE 6.	12.3		TE	The WD mentions that collected digital devices should be stored in a secure, climate controlled environment or a location that is not subject to extreme temperature or humidity. It is difficult for some organizations to create climate controlled environment due to a lack of budget.	Suggest “Digital devices should be stored in a secure environment which is of a suitable climate which is not subjected to extreme temperature or humidity changes”	Duplicate – Addressed in US 59.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				Also digital devices these days are more robust to changing environments.		
IOCE. 7	16.1		GE	This section mentions the usage of a range of things for handling exhibits . (e.g lint-free gloves in packaging a digital device, UV light shielding package area). This are ideally situation and in practise not achievable and appropriate for all cases. It is suggest that we indicate what is Mandatory and what is desirable	Indicate that the following are Mandatory : c, l, m, n (if volatile memory), p, q, r, s The rest are Desirable or appropriate in certain cases.	Duplicate – Addressed in UK 35.
IOCE 8.	10.3	b	TE	Using an atomic clock is a bit over kill for recording time especially when we know the issues of time/date information on computers.	Suggestion “Compare the time setting with a reference clock and document them and the differences. The reference clock should be checked and ensure it is within a required tolerance (e.g. 1 minute)”	Duplicate – Addressed in UK 14.
IOCE 9	11		TE	Capture of RAM and Volatile memory is still a relatively rare and complex examination. I would suggest that the relevance of capturing this type of data is assessed before attending the scene and if required taking appropriate expertise and tools. There will be certain cases where this type of examination is important (e.g. Suspect is known to be on link and use Encryption and Passwords), however in the majority of case this is not proportional to the investigation.	Suggest giving some examples of when RAM and memory needs to be examined and recommend this is consider before attending the scene so appropriate resource can be sourced.	Duplicate – Addressed in UK 15.
IOCE 10	13.1.1	g)	TE	The sweeping of WiFi devices is just as important are normal scenes involving standard alone computers as it is for Networked Computers.	Suggestion is to include this comment in section 12 as well.	Duplicate – Addressed in US 61.
IOCE 11	14.1.1		TE	In this section it states a phone should be left in the same state it was received in but later on it states it should be switched off. The current recommendation in Europe is to switch the phone off as leaving it on can change data. There may be situation which are appropriate to leaving	Suggestion “The mobile phone should be switched off upon seizure to prevent data being changed from the receipt of communication and also in modern phone erase commands. If a phone is	Accepted - Incorporate with SE 29.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: SC 27 N7570

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				device on but these must be justified (e.g. Phone is known to come from a foreign country which will cause great problems in obtained the PUK if the phone is locked). Also switching off prevents the need for farabags.	left on documented justification must be provided (e.g. Foreign Phone which would delay time critical examination in obtained PUK through INTERPOL)."	
IOCE 12	Appendix C		TE	Great care needs to be taken when producing a list of validated Imaging Tools. The main concern is that the user of the tools needs to be aware of the validation documentation and what the testing criteria where and any resulting limitation. Just stating a list of tools might mean first Responder might think all functions of a tool are o.k when the Validation only covered part of the functionality or highlight functionality not to be used. I would say this is significant of the mobile device software as we know that phone software can not get everything so user needs to be aware of limitations.	Suggestion "The following list of forensic tools have been validated by NIST. If the DEFR is to use the NIST validation as evidence that the tools are fit for purpose they must familiarise themselves with the validation documentation and ensure themselves that the test criteria and any recommendation are appropriate for there use"	Not applicable since annex is deleted – SE 45.
IOCE 13	12.2.1		TE	All of the points raised here are ideal and appropriate in some cases. It is recommended that the caterogised as Mandatory and Desirable	M = a, b, d, e, m, j (see previous comment) D = f, h, l,	Duplicate – Addressed in UK 18.
IOCE 14	12.3	b	TE	Document states Hard Disk should be placed in Anti-static bags. This is an ideal situation and not critical if they are not due to the robust of technology now.	Suggestion "The DEFR should consider the sensitivity of the digital device to static electricity, if this is a concern then device should be secured in a anti-static bag".	Duplicate – Addressed in UK 20.
IOCE 15	5		ED	Failure to do so may render it unusability ... should be unusable		Duplicate – Addressed in ZA 39.
IOCE 16	5.1		ED	"...evidence could be located eg. Hard-disk": This sentence is missing some words. Also: logical may refer to the actual digital data, not just an address. This paragraph is too vague.		Noted. Section 5.1 is renumbered to 4.3.1.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

IOCE 17	5.2		TE	No mention is made on: - acquisition of volatile data - acquisition of storage media, partitions, files and blobs under the condition of a running system - acquisition should be reliable and repeatable and well-documented		Duplicate – Addressed in UK 7.
IOCE 18	6.3		TE	Repeatability is not always possible in the event of volatile data acquisition or when the evidence can only be extracted from the medium by means of destructive research (e.g. part replacement in HDDs)	Suggest stating “This section relates to hard disks but not volatile memory as it is not possible to get repeatable results due to the dynamic nature of the memory”	Duplicate – Addressed in UK 11.
IOCE 19	8.3		TE	Could be expanded towards risk for digital evidence. Assessing the risk that evidence might be manipulated or systems under investigation might be booby-trapped may also be important to mention here.	Suggestion adding “Could data have been compromised” and “Consider of the device has been booby trapped to destroy data if switched off or accessed in a uncontrolled way”	Duplicate – Addressed in UK 12.
IOCE 20	10.2		TE	Other things to consider - whether we want to capture the modus-operandi of a suspect during abuse of a system - whether we want the suspect to believe he is still undetected (covert)		Accepted in principle - Refrain from using Latin expressions such as 'modus-operandi'. Section 10.2 is renumbered to 5.3.3.2.
IOCE 21	12.2.1		TE	Between a and b: consider logical acquisition when full-disk-encryption is suspected. First check if this may be the case by looking at the raw disk or some crypto-detection utility. Also, make a photograph of the system (if present) clock next to a DCF-clock. Record time of each performed action. Same holds for 12.2.3		Duplicate – Addressed in UK 17.
IOCE 22	13.2		TE	Consider possibility of sabotage by suspect through active network connection. Monitor for this or decide to		Duplicate – Addressed in US 62.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				disconnect.		
IOCE 23	11		TE	Prioritise collection and/or acquisition of Order of Volatility . Might be worth adding some other examines	Add examples "Sat Navs, CCRV Systems, Automotive electronic, Improvised electronics (Bank Card Skimming)	Duplicate – Addressed in UK 16.
IOCE 24	14.2		TE	"Some mobile devices have to be switched on to access the module, whilst other acquisitions can be done directly from the SIM card." Unclear what is meant by the second part of this sentence. "There is also a wide range of memory devices that are used in conjunction with mobile devices, such as MicroDrives and SD cards." These generally have a standard interface, so they can be read with standard readers and write blockers. Be considerate though that removing a storage card from a handheld device that is switched on, this action might interfere with processes running in the background. For example, suppose a navigation application is running in the background on a smartphone. Make sure it is known what happens if the memory card containing card material is removed from the smartphone, before doing this on the actual evidentiary device.		Duplicate – addressed in US 65.
IOCE 25	14.2.1		GE	"For a mobile device which is found to be on, DEFR should also use a faraday box" remove 'also' "b) If the device is continued to be left on ... to the lab for examination." It should be mentioned that GPS (factory-built into cars) enabled devices should not be moved unshielded because new location data might be gathered during		Duplicate – Addressed in US 66.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				transport. "c) If the device is at appropriate intervals to ensure the data is not lost" Preferably connect a charger to the device continuously. Make sure that a longer power cut is not left unnoticed.		
IOCE 26	14.2.2		TE	"b) Also collect all associated mobile device items such as charger, memory card, SIM card, cradle and so on." - This should go to the general section because it also holds for 'switched on' devices. - also try to find original packaging of mobile phones, these might contain notes with PIN and PUK codes		Duplicate – Addressed in UK 34.
IOCE 27	15.1		TE	Some suggested changes to be made and also moving section to general area as common to all types of devices.	"Next, the DEFR should identify the type, brand and model of the CCTV system" Also serial number should be noted, this might be useful to determine firmware versions. The manufacturer/distributor might have data on the device, accessible through serial number. "The DEFR should document all other items at the scene that may contain potential evidences such as scribbled notes, sticky notes, diary and so on." This is general for all DE investigations, move to general part.	Duplicate – Addressed in US 69.
IOCE 28	13.2	g	TE	No mention of WiFi safety. It is important that the DEFR does not introduce WiFi devices into the scene which might change pairing information on potential evidential devices. This is particularly important if investigation needs to know what devices have been connected.	Include in Section 13 somewhere "It is important that the DEFR does not introduce WiFi devices into the scene which might change pairing information on potential evidential devices. This is	Duplicate – Addressed in UK 24.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					particularly important if investigation needs to know what devices have been connected"	
--	--	--	--	--	---	--

[IT] 1	5.2	Clause a.	te	In the second part of this clause are mentioned the unallocated space and the slack space as area that the acquisition method employed must be able to obtain, but is missing the HPA (Host/Hidden Protected Area) that is neither unallocated nor slack space. (Reference: https://www.utica.edu/academic/institutes/ecii/publications/articles/EFE36584-D13F-2962-67BEB146864A2671.pdf)	Just add HPA. "[...] This acquisition method employed must be able to obtain the unallocated space, the slack space and the HPA of the media."	Accepted. HPA is also included in the terminology section 3.11. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition.
[IT] 2	5.2 12.3 13.3 15.3	Clauses a, b, c, d. Clause a, paragraph 1 Clause a, paragraph 1 Clause a, paragraph 1	te	In the document is written that DEFR should produce a hash of the image acquired using any hash function. In the forensics community is becoming (or it has already become) a standard de facto hashing the images acquired only with MD5. This for obvious reasons of performance, since it is very fast especially when it comes to big amount of data, and probably ignorance about the fact that such algorithm has been broken (collisions attack [1][2]). Since it has been also shown how to generate a document which makes complete sense with the same md5 value desired, a DEFR cannot use "any" hash function, especially when it comes to imaging just files instead of entire hard disks. Therefore, since is not good to oblige DEFR to use a certain hash algorithm, it would better at least to advice a way. A good solution would be to use both md5 and sha1 hash. Although md5 is broken (and recently also sha1 [3][4] but is still not very feasible as md5, at least for what it matters to forensics analysts), the probability to have a	Additional text will be provided upon acceptance of this comment.	Accepted in principle with modification – IT to provide content. MD5 has not been broken for hashing. Rather refer to 'currently approved / legally accepted hashing function' to future proof the standard. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition. Sections 13.3 and 15.3 are incorporated into 6.7.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<p>collision on both algorithm is very low (about 2²⁸⁸ without counting the birthday paradox, but it would be still too low). This will assure the analyst about the collisions and it is also a good solution from a performance point of view, instead of using only one stronger algorithm that will take long time with a big amount of data.</p> <p>References:</p> <p>1. http://www.iacr.org/archive/eurocrypt2005/34940019/34940019.pdf</p> <p>2. http://eprint.iacr.org/2004/199</p> <p>3. http://eurocrypt2009rump.cr.ypt/837a0a8086fa6ca714249409ddfae43d.pdf</p> <p>4. http://www.schneier.com/blog/archives/2009/06/ever_better_cry.html</p>		
[IT] 3	12.2.1 12.2.3	Clause a Clause a	te	<p>In this clause are mentioned as volatile data to acquire on a powered on computer system, only RAM and running processes. Other volatile data to collect, that are not mentioned but are very important anyway, are the information regarding the network connections that may be active and the date/time of the system. Moreover, since when we are doing incident response the computer may be infected or anyway is not trustworthy, the DEFR must always run his own trusted tools (static binaries so there are no calls to external "unreliable" libraries).</p> <p>Finally, latest computers (mainly notebook) are using a new technology called "Turbo Memory", developed by Intel. Although this is a NAND flash memory module used to load much quicker the operative system and the main applications used, it could be used also as normal memory and so it would need to be acquired before shutting down the system. This would be a "precautionary" acquisition since the functioning of this</p>	<p>Substitute with: "First and foremost, consider acquiring the digital data that may otherwise be lost if the computer system is powered off. They are also known as volatile data and data stored on Random Access Memory (RAM), running processes and network connections, date/time of the system are such data. RAM also contains useful information such as decrypted applications and passwords. Other than RAM, newest computers (mainly notebook) may be equipped with the Turbo Memory module, which may eventually contain the same kind of information stored in the RAM.</p> <p>DEFR must never trust the programs on the systems. For this reason it is</p>	<p>Accepted with modification – Introducing tools to the system may displace potential evidence and content of memory may be paged out when binaries are loaded.</p> <p>Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.</p> <p>Section 12.2.3 is renumbered to 6.1.3.3.</p>

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				module is not standard and well-known yet. A DEFR has to be aware of this.	recommended the DEFR to use his own trusted tools (static binaries). Ensure that all the actions performed and the resulting changes made to the computer system are recorded and understood.”	
[IT] 4	12.2.1		te	<p>When describing how to acquire a powered on computer system, is missing the scenario when the computer is on but is locked. In this case it's not possible to acquire volatile data in the usual way described. To do this there are several “attack” that can be used, and a DEFR must be aware of this since, in many country, a person is not obliged by law to reveal the password to unlock his own computer.</p> <p>One of this attack is called “Cold Boot Attack”. The attack relies on the data remanence property of DRAM and SRAM to retrieve memory contents which remain readable in the seconds to minutes after power has been removed [1][2]. Therefore if the RAM is removed immediately and its temperature is lowered more than - 20C°, the content of the RAM can be “frozen”. In this way the DEFR will have “physical” access to the volatile data.</p> <p>The other attack/way is to exploit the external direct access to DMA, such as firewire/IEEE1394 or PCMCIA. Devices connected through firewire have read/write access to physical memory via DMA [3][4], that means the OS will not even be “notified” of this.</p> <p>Being all this hardware standard and so independent of OS, those attacks can be applied to any computer regardless the OS used.</p> <p>References: 1. http://citp.princeton.edu/memory/</p>	A new clause would be needed. Additional text will be provided upon acceptance of this comment.	<p>Accepted in principle – IT to provide content.</p> <p>Include an editor's note: NBs to comment on what to do when machine is on but locked.</p> <p>Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.</p>

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<p>2. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-536.html</p> <p>3. http://www.storm.net.nz/static/files/ohci_11.pdf</p> <p>4. http://md.hudora.de/presentations/firewire/PacSec2004.pdf</p>		
[IT] 5	14.2.2		te	It should be specified that the mobile device has to be acquired before the SIM card. This because, in almost every mobile device, it is needed to remove the battery to access the SIM card. Removing the battery may cause the loss of important information, depending on the device.	Add clause C: "DEFR should always acquire the mobile device before to remove the battery (to access, for example, to the SIM card), in order to prevent the loss of important information."	Accepted.

JP-1	All		Ge	<p>The objective of this standard is not show clearly. Readers could be confused what is expected to do. For example, the management of the organization should be the intended user of this International Standard, because he/she is responsible in meeting the jurisdictional requirements by preparing resources to meet the gap between DEFR activity and jurisdictional requirements. Current WD provides guidance for DEFR only, which seems to be of the second priority. Management of the organization should be the intended user of this International Standard. Japanese NB concerns this standard will not be widely used because of this ambiguity.</p>	The scope, target readers and the supposed usage of this standard should be clearly defined at least in Clause 1.	Accepted with modification – The intended audience should be wider than only the DEFR, but does not include management level. Management as audience might be addressed in a future project on forensic readiness.
JP-2	All		Ge	ISO/IEC "2703X"s are addressed to support ISO/IEC "2700X"s. This WD 27037 has references to 27001 and 27002, however, it is not clearly described which portions of these standards are relevant.	Add a cross reference table of 27001/27002 vs 27037, like Annex E of 27035.	Accepted in principle – JP to contribute cross reference table to editors as soon as the new document structure have been circulated.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<p>Although 27037 is expected to give concrete shape of 13.2.3 of 27002, current version is not enough to meet. Furthermore, the other relations should be investigated. (for example, 10.10, 27002)</p> <p>To improve the above point, the cross reference between this document and ISO/IEC 27002 (and ISO/IEC 27001, if needed) seems to be effective.</p>		
JP-3	All		Ge	<p>It is not easy to understand this standard because of the structure.</p> <ul style="list-style-type: none"> - Clause 12-15 explain identification, collection, and acquisition process depends on the type of devices. It is quite useful, however, it isn't linked with Clause 11 (device list), or Annex A (potential digital evidence). - As clause 16 describes common sub-process of all type of devices, it could be related Clause 12-15. But the relation is not appeared. - Subclause 8.3 describes "risk assessment". But risk assessment is not necessarily DEFR's role. - Although the explanation concerning DEFR describes Clause 8 and Clause 10, the necessity cannot be understood. - Clause 7 is related to the entire scope of this standard. 	<p>Review the structure of this standard. Japanese NB provides example of the structure of this standard.</p> <p>See Attachment-1</p>	Accepted.
JP-4	All		Ge	<p>The scope of this standard seems to be immature.</p> <p>1, 1st para "This International Standard provides guidance on the digital evidence management describing the process of recognition and identification, collection and/or acquisition and preservation of digital data ..."</p> <p>1, 2nd para "It is applicable to organisations needing to conduct the identification, collection and/or acquisition and</p>	<p>Keep consistency on the scope through this standard.</p>	<p>Accepted – All references to 'digital data' and 'digital evidence' will be changed to 'potential digital evidence' to maintain consistency throughout the document. These changes are made where applicable in context.</p>

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<p>preservation of digital evidence ...”</p> <p>1. 5th para “Clause 6 describes the core principles for <u>identification, collection and/or acquisition and preservation of potential digital evidence</u>”</p> <p>1.1 1st para “who are responsible in <u>identifying, collecting and/or acquiring and preservation of potential digital evidence</u>”</p> <p>1.2 1st para “...that describe the process of recognizing and identifying, collecting and/or acquisition and preserving potential digital evidence.”</p> <p>5. 2nd para “Digital evidence management includes a generic model of <u>identification, collection and/or acquisition, preservation, analysis and presentation of digital evidence.</u>”</p> <p>5. Note “Note: The scope of this guideline is <u>identification, collection and/or acquisition and preservation only</u>”</p>		
JP-5	All		Ge	<p>In this document, the verbal forms don't seem to be used appropriately.</p> <ul style="list-style-type: none"> - Although this standard provides just “guidelines” (not “REQUIREMENTS”), “must” appears frequently. - Lots of “may” or “can” are used in 27037. <p>Verbal forms for the expression are defined in ISO/IEC Directive Part 2, Annex H.</p>	<p>Replace “must” with “should”. And Review “may” and “can” are used appropriately or not.</p>	Accepted.
JP-6	Introduction and '1 Scope'	All	Ge	<p>Validity of digital evidence rests on the jurisdictions, and therefore, there is no internationally common set of legal or regulatory base to support validity of digital evidence.</p>	<p>In order to make the evidence valid, users of this International Standard are required to adapt and amend the procedures shown in this standard in</p>	Accepted. Incorporated into Section 1, Scope.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: SC 27 N7570

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					accordance with the nation's legal requirements for evidence. Incorporate this requirement in the Introduction and '1 Scope'.	
JP-7	Introduction	5 th para.	Ge	The paragraph reads as follows. This standard should not replace specific legal requirements of a particular jurisdiction. Instead, this standard may serve as a practical guideline for Digital Evidence First Responder in investigations involving digital evidence <u>and may facilitate exchange of digital evidence between jurisdictions.</u> This is misleading. Validity of digital evidence is solely judged by the court in charge of the case based on the applicable national or state law which the court is subject to. The other nation's jurisdiction does not take part in the judgement.	Delete the last part of this paragraph (after "and may facilitate...").	Rejected – A new paragraph will be constructed by the editors and JP to eliminate potentially misleading content. A stronger emphasis will be placed on the exchange of digital evidence between jurisdictions in the new content. The new content will refer to ' DEFR and/or Digital Evidence Specialists'.
JP-8	1.2	Objective	Ge	The WD reads as follows; Not only it will assist organisations in their disciplinary procedures, it will also facilitate the exchange of potential digital evidence between jurisdictions. This is misleading. See JP-7 above.	Delete this sentence.	Rejected – A new paragraph will be constructed by the editors and JP to eliminate potentially misleading content.
JP-9	1		Ed	It is inappropriate to write the structure of this standard in Clause 1 (Scope).	Move the 5 th para to other clause. Some of 27000 series have Clause 3 "Structure of this standard" to describe such information.	Accepted - Paragraph 5 has been addressed in ZA 22.
JP-10	Introduction 1		Ed	"Digital Evidence First Responder" is used in Introduction, but DEFR (Digital Evidence First Responder) is defined 3.7. Is such use appropriate?		Rejected.
JP-11	1		Ed	Clause 1 has redundant structure within itself. Similar contents could be found in the paragraphs just below the	Delete subclauses 1.1 and 1.2 of clause	Accepted – Content of ZA 25, ZA 27

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				clause and subclauses 1.1 or 1.2.	1.	and AU 5.1 will be combined and incorporated into the new clause 1.
JP-12	2		TE	Are 27001 and 27002 “Normative Reference”? This standard can be read by itself, not need 27001 or 27002 to understand.	Remove 27001 and 27002 from Clause 2 and add these standards to the Bibliography list.	Accepted. Section on normative references becomes obsolete, and all subsequent section numbering are adjusted accordingly.
JP-13	2		TE	Is 10118 “Normative Reference”? This standard just says that it is appropriate to use the hash algorithm explained by 10118. This seems to be just “information”.	Remove 10118 from Clause 2 and add to the Bibliography list.	Accepted. Section on normative references becomes obsolete, and all subsequent section numbering are adjusted accordingly.
JP-14	5		Ed	Title of clause 5 is not appropriate. The content of clause 5 shows overview of the process.	Review the title of Clause 5.	Accepted - New structure according to JP 18 changes this title to 'Overview'.
JP-15	5		Te	Clause 5 explains the overall of Digital Evidence Management. However, the scope of this standard is a part of “digital evidence management”, this clause should be reviewed for the following reasons: - The last sentence of page 4 (maybe Editor’s note?) is the most important, because Clause 5 describes over the scope of this standard. - 4 types of acquisition methods are explained in 5.2, but these methods are not use the other part of this standard.	Change clause 5 as follows: - Move this sentence as main text. - Review the necessity of these explanations of acquisition methods.	Accept in principle. Move note to first sentence in the main text. Remove reference to analysis and presentation (out of the standard's scope). More NBs commented on acquisition methods. This section will be extended to enhance content.
JP-16	Annex C	All	Te	Products are listed in Annex C. Any mention to products is inappropriate for an International Standard.	Delete Annex C.	Duplicate – Addressed in SE 45.
JP-17	Bibliography	[1]	Te	Bibliography contains reference to the ISO/IEC Directives, Part 2, which is intended to be read by the writers or editors of the International Standards and inappropriate to be listed here. Other references should also be checked on the same	Delete reference to ISO/IEC Directives, Part 2 in the Bibliography. Delete other references if those are for the writers or editors of standards, and not for the readers of this standard.	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				principle.		
JP-18	All			Change structure of document.	See below:	Accepted.

Current Structure of 1st WD27037		Proposed Structure	
	Foreword		Foreword
	Introduction		Introduction
1	Scope	1	Scope
1.1	Audience		
1.2	Objective		
2	Normative references	2	Normative references
3	Terms and definitions	3	Terms and definitions
4	Abbreviated terms	4	Abbreviated terms
		5	Overview
5	Digital Evidence Management	5.1	Digital evidence management process
5.1	Identification	5.1.1	Identification

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

Current Structure of 1st WD27037		Proposed Structure	
5.2	Collection and/or Acquisition	5.1.2	Collection and/or Acquisition
5.3	Preservation	5.1.3	Preservation
5.4	Analysis	5.1.4	Analysis
5.5	Presentation	5.1.5	Presentation
6	Core Principles for Identification, Collection and/or Acquisition and Preservation of Potential Digital Evidence	5.2	Principles
6.1	Methodical	5.2.1	Methodical
6.2	Auditable	5.2.2	Auditable
6.3	Repeatable	5.2.3	Repeatable
6.4	Defensible	5.2.4	Defensible
		6	Key components
7	Chain of custody	6.1	Chain of custody
	(moved from current 8.3)	6.2	Risk assessment
8	Digital Evidence First Responder	6.3	Digital Evidence First Responder

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

Current Structure of 1st WD27037		Proposed Structure	
8.1	General	6.3.1	General
8.2	Competency	6.3.2	Competency
	(moved from current 10)	6.3.3	Initial actions
		6.3.3.1	Secure and protect the location
		6.3.3.2	Employ Due Care
		6.3.3.3	Documentation
8.3	Risk assessment		
9	Briefing	6.4	Briefing
	(moved from current 16.1)	6.5	Packaging of potential digital evidence
	(moved from current 16.2)	6.6	Transporting of potential digital evidence
10	Initial Actions of A Digital Evidence First Responder		
10.1	Secure and protect the location		
10.2	Employ Due Care		

1 MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

	Current Structure of 1st WD27037		Proposed Structure
10.3	Documentation		
11	Prioritize Collection and/or Acquisition by Order of Volatility	6.7	Prioritize Collection and/or Acquisition by Order of Volatility
		7	Use cases of identification, collection and/or acquisition and preservation
12	Computers, Storage Media and Peripheral Devices	7.1	Computers, Storage Media and Peripheral Devices
12.1	Identification	7.1.1	Identification
12.1.1	Physical location search and documentation	7.1.1.1	Physical location search and documentation
12.1.2	Non-digital evidence collection	7.1.1.2	Non-digital evidence collection
12.2	Collection and/or Acquisition	7.1.2	Collection and/or Acquisition
12.2.1	Powered On Computer System	7.1.2.1	Powered On Computer System
12.2.2	Powered Off Computer System	7.1.2.2	Powered Off Computer System
12.2.3	Mission Critical Computer System	7.1.2.3	Mission Critical Computer System
12.2.4	Storage Media	7.1.2.4	Storage Media
12.3	Preservation	7.1.3	Preservation

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

	Current Structure of 1st WD27037		Proposed Structure
13	Networked Computers and Network Devices	7.2	Networked Computers and Network Devices
13.1	Identification	7.2.1	Identification
13.1.1	Physical location search and documentation	7.2.1.1	Physical location search and documentation
13.1.2	Non-digital evidence collection	7.2.1.2	Non-digital evidence collection
13.2	Collection and/or Acquisition	7.2.2	Collection and/or Acquisition
13.3	Preservation	7.2.3	Preservation
14	Mobile Devices	7.3	Mobile Devices
14.1	Identification.	7.3.1	Identification.
14.1.1	Physical location search and documentation	7.3.1.1	Physical location search and documentation
14.2	Collection and acquisition	7.3.2	Collection and acquisition
14.2.1	Switched on mobile device	7.3.2.1	Switched on mobile device
14.2.2	Switched off mobile device	7.3.2.2	Switched off mobile device
14.3	Preservation	7.3.3	Preservation

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

	Current Structure of 1st WD27037		Proposed Structure
15	Digital CCTV System	7.4	Digital CCTV System
15.1	Identification	7.4.1	Identification
15.2	Collection and/or Acquisition	7.4.2	Collection and/or Acquisition
15.3	Preservation	7.4.3	Preservation
16	Packaging and transporting of potential digital evidence		
16.1	Packaging		
16.2	Transporting		
Annex A	Examples of potential digital evidence that relates to specific types of investigations	Annex A	Examples of potential digital evidence that relates to specific types of investigations
Annex B	Examples of electronic devices and potential digital evidence	Annex B	Examples of electronic devices and potential digital evidence
Annex C	List of Validated Imaging Tools for Digital Evidence Acquisition	Annex C	List of Validated Imaging Tools for Digital Evidence Acquisition
	Bibliography		Bibliography

SE 1		Ge	Overall the document is too detailed.		Accepted with modification – The
------	--	----	---------------------------------------	--	----------------------------------

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

						document should be modified to be more consistent regarding the level of detail included. In the new WD there should be a clearer distinction between 'must haves' (where detail is required) and 'nice to haves' (where less detail is required). This comment is addressed in more detail in IOCE 7, IOCE 13, UK 18, UK 35, US 49 and US 83.
SE 2			Ge	The content of the document varies from very basic procedures to a highly technical level, such as 14.2.1 c).	Consider keeping the content at the same level through out the whole document.	Duplication – Addressed in SE 1.
SE 3			Ge	At some extent the document raises more questions than it answers. It should be more obvious who is the target audience and how the standard will impact on existing procedures		Noted - SE to provide specific content where the document raises questions. The intended audience is addressed in JP 1.
SE 4	Whole document		Te	We oppose the use of the term “copy” throughout the document which is not accurate due to lack of write history.	Rephrase to “bitwise copy” or “forensic copy”.	Accepted with modification – Editors' discretion to use alternative terms where applicable. Include editor's note for comment on the use of the terms.
SE 5	Scope or 5		Te	Clarify the status of this standard in relationship to national law, rules and regulations.	Add sentence: “Application of this standard requires compliance with national law, rules and regulations.”	Accepted. Included in Section 1, Scope.
SE 6	3		Te	Common terms related to information security should not be defined in this document. Only terms directly related to the forensic field should be defined.	Delete all terms which are defined in other ISO standards. Retain terms and definitions such as Digital Evidence First Responder.	Accepted in principle – SE to provide content.
SE 7	3.11, 3.12		Te	We oppose the expression “exact mirror copy”, which is not accurate due to lack of write history.	Rephrase to “bitwise copy” or “forensic copy”.	Accepted in principle – Incorporate with AU9.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

SE 8	3.6		Te	It is not possible or practical to obtain a forensic image in all cases. Performance intensive systems or critical infrastructure systems may not always allow forensic copying, as well as in cloud computing or virtual environments.	<p>“digital evidence copy”</p> <p>Only retain this sentence: a copy of digital data obtained in a forensically sound manner.</p> <p>Delete the sentence: Also called a forensic image.</p>	Accepted in principle – Incorporate with AU8. 3.6 is renumbered to 2.5.
SE 9	3.7		Te	Change definition as proposed, there are different ways to collect digital evidence.	Digital Evidence First Responder person(s) collecting digital evidence who is authorized, qualified and/or trained in digital evidence collection with responsibility for handling that evidence	Accepted in principle – SE and AU to redefine definition that is not the same as the definition for Digital Evidence Specialist, the focus should be on first person on scene, not qualification. 3.7 is renumbered to 2.6.
SE 10	New		Te	Proposed new role to be referenced in the text.	Digital Evidence Examiner person(s) trained in analyzing digital evidence and responsible for the analysis and scientific based conclusions	Rejected - New term for Digital Evidence Specialist will be included (see AU 8.1).
SE 11	New		Te	Proposed new role to be referenced in the text.	Supporting expert person(s) providing expertise in his/her field of competence as requested by the DEE	Rejected - New term for Digital Evidence Specialist will be included (see AU 8.1).
SE 12	5		Te	Move text regarding environment from 16.2 to 5 and change the text to be more general.	New text in clause 5: The entire process should allow for an average environment: moisture, high humidity and excessive heat or cold may have a negative impact on the data stored on the potential evidence media.	Accepted in principle. In the new structure, text from 16.1 and 16.2 are moved to new section 5.
SE 13	6.3 b), d)		Te	Already covered by bullet c). b) and d) are unreasonable.	Delete b) and d)	Duplicate – Addressed in AU 26.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

SE 14	6.4 Note		Te	This may differ from country to country.	Change "required" to "preferred"	Accepted. Section 6.4 is renumbered to 4.1.4.
SE 15	8		Te		Change heading of clause 8 to: Roles and responsibilities and explain different roles further.	Accept in principle – The new structure according to JP 18 determines the relevant clause. Roles and responsibilities of both DEFR and Digital Evidence Specialist will be included.
SE 16	8	Second sentence	Te	This sentence implies unnecessary limitations	Remove sentence: A DEFR may not be involved in the analysis and development of the report of the analysis.	Accept with modification – one person can have more than one role, but a DEFR as such should not be involved with analysis and reporting.
SE 17	11		Te		Delete text from "Devices.." to circumstances." Insert new text: This includes all information storage equipment, for example ICT and external storage.	Accepted. Section 11 is renumbered to 5.8.
SE 18	12.2.1		Te	Too detailed guidance which is partly outdated and some methods are not efficient.	Remove bullet point f-j)	Rejected – Floppy disk drive may still be relevant in legacy systems. Incorporate as Desirable (see UK 18). Refer to SE 21: reject use of words step-by-step.
SE 19	12.2.2		Te	Too detailed guidance which is partly outdated and some methods are not efficient.	Remove bullet point c-g	Duplicate – Addressed in SE 18.
SE 20	12.2.3		Te	No evidence supports that earlier data on the target device may interfere with the forensic storage device. The requirement for a validated tool is impossible to fulfill.	Remove bullet point c	Duplicate – Addressed in SE 18.
SE 21	12.2.3			This is not always the most proper procedure.	Delete sentence: Following is the step-by-step guidelines to conduct	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					acquisition on mission critical computer system:	Section 12.2.3 is renumbered to 6.1.3.3.
SE 22	12.2.4 d)		Te		Delete text: "suitable for the nature of the media, such as shrink wrap plastic, to avoid contamination of the media prior to transporting to another location. Shock resistance packaging can be used to avoid physical damage to any components of the media."	Accepted - DEFR should handle case by case. The jurisdiction may have an influence on this. Section 12.2.4 is renumbered to 6.1.3.4.
SE 23	12.2.4 j)		Te		Delete text: "a secure, climate controlled environment or a location that is not subject to extreme temperature or humidity. It should not be exposed to magnetic fields, dust, vibration, moisture, or any other environmental elements that may damage it." Replace with: "in a suitable environment for data preservation."	Accepted. Section 12.2.4 is renumbered to 6.1.3.4.
SE 24	13.1.1 a)		Te	Remove a) since it is covered by bullet point b).	Delete bullet point a).	Accept with modification – merge and remove duplication.
SE 25	13.1.1 e), f)		Te	Remove bullet points e) and f) since they are covered by the introduction in 3.1.	Delete bullet point e) and f).	Accepted.
SE 26	13.3 b)		Te	Already covered by the text "suitable for the device".	Delete text: "such as shrink wrap plastic, to avoid contamination of the network device(s) prior to transporting to other location(s)."	Accepted.
SE 27	12.2.4 13.3.3 d)		Te	The requirement for "ink pen" is too specific. The choice of pen may change depending on the environment and circumstances.	Change to a more generic requirement, such as "suitable for labeling and archiving".	Accepted. Section 12.2.4 is renumbered to 6.1.3.4.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

SE 28	13.3 d), e), f) 12.3 d), e), f)		Te	This text is repeated in several places throughout the document.	All guidelines covering the same issue should be in one section of the standard. Propose to move text concerning covering and packaging to clause 16.	Accepted.
SE 29	14.1.1		Te	Under some circumstances it will be more important to disconnect the mobile device from the network by switching it off, rather than keeping it on. Switching it off will protect information from being erased or lost. If the PIN code is not available it is correct to keep the device on. In Sweden it is possible to request the PUK code from the operator.	Take this in to consideration when updating the text.	Accepted with modification – Include note that this is not applicable in all countries.
SE 30	16		Te	All guidelines regarding packaging should be in clause 16 in order to make easy to access for the user. In the current version of the document it is spread out through out the document.	Update the document accordingly.	Duplicate – Addressed in AU 78.1.
SE 31	16.1 d)		Te	The example may be misleading in some circumstances.	Delete the example: "such as polypropylene"	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
SE 32	16.1 h)		Te	The guidelines provided in bullet point h) is redundant.	Delete bullet point h).	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
SE 33	16.1 i)		Te	This is an explanation of the concept, but provides no guidance.	Additional guideline should be provided, such as to transfer the content to other media.	Accepted in principle – SE to provide content. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
SE 34	16.1. j) 5		Te	Already covered by second sentence in clause 5, consider adding generic text on handling all digital evidence with care in clause 5.	Delete sentence: "Disks should never be flexed, bent or picked up by the centre hole of the disk during the packaging process. DEFRs must handle	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					potential digital evidence devices with care and prevent the media from being bumped or dropped.” Consider adding generic text on handling all digital evidence with care in clause 5.	
SE 35	16.1 l)		Te	The requirement for “ink” is too specific. The choice of labeling may change depending on the environment and circumstances.	Change to a more generic requirement, such as “suitable for labeling and archiving”.	Superceded by SE 27.
SE 36	16.1 m)		Te	Out of a national perspective the guidance on chain of custody provided may be too specific and not applicable.	Change sentence to: “To ensure correct identification, the investigator should tag each evidence.”	Accepted in principle. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
SE 37	16.1 o)		Te		Add sentence: “In case of prioritizing the decision should be made by the commissioning body.”	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
SE 38	16.1 q)		Te	The examples are too limiting.	Delete examples: “such as serial number, model number, and part number. Delete text: “of a floppy disk or hard disk”	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
SE 39	16.1 s)			National law, rules and regulations may vary.	Delete bullet point s)	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
SE 40	16.2		Te	Too specific and extensive for some nations.	Delete sentence: “If possible, the DEFR should photograph/videotape and document the handling of evidence leaving the scene to the transport vehicle.” and “If possible, the DEFR should photograph/videotape and	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					document the handling of evidence leaving the transport vehicle to the examination and storage facility.	
SE 41	16.2		Te	Move text regarding environment from 16.2 to 5 and change the text to be more general.	Delete this text in clause 16.2 and insert amended text in 5: The transportation process should also allow for an average environment: moisture, high humidity and excessive heat or cold may have a negative impact on the data stored on the potential evidence media.	Accepted - New structure according to JP 18 will determine new clause. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
SE 42	Annex A		Te	The purpose and justification of this table need to be explained in the document. We view it as a suitable overview for the commissioning body. It is not a complete list and the references of evidence relating to certain types of crimes need improvement.	Annex A need to be further discussed and developed if it is to be retained in the document.	Duplicate – Addressed in AU 84.
SE 43	Annex B		Te		Change sentence to: “Table 2 – Electronic devices that may contain potential digital evidence”	Accepted to rework the Annex or to link to existing external site for further information.
SE 44	Annex B		Te	This annex may be outdated shortly after the standard is published. Will there be a mechanism for updating the annex in line with the technical development?	For discussion during the meeting in Redmond.	Duplicate – Addressed in AU 85.
SE 45	Annex C		Te	This annex may be outdated shortly after the standard is published. Will there be a mechanism for updating the annex in line with new releases? The list of tools in not complete and the meaning of “validated” in not explained. Does it mean that they deliver the same results with same level of security. The actual performance of the tools is not displayed, with the benefits and problems of each tool.	Delete Annex C.	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

UK 1	Document Information Page	Title	Ge	Previous DoC: "UK NB to propose a new project on the forensic readiness within an organization; UK NB to liaise with SC7/WG1A on digital forensic governance project."	None at this iteration : awaiting discussions with SC7/WG1A on digital forensic governance project. This may lead to a proposal for a new project on forensic readiness within an organization, which would probably be best met by changing ISO/IEC 27037 from single-part to multi-part standard	Noted - UK to propose new project at next iteration. Previous DoC rejected this proposal to prevent a potential delay in the progress of this project.
UK 2	2	Normative References	Ed	Should include both ISO/IEC 27031 and ISO/IEC27035 (the latter to meet disposition of comments on ISO//IEC27035, SC27 N7565)	Add ISO/IEC 27031 and ISO/IEC27035	Accepted with modification – These standards will be included in the bibliography. Section on normative references becomes obsolete, and all subsequent section numbering are adjusted accordingly.
UK 3	3		Ge	The use of the term "digital evidence" has already been defined, and its definition accepted, on an international basis by the IOCE (see www.ioce.org). IOCE defined numerous definitions at the request of the G8 and four were refined and ultimately accepted and promoted by the G8 as internationally recognized and have been in use for years.	Rather than develop new definitions we request that the SC27 either incorporate the existing IOCE/G8 definitions or contact the IOCE to possibly request modification of the existing definitions.	Duplicate - Addressed in IOCE 1.
UK 4	5	Digital Evidence Management	Ed	The note "The scope of this guideline is identification, collection and/or acquisition and preservation only." will need to be reviewed at next iteration once/if progress has been made with SC7 WG1A	None at this iteration : if discussions with SC7/WG1A on digital forensic governance project lead to a proposal for a new project on forensic readiness within an organization, ISO/IEC 27037 may be changed from single-part to multi-part standard, and this comment would need appropriate revision. Otherwise, some explanatory text on Forensic Readiness and confirmation that it is out of scope will be needed in	Noted - UK to propose new project separately.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					this section.	
UK 5	5		Ed	“Failure to do so may render it unusability”	Replace with: “Failure to do so may render it unusable”	Duplicate – Addressed in ZA 39.
UK 6	5.1		Ed	"...evidence could be located eg. Hard-disk": This sentence is missing some words. Also: “logical” may refer to the actual digital data, not just an address. This paragraph is too vague.	Rephrase	Accepted in principle – Rewording to be incorporated with US 22 and US 23. Section 5.1 is renumbered to 4.3.1.
UK 7	5.2		Te	Additional topics are needed.	Add: - acquisition of volatile data - acquisition of storage media, partitions, files and blobs under the condition of a running system - acquisition should be reliable and repeatable and well-documented	Accepted with modification - Adapt to fit structure of the section. Method needs to be reliable but not necessarily repeatable, focus more on the outcome. The method used need to be explained. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition. UK to provide content on ‘acquisition of storage media, partitions, files and blobs under the condition of a running system’.
UK 8	6.1		Te	Clarification is required over what the term Independent Digital Forensic Experts mean in the context of validation. Is this a person external to the organisation using the tool. If so this is not appropriate as there will be internal tools developed for computer examination which have been validated internally and demonstrated as fit for purpose.	Suggested change. “All tools used by the DEFR must have been validated prior to use. This validation can be carried out externally or internally but the evidence must be available upon any challenge of the technique.”	Accepted. Section 6 is renumbered and split into 4.1 and 4.2.
UK 9	6.4		Te	In the following sections it mentions that DEFR should demonstrate competency before carrying out an examination. However, there is no mention of ongoing competency assessment. How do we know someone is still competent 2-3 years down the line?	Suggest: “DEFR should undergo initial tests to ensure he/she is capable of performing the examination reliably. In addition the DEFR should be regularly reviewed to ensure ongoing competency.”	Accepted in principle – UK to propose content on initial test. Include an editor's note: NBs to comment on approaches for demonstrating and maintaining competency for both the DEFR and

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

						Digital Evidence Specialist. This may include certifications, qualifications, etc. Section 6.4 is renumbered to 4.1.4.
UK 9.1	8.1		Te	In the following sections it mention that DEFR should demonstrate competency before carrying out an examination. However, there is no mention of ongoing competency assessment. How do we know someone is still competent 2-3 years down the line?	Suggest: "DEFR should undergo initial tests to ensure he/she is capable of performing the examination reliably. In addition the DEFR should be regularly reviewed to ensure ongoing competency."	Duplicate – Addressed in UK 9.
UK 9.2	8.2		Te	In the following sections it mention that DEFR should demonstrate competency before carrying out an examination. However, there is no mention of ongoing competency assessment. How do we know someone is still competent 2-3 years down the line?	Suggest: "DEFR should undergo initial tests to ensure he/she is capable of performing the examination reliably. In addition the DEFR should be regularly reviewed to ensure ongoing competency."	Duplicate – Addressed in UK 9.
UK 10	6.2		Ge	The note in this section mentions that direct cost needs to be considered to carry out the standard (usually for civil matters) because in general the highest possible standards are also the most expensive. What actually needs to be considered is what quality level is required for the specific examination. Therefore costs should consider to be proportional to the quality level required and the evidence weight of potential evidence found.	Suggest." NB Direct costs need to be consider in relation to evidential significance of the potential data stored on the device and the required quality level of the examination"	Duplicate – Addressed in IOCE 3.
UK 11	6.3		Te	Repeatability is not always possible in the event of volatile data acquisition or when the evidence can only be extracted from the medium by means of destructive research (e.g. part replacement in HDDs)	Suggest stating "This section relates to hard disks but not volatile memory as it is not possible to get repeatable results due to the dynamic nature of the memory"	Accepted. Section 6.3 is renumbered to 4.1.2.
UK 12	8.3		Te	Could be expanded towards risk for digital evidence. Assessing the risk that evidence might be manipulated or systems under investigation might be booby-trapped may	Suggestion adding "Could data have been compromised" and "Consider of the device has been booby trapped to	Accepted with modification – Refer to logic bomb rather than booby trap.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				also be important to mention here.	destroy data if switched off or accessed in a uncontrolled way”	Section 8.3 is renumbered to 5.2.
UK 13	10.2		Te	Could be expanded to cover other aspects of the process.	Other things to consider - whether we want to capture the modus-operandi of a suspect during abuse of a system - whether we want the suspect to believe he is still undetected (covert)	Duplicate – Addressed in IOCE 20.
UK 14	10.3	b	Te	Using an atomic clock is a bit over kill for recording time especially when we know the issues of time/date information on computers.	Suggest: “Compare the time setting with a reference clock and document them and the differences. The reference clock should be checked and ensure it is within a required tolerance (e.g. to the same precision as an internet “Stratum 2” timebase)”	Rejected – Addressed in AU 38.2.
UK 15	11		Te	Capture of RAM and Volatile memory is still a relatively rare and complex examination. I would suggest that the relevance of capturing this type of data is assessed before attending the scene and if required taking appropriate expertise and tools. There will be certain cases where this type of examination is important (e.g. Suspect is known to be on link and use Encryption and Passwords), however in the majority of case this is not proportional to the investigation.	Suggest giving some examples of when RAM and memory needs to be examined and recommend this is consider before attending the scene so appropriate resource can be sourced.	Accepted in principle – UK to provide content. Section 11 is renumbered to 5.8.
UK 16	11		Te	Prioritise collection and/or acquisition of Order of Volatility . Might be worth adding some other examines	Add examples “Sat Navs, CCRV Systems, Automotive electronic, Improvised electronics (Bank Card Skimming)	Accepted. Section 11 is renumbered to 5.8.
UK 17	12.2.1		Te	Additional information should be inserted	Between a and b: consider logical acquisition when full-disk-encryption is suspected. First check if this may be the	Accept with modification – 'System clock' should be changed to 'reliable

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					case by looking at the raw disk or some crypto-detection utility. Also, make a photograph of the system (if present) clock next to a DCF-clock. Record time of each performed action. Same holds for 12.2.3	time source'. Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.
UK 18	12.2.1		Te	All of the points raised here are ideal and appropriate in some cases. It is recommended that the caterogised as Mandatory and Desirable	M = a, b, d, e, m, j (see comments on 16.1) D = f, h, l,	Accepted. Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.
UK 19	12.2.1, 12.2.2, 12.2.3		Te	The WD refers the method of sanitizing data in accordance with the US DoD 5220.22-M National Industrial Security Program Operating Manual. Although I admit that the manual developed by US DoS is excellent, it seems to be inappropriate to refer the specific document developed by one specific organization in the WD without reviewing in ISO. In addition, there may be other solution which are appropriate which do not fall into this criteria. The main fact is to be sure that the hard disk is clean before it is used.	Suggested "The image copy will be stored on a target disk which has been sanitized of any previous data. The sanitization process must have been validated to ensure that previous data remains. One possible solution is the follow the NISPOM requirements (US DoD 5220.22-M National Industrial Security Program Operating Manual)."	Duplicate – Addressed in IOCE 5.
UK 20	12.3	b	Te	Document states Hard Disk should be placed in Anti-static bags. This is an ideal situation and not critical if they are not due to the robust of technology now.	Suggestion "The DEFR should consider the sensitivity of the digital device to static electricity, if this is a concern then device should be secured in a anti-static bag".	Accepted in principle – incorporate with AU 65.1. Section 12.3 is incorporated into 5.7.
UK 21	12.3		Te	The WD mentions that collected digital devices should be stored in a secure, climate controlled environment or a location that is not subject to extreme temperature or humidity. It is difficult for some organizations to create climate controlled environment due to a lack of budget. Also digital devices these days are more robust to changing environments.	Suggest "Digital devices should be stored in a secure environment which is of a suitable climate which is not subjected to extreme temperature or humidity changes"	Duplicate – Addressed in US 59.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: SC 27 N7570

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

UK 22	13.1.1	g)	Te	The sweeping of WiFi devices is just as important as normal scenes involving standard alone computers as it is for Networked Computers.	Suggestion is to include this comment in section 12 as well.	Duplicate – Addressed in US 61.
UK 23	13.2		Te	Additional information should be inserted	Consider possibility of sabotage by suspect through active network connection. Monitor for this or decide to disconnect.	Duplicate – Addressed in US 63.
UK 24	13.2	g	Te	No mention of WiFi safety. It is important that the DEFR does not introduce WiFi devices into the scene which might change pairing information on potential evidential devices. This is particularly important if investigation needs to know what devices have been connected.	Include in Section 13 somewhere “It is important that the DEFR does not introduce WiFi devices into the scene which might change pairing information on potential evidential devices. This is particularly important if investigation needs to know what devices have been connected”	Accepted in principle – Include generalised content, similar to 13.1.1. g.
UK 25	14.1.1		Te	In this section it states a phone should be left in the same state it was received in but later on it states it should be switched off. The current recommendation in Europe is to switch the phone off as leaving it on can change data. There may be situation which are appropriate to leaving device on but these must be justified (e.g. Phone is known to come from a foreign country which will cause great problems in obtained the PUK if the phone is locked). Also switching off prevents the need for farabags.	Suggestion “The mobile phone should be switched off upon seizure to prevent data being changed from the receipt of communication and also in modern phone erase commands. If a phone is left on documented justification must be provided (e.g. Foreign Phone which would delay time critical examination in obtained PUK through INTERPOL).”	Duplicate – Addressed in IOCE 11.
UK 26	14.2		Te	"Some mobile devices have to be switched on to access the module, whilst other acquisitions can be done directly from the SIM card." Unclear what is meant by the second part of this sentence.	Clarify phraseology	Accepted – Incorporate with US 65.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

UK 27	14.2		Te	"There is also a wide range of memory devices that are used in conjunction with mobile devices, such as MicroDrives and SD cards." These generally have a standard interface, so they can be read with standard readers and write blockers. Be considerate though that removing a storage card from a handheld device that is switched on, this action might interfere with processes running in the background. For example, suppose a navigation application is running in the background on a smartphone. Make sure it is known what happens if the memory card containing card material is removed from the smartphone, before doing this on the actual evidentiary device.	Clarify phraseology	Accepted – Incorporate with US 65.
UK 28	14.2.1		Ge	"For a mobile device which is found to be on, DEFR should also use a faraday box"	Remove 'also'	Accepted.
UK 29	14.2.1	b)	Te	"If the device is continued to be left on ... to the lab for examination." It should be mentioned that GPS (factory-built into cars) enabled devices should not be moved unshielded because new location data might be gathered during transport.	Clarify phraseology	Duplicate – Addressed in US 66.
UK 30	14.2.1	c)	Te	"If the device is at appropriate intervals to ensure the data is not lost"	Clarify phraseology, including: - Preferable connection to a charger to the device continuously. - Making sure that a longer power cut is not left unnoticed.	Duplicate – Addressed in IOCE 25.
UK 31	14.2.2	b)	Te	"b) Also collect all associated mobile device items such as charger, memory card, SIM card, cradle and so on."	This should go to the general section because it also holds for 'switched on' devices.	Accepted.
UK 32	14.2.2	b)	Te	Additional steps	Also try to find original packaging of	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					mobile phones, these might contain notes with PIN and PUK codes	
UK 33	15.1		Ge	Also serial number should be noted, this might be useful to determine firmware versions. The manufacturer/distributor might have data on the device, accessible through serial number.	a) Rephrase as "The DEFR should document all other items at the scene that may contain potential evidences such as scribbled notes, sticky notes, diary and so on." b) This is general for all DE investigations, move to general part.	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.
UK 34	15.1		Te	Rephrase	"Next, the DEFR should identify the type, brand and model of the CCTV system"	Accepted – incorporate with UK 33.
UK 35	16.1		Ge	This section mentions the usage of a range of things for handling exhibits (e.g lint-free gloves in packaging a digital device, UV light shielding package area). This are ideally situation and in practise not achievable and appropriate for all cases. It is suggest that we indicate what is Mandatory and what is desirable	Indicate that the following are Mandatory : c, l, m, n (if volatile memory), p, q, r, s The rest are Desirable or appropriate in certain cases.	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
UK 36	Annex C	List of Validated Imaging Tools for Digital Evidence Acquisition		Table 3 provided no detail as to provenance of NIST validation process. Great care needs to be taken when producing a list of validated Imaging Tools. The main concern is that the user of the tools needs to be aware of the validation documentation and what the testing criteria where and any resulting limitaiton. Just stating a list of tools might mean first Responser might think all functions of a tools are o.k when the Validation only covered part of the functionality or highlight functionality not to be used. I would say this is significant of the mobile device software as we know that phone software can not get everything so user needs to be aware of limitations.	a) Add details before Table 3 of name of associated Federal Information Processing Standard (FIPS) or similar against which the validation is carried out b) Add note: "If the DEFR is to use the NIST validation as evidence that the tools are fit for purpose they must familiarise themselves with the validation documentation and ensure themselves that the test criteria and any recommendation are appropriate for there use"	Not applicable since annex is deleted – SE 45.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

US 01			GE	No mention is made about the possibility of doing a logical acquisition versus an image. There are many instances in which a logical acquisition is necessary and the document is not complete without discussion of it. Understanding of logical acquisitions is also important in ESI discovery.	There are many instances in which a logical acquisition is necessary and the document is not complete without discussion of it. Many "experts" are insisting that the only forensically sound evidence is a complete image of a "hard drive." Many times logical copies or portions of a hard drive are all that is available.	Accepted in principle – A reference to logical image will be included in the text, with an example where some drives are too big to image (e.g. SAN).
US 02	Introduction	Paragraph 2	Ed	The last sentence makes mention of "a certain certification criteria." However, nowhere else in the document is there any mention of certification.	Remove the last sentence of the second paragraph.	Accepted.
US 03	Introduction	Paragraph 3	Ed	This standard is unlikely to have any impact on cross-border jurisdictional issues or legal proceedings. Each jurisdiction typically has its own requirements for handling and using evidence.	Delete the third paragraph.	Accepted with modification – First sentence of the third paragraph will be deleted, and the remainder of the paragraph reworded. Reworded paragraph is incorporated with paragraph 2.
US 04	1.2		Ed	There is a wording problem with the 2 nd sentence.	Suggest changing to: "Not only will it assist organisations in their disciplinary procedures, it may also facilitate the exchange of potential digital evidence between jurisdictions."	Noted – Addressed in ZA 27.
US 05	3		GE	Many definitions already exist and have been generally accepted by the digital evidence communities. Some of your definitions contained in Section 3 conflict with many commonly accepted terms.	Recommend review and acceptance of terms already defined by recognized digital evidence bodies such as IOCE, SWGDE, SWGIT, etc.	Accepted in principle – US to provide content.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

US 06	3.1		GE	'Acquisition', derived from the word acquire, generally includes physical collection of items and not leaving the original items behind.	Modify definition of 'acquisition' to include collection and remove term collection.	Rejected – There need to be a distinction between collection and acquisition.
US 07	3.1		GE	An 'Acquisition' can be performed regardless of whether the original physical items are left behind or not – its up to each jurisdiction and its legal requirements as to whether original items will be collected or not.	Remove requirement of 'leaving the original evidence' after copying or imaging	Accepted.
US 08	3.1		Ge	The process of copying the image at the scene is also referred to as Retrieval.	Add Retrieval to this definition.	Accepted with modification – Include a note that the copy is retrieved and stored securely.
US 09	3.3		TE	Definition of 'blob' already exists and it should not be redefined. Additionally, a blob of digital information does NOT have to be specific to multimedia files	Use existing definition of blob and site reference, or remove completely	Accepted to remove – see AU 6.
US 10	3.5		GE	Definition of 'digital evidence' has been defined by the IOCE and accepted by the participating international parties as well as the G8. Do not redefine and site reference to IOCE	Use existing definition and site reference. IOCE's definitions can be found at the bottom of the page at: http://ioce.org/core.php?ID=5	Duplicate - Addressed in IOCE 1.
US 11	3.8		GE	Definition of 'hash code' already exists – either use existing definition or at least expand the current definition so that it is more understandable of what a hash code really is.	Use existing definition or make wording more accurate and understandable. The combined SWGDE/SWGIT glossary can be found at: http://swgde.org/documents/swgde2009/SWGDE_SWGITGlossaryV2.3.pdf	Duplicate – Addressed in AU 8.2.
US 12	3.9		GE	Definition of 'hash-function' already exists – either use existing definition or at least expand the current definition so that it is more understandable of what a hash code really is.	Use existing definition or make wording more accurate and understandable. The combined SWGDE/SWGIT glossary can be found at: http://swgde.org/documents/swgde2009/SWGDE_SWGITGlossaryV2.3.pdf	Accepted to use existing definition – 'function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - it is computationally infeasible to find for a given output, an input which maps to

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

						this output. - it is computationally infeasible to find for a given input, a second input which maps to the same output. NOTE - Computational feasibility depends on the specific security requirements and environment' [ISO/IEC 10118-1:2000].
US 13	3.17		TE	Often changes to digital evidence are unavoidable and must be performed for various reasons, but this does not 'spoil' the evidence. A note should be included here so that the reader understands that not all changes made to evidence cause 'spoilage' even if unintended.	Add note of caution.	Accepted in principle – US to provide content and incorporated with AU 10.2.
US 14	3.17		Ed	Spoilage can occur independent off accidental or intentional changes. The term "spoliation" is used in US law.	Suggest removing the word "accidental"	Duplicate – Addressed in AU 10.2.
US 15	3.18		Ed	The term "tampering" is not used by itself (i.e., it is always paired with "spoilage"). Further, it is not used consistently because the word "damage" is used frequently.	Suggest deleting the definition as well as removing it throughout the document.	Accepted – The terms need to be used consistently throughout the document. The term 'damage' is replaced with 'tampering' where appropriate in context. Rejected – The definition will not be deleted. 3.18 is renumbered to 2.19.
US 16	3.19		Te	Definition of timestamp is all wrong. If you look at the ANSI/ISO definition this would comprise a time mark. We need to get nomenclature straight.	Use ANSI/ISO definition and be clear that of distinction between a time mark (unencrypted); time stamp (encrypted but not trusted) and trusted (source of time is both trusted and protected, and output is encrypted and not under control of others.) Check the ANSI definition.	Accepted in principle – Replace with: 'time variant parameter which denotes a point in time with respect to a common time reference' (ISO/IEC 11770-1:1996). 3.19 is renumbered to 2.20.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

US 17	3.20		TE	All volatile data is not necessarily diminished in its evidential value, or 'spoiled' as per your definition, by doing things such as switching the power off to a system. Spoilage is possible but not definite in every situation.	Reword to the affect of 'data that is easily modified, possibly causing spoilage, for example....' Please use term spoliation. Spoilage is for legumes and fruits.	Accepted in principle - Modify to fit directives. 3.20 is renumbered to 2.22.
US 18	4		Ed	BIOS is listed as a definition.	Suggest changing to: BIOS basic input/output system	Accepted.
US 19	5		ED	Spelling problem. "Failure to do so may render it unusability ... "	Should be: unusable "Failure to do so may render it unusable ... "	Duplicate – Addressed in ZA 39.
US 20	5	2nd paragraph	Ed	The word "reliability" is used, but it is unclear what is meant.	Suggest adding a definition for reliability or consider an alternate word like "authenticity". Be careful with the use of authenticity, as it has a very narrow legal definition.	Accepted – 'property of consistent intended behaviour and results' [ISO/IEC FDIS 27000]. Included as 2.14.
US 21	5	2nd paragraph	Te	Presentation is out of scope for this standard.	Suggest deleting "presentation" from last sentence as well as the note.	Accepted – Noted in JP 15 resolution as well.
US 22	5.1		TE	"...evidence could be located eg. Hard-disk": This sentence is missing some words.	Modify first paragraph, second sentence to say '...evidence could be located on a physical device, such as a hard disk'.	Accepted in principle – incorporate with AU 16. Section 5.1 is renumbered to 4.3.1.
US 23	5.1		TE	'logical' refers to an address or location where potential evidence can be located ON a physical device such as a hard disk. Also: logical may refer to the actual digital data, not just an address. This paragraph is too vague.	Suggest rewriting the paragraph.	Accepted in principle – incorporate with AU 16. Section 5.1 is renumbered to 4.3.1.
US 24	5.2		GE	Often a situation exists where only a logical acquisition of data can be obtained.	The method of performing a logical acquisition should added – this can be on both a file and partition level.	Accepted. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition..

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

US 25	5.2		TE	No mention is made on: - acquisition of volatile data - acquisition of storage media, partitions, files and blobs under the condition of a running system - acquisition should be reliable and repeatable and well-documented	Consider adding: - acquisition of volatile data - acquisition of storage media, partitions, files and blobs under the condition of a running system - acquisition should be reliable and repeatable and well-documented	Duplicate – Addressed in UK 7.
US 26	5.3	1st paragraph	Te	The phrase “and to be deemed admissible” is not relevant to investigating incidents; it is a matter associated with having potential evidence being admitted into a court (or similar) proceeding.	Suggest removing the phrase because admissibility is not mentioned elsewhere in the document.	Accepted. Section 5.3 is renumbered to 4.3.4.
US 27	5.4		Te	It is probably worth noting that DEFRs are frequently not the people who perform the forensic analysis of the digital evidence.	Suggest including a note:	Not applicable since section is deleted – JP 15.
US 28	5.5		Te	Presentation is out of scope for this standard.	Suggest deleting this section.	Not applicable since section is deleted – JP 15.
US 29	5, 6 (and possibly others)		GE	Use of terms ‘scientifically proven’ or scientifically derived’ etc – these terms are very vague and undefined and is not obvious how you intended them – you should define them as you intend them to be meant. Additionally there are times when no ‘scientifically proven’ or ‘derived’ methods exist and an examiner must use his knowledge and skills to invent a new process etc.	Add definitions for these terms and limit their use where appropriate – not all methods used will meet this requirement	Accepted in principle – US to provide content.
US 30	6.1		GE	It is unknown what is meant by a method being ‘transparent’	Replace word ‘transparent’ with what is meant by the term. Consider the word “validated.”	Accepted with modification - Validated is not the same as transparent. New text will be included to clarify the meaning of transparency. Section 6.1 is renumbered to 5.2.1.
US 31	6.1		GE	Objection to third paragraph, item b) – the forum for which	Remove item b)	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				the data is intended should not impact the method chosen - this will minimize bias. The method chosen should be regardless of forum.		Section 6.1 is renumbered to 5.2.1.
US 32	6.1		Te	Having methods tested by independent digital forensic experts is very unclear. Recommend clarifying this sentence by stating that the methods must be accepted by the forensic discipline. Is this an person external to the organisation using the tool. If so this is not appropriate as there will be internal tools developed for computer examination which have been validated internally and demonstrated as fit for purpose.	Suggested change. "All tools used by the DEFR must have been validated prior to use. This validation can be carried out externally or internally but the evidence must be available upon any challenge of the technique." Also, consider adding: "Methods must be acceptable by then current best forensic practices."	Accepted with modification – Incorporate with IOCE 2 and UK 8. Section 6.1 is renumbered to 5.2.1.
US 33	6.2		GE	It is unknown what is mean by 'evidential standard' – throughout the document you use the terms 'method' or 'procedure' or 'technique' instead	Replace 'evidential standard' with 'methods, techniques, and/or procedures'	Accepted. Section 6.2 is renumbered to 4.1.1..
US 34	6.2		GE	The note in this section mentions that direct cost needs to be considered to carry out the standard (usually for civil matters) because in general the highest possible standards are also the most expensive. What actually needs to be considered is what quality level is required for the specific examination. Therefore costs should consider to be proportional to the quality level required and the evidence weight of potential evidence found.	Suggest new bullet." Direct costs need to be consider in relation to evidential significance of the potential data stored on the device and the required quality level of the examination"	Duplicate – Addressed in IOCE 3.
US 35	6.3		GE	Suggest creating a new section for "reproducible", which consists of the same elements as repeatability, minus items b) and d).	Add the proposed section.	Accepted in principle – US to provide content to incorporate into existing section. Section 6.3 is renumbered to 4.1.2.
US 36	6.3		GE	Repeatability should be independent of period of time – it is not clear why this requirement was in place	Remove item e)	Rejected – Addressed in AU 27.
US 37	6.3		TE	Repeatability is not always possible in the event of	Suggest stating "This section relates to	Duplicate – Addressed in UK 11.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				volatile data acquisition or when the evidence can only be extracted from the medium by means of destructive research (e.g. part replacement in HDDs)	hard disks but not volatile memory as it is not possible to get repeatable results due to the dynamic nature of the memory”	
US 38	6.4		GE	Defensibility of a DEFR’s actions and methods have little to do with Chain of Custody – having a well documented Chain of Custody does NOT imply that a DEFR’s techniques are defensible.	The reference to Chain of Custody should be removed, or at a minimum it should not be implied that having a well documented Chain of Custody will ensure defensibility.	Accepted – The reference will be removed. Section 6.4 is renumbered to 4.1.4.
US 39	6.4		TE	In the following sections it mentions that DEFR should demonstrate competency before carrying out an examination. However, there is no mention of ongoing competency assessment. How do we know someone is still competent 2-3 years down the line?	Suggested Changes “DEFR should undergo initial tests to ensure he/she is capable of performing the examination reliably. In addition the DEFR should be regularly reviewed to ensure ongoing competency.”	Duplicate – Addressed in UK 9.
US 39.1	8.1		TE	In the following sections it mentions that DEFR should demonstrate competency before carrying out an examination. However, there is no mention of ongoing competency assessment. How do we know someone is still competent 2-3 years down the line?	Suggested Changes “DEFR should undergo initial tests to ensure he/she is capable of performing the examination reliably. In addition the DEFR should be regularly reviewed to ensure ongoing competency.”	Duplicate – Addressed in UK 9.
US 39.2	8.2		TE	In the following sections it mentions that DEFR should demonstrate competency before carrying out an examination. However, there is no mention of ongoing competency assessment. How do we know someone is still competent 2-3 years down the line?	Suggested Changes “DEFR should undergo initial tests to ensure he/she is capable of performing the examination reliably. In addition the DEFR should be regularly reviewed to ensure ongoing competency.”	Duplicate – Addressed in UK 9.
US 40	8.1	Note	Ed	There are multiple problems with the wording in the note: “Note: Competence of a DEFR varies from from one jurisdiction to another. However, it is utmost important for a DEFR to undergo a competency test or similar to	Suggest changing to: “Note: Competence of a DEFR may vary from one jurisdiction to another. However, it is of utmost importance for	Accepted. Section 8.1 is renumbered to 5.3.1.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: SC 27 N7570

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				ensure he/she is capable to deliver his/her tasks without tampering or spoiling the data that has the potential evidentiary value.”	a DEFR to undergo a competency test or similar to provide a measure of assurance that the DEFR is capable of performing the necessary tasks without tampering or spoiling the data, which may be of evidentiary value.”	
US 41	8.1		Te	This section describes the importance of integrity, which is typically associated with preventing or detecting data corruption. However, there is no mention of authenticity, which could have a major impact on the admissibility of the evidence.	Suggest changing to: “However, the role of DEFR is vital in ensuring the integrity and authenticity of potential digital evidence.”	Accepted. Section 8.1 is renumbered to 5.3.1.
US 42	8.3		TE	Could be expanded towards risk for digital evidence. Assessing the risk that evidence might be manipulated or systems under investigation might be booby-trapped may also be important to mention here.	Suggestion adding “Could data have been compromised” and “Consider of the device has been booby trapped to destroy data if switched off or accessed in a uncontrolled way”	Duplicate – Addressed in UK 12.
US 43	10.2		TE	Other things to consider - whether we want to capture the modus-operandi of a suspect during abuse of a system - whether we want the suspect to believe he is still undetected (covert)	Suggest adding bullets for these items.	Duplicate – Addressed in IOCE 20.
US 44	10.3	b)	Te	Sensitivity to time does not imbue evidence with integrity. Neither does an atomic clock, whatever that is. Documenting time differential between system clock and atomic clock as a reliable indicator?	Sensitivity to time is a nonsense term. The objective is accuracy; i.e., a trusted source of time, and protected output that can be robustly associated with a data generating event.	Rejected – Addressed in AU 38.2.
US 45	10.3	b)	TE	Just because a system is on does not imply that it would be safe to gather the date and time of the system. There exist systems that require much user interaction in order to get the date/time info. Caution should be added to	Modify item b) to add caution regarding possible modification to the system that might occur, depending on the system, to retrieve the data and time and that only properly trained personnel should	Accepted in principle – Incorporate with AU 38.2. Section 10.3 is renumbered to 5.3.3.3.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				item b) in regards to getting the date/time info	do so.	
US 46	11		TE	Capture of RAM and Volatile memory is still a relatively rare and complex examination. Suggest that the relevance of capturing this type of data is assessed before attending the scene and if required taking appropriate expertise and tools. There will be certain cases where this type of examination is important (e.g. Suspect is known to be on link and use Encryption and Passwords), however in the majority of case this is not proportional to the investigation.	Suggest giving some examples of when RAM and memory needs to be examined and recommend this is consider before attending the scene so appropriate resource can be sourced.	Duplicate – Addressed in UK 15.
US 47	11		TE	Prioritise collection and/or acquisition of Order of Volatility. Might be worth adding some other examines	Add examples “Sat Navs, CCRV Systems, Automotive electronic, Improvised electronics (Bank Card Skimming)	Duplicate – Addressed in UK 16.
US 48	12.2.1 12.2.2 12.2.3		TE	The WD refers the method of sanitizing data in accordance with the US DoD 5220.22-M National Industrial Security Program Operating Manual. Although I admit that the manual developed by US DoS is excellent, it seems to be inappropriate to refer the specific document developed by one specific organization in the WD without reviewing in ISO. In addition, there may be other solution which are appropriate which do not fall into this criteria. The main fact is to be sure that the hard disk is clean before it is used.	Suggested “The image copy will be stored on a target disk which has been sanitized of any previous data. The sanitization process must have been validated to ensure that previous data remains. One possible solution is the follow the NISPOM requirements.”	Duplicate – addressed in IOCE 5.
US 49	12.2.1		TE	All of the points raised here are ideal and appropriate in some cases. It is recommended that the categorized as Mandatory and Desirable	M = a, b, d, e, m, j (see previous comment) D = f, h, l,	Duplicate – Addressed in UK 18.
US 50	12.2.1		TE	Between a and b: consider logical acquisition when full-disk-encryption is suspected. First check if this may be the case by looking at the raw disk or some crypto-detection utility.	Add the suggested bullets between a) and b) * checking for encryption	Duplicate – Addressed in UK 17.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				Also, make a photograph of the system (if present) clock next to a DCF-clock. Record time of each performed action. Same holds for 12.2.3	* taking photograph	
US 51	12.2.1	b)	TE	With some of the more advanced operating systems that exist today pulling the power supply is often a more damaging action then shutting the system down appropriately and explaining any changes that take affect. The need for a senior level, highly training DEFR is required who can understand the impact of choosing between either pulling the plug or shutting down gracefully. Having step b) is dangerous without knowing the consequences. It can also be damaging to some peripheral devices such as RAID storage etc.	Change item b) so that the DEFR understands that a decision must be made as to which option to choose and must be based on variables such as hardware type, operating system, etc.	Accepted with modification - The order of the steps depends on the situation. The DEFR may need to get advice from a specialist. Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.
US 52	12.2.1	i)	TE	Objection to removal of the hard drive in general as not being necessary. First, often leaving the hard drive mounted inside of the computer allows for the best mode of packaging the evidence. Second, some imaging tools utilize a bootable device which uses the suspect computer system with the hard drive mounted to acquire an image copy. Lastly, if multiple drives are installed as a RAID internal in the suspect computer – improper removal could hamper future acquisition of the RAID.	Remove item i).	Rejected – addressed in FIRST 45 and AU 56.1.
US 53	12.2.1	j)	TE	The imaging process should be moved up after item e). Sometimes the floppy drive is needed during the acquisition process so item j) should be before placing tape over the floppy drive, and sometimes the suspect computer system is utilized to perform the acquisition so tape should not yet be placed over the power supply.	Move item j) after item e)	Accepted. Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.
US 54	12.2.1	j)		Nothing is mentioned about multiple hard drives that are set up in the suspect computer as a RAID – nothing about identification of it, acquisition of it, special considerations about it etc.	Either make RAID a limitation to the document and add the limitation to the Scope section, or new requirements must be added to may sections to	Accepted – Include guidelines on how to handle RAID. Include an editor's note: NBs to comment on guidelines on how to

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					handle RAID setups.	handle RAID. Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.
US 55	12.2.2	f)	TE	Objection to removal of the hard drive in general as not being necessary. First, often leaving the hard drive mounted inside of the computer allows for the best mode of packaging the evidence. Second, some imaging tools utilize a bootable device which uses the suspect computer system with the hard drive mounted to acquire an image copy. Lastly, if multiple drives are installed as a RAID internal in the suspect computer – improper removal could hamper future acquisition of the RAID.	Remove item f).	Duplicate – Addressed in SE 18.
US 56	12.2.2	g)	TE	The imaging process should be moved up after item b). Sometimes the floppy drive is needed during the acquisition process so item j) should be before placing tape over the floppy drive, and sometimes the suspect computer system is utilized to perform the acquisition so tape should not yet be placed over the power supply.	Move item g) after item b)	Accepted. Section 12.2.2 is renumbered and split into 6.1.2.2 and 6.1.3.2.
US 57	12.2.2	g)		Nothing is mentioned about multiple hard drives that are set up in the suspect computer as a RAID – nothing about identification of it, acquisition of it, special considerations about it etc.	Either make RAID a limitation to the document and add the limitation to the Scope section, or new requirements must be added to may sections to handle RAID setups.	Duplicate – Addressed in US 54.
US 58	12.3		Te	Digital signatures are fine, but it appears that there is no requirement for trusted time to be associated with the evidence in a cryptographically assured manner.	There may be no requirement for this at the moment, but attorneys (including myself) are succeeding in mounting challenges to digital evidence where an untrusted time value is grafted onto a data blob. This is also a repeatable challenge tool for attorneys. Recommend that robust association of a trusted time value with digital	Accepted in principle – US to provide content. Section 12.3 is incorporated into 5.7.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					evidence, at time relevance is asserted (think instantiation).	
US 58.1	13.3		Te	Digital signatures are fine, but it appears that there is no requirement for trusted time to be associated with the evidence in a cryptographically assured manner.	There may be no requirement for this at the moment, but attorneys (including myself) are succeeding in mounting challenges to digital evidence where an untrusted time value is grafted onto a data blob. This is also a repeatable challenge tool for attorneys. Recommend that robust association of a trusted time value with digital evidence, at time relevance is asserted (think instantiation).	Duplicate – Addressed in US 58.
US 59	12.3		TE	The WD mentions that collected digital devices should be stored in a secure, climate controlled environment or a location that is not subject to extreme temperature or humidity. It is difficult for some organizations to create climate controlled environment due to a lack of budget. Also digital devices these days are more robust to changing environments.	Suggest “Digital devices should be stored in a secure environment which is of a suitable climate which is not subjected to extreme temperature or humidity changes”	Accepted – Incorporate with SE 23. Section 12.3 is incorporated into 5.7.
US 60	12.3	b	TE	Document states Hard Disk should be placed in Anti-static bags. This is an ideal situation and not critical if they are not due to the robust of technology now.	Suggestion “The DEFR should consider the sensitivity of the digital device to static electricity, if this is a concern then device should be secured in a anti-static bag”.	Duplicate – Addressed in UK 20.
US 61	13.1.1	g)	TE	The sweeping of WiFi devices is just as important are normal scenes involving standard alone computers as it is for Networked Computers.	Suggestion is to include this comment in section 12 as well.	Accepted.
US 62	13.2		TE	Consider possibility of sabotage by suspect through active network connection. Monitor for this or decide to disconnect.	Suggestion is to include this comment in section 13.2	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

US 63	13.2	g	TE	No mention of WiFi safety. It is important that the DEFR does not introduce WiFi devices into the scene which might change pairing information on potential evidential devices. This is particularly important if investigation needs to know what devices have been connected.	Include in Section 13 somewhere "It is important that the DEFR does not introduce WiFi devices into the scene which might change pairing information on potential evidential devices. This is particularly important if investigation needs to know what devices have been connected"	Duplicate – Addressed in UK 24.
US 64	14.1.1		TE	In this section it states a phone should be left in the same state it was received in but later on it states it should be switched off. The current recommendation in Europe is to switch the phone off as leaving it on can change data. There may be situation which are appropriate to leaving device on but these must be justified (e.g. Phone is known to come from a foreign country which will cause great problems in obtained the PUK if the phone is locked). Also switching off prevents the need for farabags.	Suggestion "The mobile phone should be switched off upon seizure to prevent data being changed from the receipt of communication and also in modern phone erase commands. If a phone is left on documented justification must be provided (e.g. Foreign Phone which would delay time critical examination in obtained PUK through INTERPOL)."	Duplicate – Addressed in IOCE 11.
US 65	14.2		TE	"Some mobile devices have to be switched on to access the module, whilst other acquisitions can be done directly from the SIM card." Unclear what is meant by the second part of this sentence. "There is also a wide range of memory devices that are used in conjunction with mobile devices, such as MicroDrives and SD cards." These generally have a standard interface, so they can be read with standard readers and write blockers. Be considerate though that removing a storage card from a handheld device that is switched on, this action might interfere with processes running in the background. For example, suppose a navigation application is running in	Suggest clarifying the unclear sentence. Also suggest incorporate language about the use of write blockers.	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				the background on a smartphone. Make sure it is known what happens if the memory card containing card material is removed from the smartphone, before doing this on the actual evidentiary device.		
US 66	14.2.1		GE	"a) For a mobile device which is found to be on, DEFR should also use a faraday box" "b) If the device is continued to be left on ... to the lab for examination." "c) If the device is at appropriate intervals to ensure the data is not lost"	For a): remove 'also' For b): It should be mentioned that GPS (factory-built into cars) enabled devices should not be moved unshielded because new location data might be gathered during transport. For c): It should be mentioned that preferably connect a charger to the device continuously. Make sure that a longer power cut is not left unnoticed.	Accepted.
US 67	14.2.2	b)	TE	"b) Also collect all associated mobile device items such as charger, memory card, SIM card, cradle and so on."	- This should go to the general section because it also holds for 'switched on' devices. - also try to find original packaging of mobile phones, these might contain notes with PIN and PUK codes	Duplicate – Addressed in UK 34.
US 68	15		Ge	Recommend including embedded Digital Video Recorder (DVR) in this sentenced.	DEFR must understand that the approach to extract video sequences from a PC based or embedded DVR CCTV system is different from conventional digital data extraction from a PC.	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.
US 69	15.1		TE	Some suggested changes to be made and also moving section to general area as common to all types of devices.	"Next, the DEFR should identify the type, brand and model of the CCTV system" Also serial number should be noted, this might be useful to determine firmware	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					versions. The manufacturer/distributor might have data on the device, accessible through serial number. "The DEFR should document all other items at the scene that may contain potential evidences such as scribbled notes, sticky notes, diary and so on." This is general for all DE investigations, move to general part.	
US 70	15.1 c		Ge	Recommend adding actively recording cameras	Note the number of cameras connected to the CCTV system and the cameras that are actively recording.	Accepted – incorporate with UK 33.
US 71	15.1 e		Ge	Recommend adding a caution to not change any settings while reviewing the basic settings. If the time is not correct it should be left uncorrected or the system will not be able to find the video files.	Add wording: "Be careful not to change any settings while reviewing the system and the hard drive space."	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.
US 72	15.2 a		Te	Add a comment to have the DEFR review the video to determine if the incident was even recorded.	"a) The storage size and the overwrite time should also be noted. This will let the DEFR know how long the video sequences will be retained on the system.	Not applicable since section has been deleted – AU 76.
US 73	15.2 b		Te	Recommend moving point a to point b and add that all camera recordings should be acquired during the time of interest.	b) Before the collection and/or acquisition process can be started, the DEFR should determine the time period required. He/she should acquire all camera recordings during the time of interest.	Not applicable since section has been deleted – AU 76.
US 74	15.2 d		Te	Recommend adding to check to ensure there is actually video of the incident recorded.	d) One of the most important steps is the confirmation that the video sequences actually exists and were	Not applicable since section has been deleted – AU 76.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					recorded of the incident.	
US 75	15.2 f		Ge	Recommend changing wording: to may not be practical	f) The practicality of acquisition must be checked. The general principle is to consider using the least intrusive method, but this needs to be balanced with circumstances of cost and time. Also long sequences of video from multiple cameras may require a very large storage size which may not be practical. The acquisition process may also take several hours to complete.	Not applicable since section has been deleted – AU 76.
US 76	15.2 g		Te	Recommend changing wording in the third bullet.	-Acquire the video files via a network connection. This may be available if the CCTV system is a PC based system or an embedded DVR based system may also have a network port.	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.
US 77	15.2 g		Te	Recommend changing wording in the fourth bullet by adding a note explaining that the hard disk may not play because it requires the systems hardware for playback.	-A quick method is by replacing the CCTV system's hard disk with a blank or cloned hard disk. However, there are several risks that the DEFR should assess before using this method such as compatibility of the new hard disk with the system and the compatibility of the removed hard disk with other systems for examination. Note: the hard disk may require the system's hardware for playback.	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.
US 78	15.2 h		Te	The files should be check for playability on another system to ensure it will play.	h) Upon completing the acquisition, the acquired file should be check to confirm that the right file or the right portion of the file has been acquired. The file should also be checked with the player	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					software (for proprietary file formats) for its playability on another system.	
US 79	15.2 i		Te	Information is written to media not just a drive.	i) The media which contains the acquired file should be treated as the master copy.	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.
US 80	15.2 j		Te	The system should be verified that it is working again.	j) Subsequently, DEFR should restart the CCTV system if it was powered off. This should be done in the presence of the authorized person on the premise and verified that the system is working again.	Accepted – Detailed section on CCTV will be removed and the relevant sections move to appropriate corresponding sections on network devices.
US 81	15.3 a		Te	Hashing is only necessary when an examination is conducted on the data. It is not necessary for only preservation. Digital signatures, seals, and Biometrics are not necessary.	Using hashing algorithm on data that will be used for the examination.	Not applicable since section has been deleted – AU 76.
US 82	15.3 d		Ge	Ball point ink pens can damage disc. Suggest a felt tipped permanent marker.	d) The DEFR should label the collected items using a felt tipped permanent marker.	Superseded by SE 27.
US 83	16.1		GE	This section mentions the usage of a range of things for handling exhibits .(e.g lint-free gloves in packaging a digital device, UV light shielding package area). This are ideally situation and in practise not achievable and appropriate for all cases. It is suggest that we indicate what is Mandatory and what is desirable	Indicate that the following are Mandatory : c, l, m, n (if volatile memory), p, q, r, s The rest are Desirable or appropriate in certain cases.	Duplicate – Addressed in UK 35.
US 84	Annex C		GE	The NIST Computer Forensic Tool Testing Project, of which SWGDE members participate, does NOT validate software for any organization's requirements. Whether a tool is considered valid for one agency's technique, policy or procedure is dependent on that agency's requirements.	This Annex should be removed.	Duplicate – Addressed in SE 45.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				NIST does not test against every agency's requirements, but instead tests to confirm or verify that a tool works as stated by the vendor. This type of testing is NOT validation testing, but rather a form of verification testing. Additionally, this list is a constantly changing list and therefore would immediately outdate any one version of this document at any point in time. And finally, as your column headings attest, the title of the annex refers to Imaging Tools yet not all tools listed are imaging tools and not all perform acquisition.		
--	--	--	--	---	--	--

ZA 1	All	All	Ge	Consistent capitalisation throughout the document: digital evidence first responders	Change to: Digital Evidence First Responders	Accepted.
ZA 2	All	All	Ge	The general sentence length employed in the document is rather excessive, making the standard difficult to read.	Make sentences shorter and to the point. Rather start a new sentence instead of leaving a very long sentence to trail off into obscurity.	Accepted.
ZA 3	All	All	Ed	Inconsistent alignment of paragraphs. Some are left aligned, while most are justified.	Alignment of paragraphs must be justified. Use the ISO/IEC standard template to ensure that styles are correct.	Accepted.
ZA 4	All	All	Te	The document shall be referred to as an International Standard. (Directives part 2, clause 6.6.7.2)	Replace all occurrences of "this standard" with "this International Standard" (note the capital letters)	Accepted.
ZA 5	All	All	Te	Hanging paragraphs shall be avoided since reference to them is ambiguous. (Directives part 2, clause 5.2.4)	Introduce the necessary clause heading to remove hanging paragraphs.	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

ZA 6	All	All	Te	NOTES are incorrectly drafted.	Adhere to clause 6.5.1 of the ISO/IEC directives part 2. Use the ISO/IEC standard template to ensure that styles are correct.	Accepted.
ZA 7	All	All	Te	Inconsistent and often incorrect drafting of lists.	Adhere to clause 5.2.5 of part 2 of the directives.	Accepted.
ZA 8	Introduction	Paragraph 1	Ed	Spelling mistake: admissability	Change to: admissibility	Duplicate - Addressed in FIRST 2.
ZA 9	Introduction	Paragraph 1	Te	Sentence reads difficult: "The process of the investigation emphasizes the integrity of the digital evidence and the right procedure in obtaining the digital evidence to ensure its admissability in meeting its purposes."	Change to: "The investigation process is designed to maintain the integrity of the digital evidence – the correct procedure in obtaining digital evidence will ensure its admissability in meeting its purposes."	Accepted with modification – This sentence will be incorporated with FIRST 1 to read as ' The investigation process is designed to maintain the integrity of the digital evidence – the legally acceptable methodology in obtaining digital evidence will ensure its admissability in meeting its purposes.'
ZA 10	Introduction	Paragraph 2	Ed	Change 'give' to 'provide' – more formal. "Key components that give credibility..." change to "Key components that provide credibility..."	"Key components that give credibility..." change to "Key components that provide credibility..."	Accepted.
ZA 11	Introduction	Paragraph 2	Ed	Grammatically incorrect	... a proper procedure needs to be carried out with due care to ensure that the integrity of evidentiary...	Accepted.
ZA 12	Introduction	Paragraph 2	Ed	Grammatically incorrect	... is the methodology applied ...	Accepted.
ZA 13	Introduction	Paragraph 3	Ed	Sentence structure can be improved: "It becomes a great concern to many when incidents occured involved cross-border jurisdictions."	Change to: "It becomes a great concern to many when incidents involving cross-border jurisdictions occur."	Not applicable since sentence is deleted – US 3.
ZA 14	Introduction	Paragraph 3	Ed	Sentence structure can be improved: "This has prompted for this International Standard to be developed to be used not only for legal proceedings, but also for disciplinary	Change to: "In order to address this concern, the International Standard is being developed. It is intended not only	Accept with modification – This suggested text will be incorporated into the newly reworded paragraph referred

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<i>procedures and other related purposes in handling digital evidence.”</i>	<i>for legal proceedings, but also for disciplinary procedures and other related actions in handling digital evidence.”</i>	to in US 3.
ZA 15	Introduction	Paragraph 4	Ed	Grammatically incorrect	This International Standard provides guidance for individuals and Digital Evidence First Responders who perform required tasks in the investigation including identifying, collecting and/or acquiring and preserving of digital evidence. This International Standard is relevant to ensure that digital evidence is managed in accordance with acceptable and practical ways that are acceptable worldwide with the objective to preserve its integrity.	Accepted.
ZA 16	Introduction	Paragraph 5	Ed	Digital Evidence First Responder should be plural in this sentence structure.	Change to: Digital Evidence First Responders	Accepted.
ZA 17	Introduction	Paragraph 6	Ed	Order of words incorrect: <i>“It does not also include matters...”</i>	Change to: <i>“It also does not include matters...”</i>	Accepted.
ZA 18	Introduction	Paragraph 7	Te	This is not a proposed standard.	Replace “This proposed standard” with “This International Standard”	Accepted.
ZA 19	1	Paragraph 1	Ed	Grammatically incorrect	... provides guidance on digital evidence management, describing ...	Not applicable since sentence is changed – AU 1D.
ZA 20	1	Paragraph 2	Te	Logical order of events: first list real time, and then after the incident.	Change to: <i>“It is applicable to organisations needing to conduct the identification, collection and/or acquisition and preservation of digital</i>	Not applicable since sentence is deleted – AU 2.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					<i>evidence in the event of computer incidents, while the incidents happen in real time or after the incidents happened."</i>	
ZA 21	1	Paragraph 5	Te	This paragraph states that "The application of this International Standard is possible in principle..." This is a strange thing to say. The reason for it is unclear, since guidelines in an International Standard should be possible in practice. Also, the statement that special consideration is paid to identifying the competence needed by a DEFR is rather vague.	Remove this paragraph.	Accepted.
ZA 22	1	Paragraph 5	Te	The scope is not the place for explaining the document structure. If at all necessary, move it to another clause. However, such a description of the structure of the document does not add value to the document as a whole.	Remove par. 5 and all the bullets.	Accepted.
ZA 23	1	Paragraph 5 bullets	Ed	Consistent punctuation	End all bullets with █	Not applicable since sentence is deleted – ZA 22.
ZA 24	1.1		Te	Add more description for better understanding.	Change the last sentence to: <i>"This standard deals with common situations encountered throughout the whole digital management process."</i>	Accepted with modification - Content of ZA 25, ZA 27 and AU 5.1 are combined and incorporated in existing clause 1. These comments and suggested rewording will be addressed in the new text.
ZA 25	1.2	All	Te	The "objective" fits in with "scope", i.e. the content currently in the hanging paragraphs in clause 1.	Combine the contents of this clause with the content currently in the hanging paragraphs in clause 1 under a clause 1.1 Overview.	Accepted with modification - Content of ZA 25, ZA 27 and AU 5.1 are combined and incorporated in existing clause 1. These comments and suggested rewording will be addressed in the new text.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

ZA 26	1.2.		Ed	Spelling mistake: colleccting	Change to: collecting	Accepted.
ZA 27	1.2		Te	Sentence structure can be improved: <i>“Not only it will assist organisations in their disciplinary procedures, it will also facilitate the exchange of potential digital evidence between jurisdictions.”</i>	Change to: <i>“It aims to assist organisations in their disciplinary procedures, as well as to facilitate the exchange of potential digital evidence between jurisdictions.”</i>	Accepted with modification - Content of ZA 25, ZA 27 and AU 5.1 are combined and incorporated in existing clause 1. These comments and suggested rewording will be addressed in the new text.
ZA 28	3	Par. 1	Ed	Punctuation (full stop needed)	Replace “definitions apply:” with “definitions apply.”	Accepted.
ZA 29	3	All	Te	The drafting and presentation of terms and definitions does not adhere to the directives.	The drafting of terms and definitions shall adhere to Annex D of part 2 of the directives.	Accepted. Definitions are changed accordingly.
ZA 30	3.1		Te	The definition for acquisition is not complete.	Acquisition: process of making an identical copy or image of potential digital evidence at the incident scene whilst leaving the original evidence in exactly the same state that it was found	Rejected.
ZA 31	3.1.		Te	The acquisition process should always leave the original data in the same state as before the acquisition process. This is one of the fundamental rules of digital evidence admissibility in court.	Change to: <i>“a process of copying or imaging potential digital evidence at the incident scene and leaving the original evidence in tact after copying or imaging is performed”</i>	Rejected.
ZA 32	3.6		Te	See the directives for drafting terms and definitions.	If “forensic image” is considered a synonym of “digital evidence copy” it should be indicated as such. Else, use a NOTE.	Noted – The reference to ‘forensic image’ will be removed from the text. 3.6 is renumbered to 2.5.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

ZA 33	3.8 & 3.9		Ed	Font size is wrong with regards to the rest of the document. Font for 3.8 & 3.9 seems to be smaller.		Accepted.
ZA 34	3.8 & 3.10		Te	The two definitions (3.8 and 3.10) seem to be the same	Remove 3.8	Duplicate – Addressed in AU 8.2.
ZA 35	3.9		Te	Definition is inadequate.	Change to: <i>“mathematical function that takes data as input and generates a one-way unique fingerprint for the data, consisting of a fixed length string of bits”</i>	Rejected – Addressed in US 12.
ZA 36	3.20		Te	Definition is inadequate.	Change to: <i>“data that is especially prone to change and that can be easily spoiled, for example by switching off the power or passing through a magnetic field. Volatile data also includes data that changes as the system state changes. Examples include data stored in RAM and dynamic IP addresses”</i>	Accepted in principle – Incorporate with US 17, modify to fit directives. 3.20 is renumbered to 2.22.
ZA 37	3.20		Te	See the directives for drafting terms and definitions.	Use NOTES and EXAMPLES	Accepted.
ZA 38	4	BIOS	Te	State only terms for which the abbreviation is used. Define the term in Clause 3 if necessary.	BIOS basic input/output system	Duplicate – Addressed in US 18.
ZA 39	5	Paragraph 1	Te	Wrong choice of word: unusability	Change to: <i>“Failure to do so may render it unusable or may lead to an inaccurate conclusion.”</i>	Accepted.
ZA 40	5.1	Par 1	Ed	Grammatical error	Physical refers to representation of potential digital evidence in hardware and software components...	Not applicable since sentence changed – AU 16.
ZA 41	5.1	Par 1	Ed	Inconsistent word use. The word Hard-disk and hard disk is used in the document.	Settle on the correct usage and use throughout document to create consistency. It seems that hard disk is the more common use and thus Hard-	Accepted. Section 5.1 is renumbered to 4.3.1.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					disk should be changed to hard disk.	
ZA 42	5.1	Paragraph 1	Ed	Change 'could' to 'can'. Misspelled e.g.	Change to: <i>“Physical refers to the presentation of potential digital evidence in hardware and software components while logical refers to the address or location where the potential evidence can be located e.g. hard-disk.”</i>	Not applicable since sentence changed – AU 16.
ZA 43	5.1	1 and 2	Te	The use of “physical” and “logical” are unclear, especially under the heading ‘Identification’. Only during acquisition can one mention logical. The logical part cannot be identified during the identification process, but only the physical digital storage media. The use of the word “Potential digital evidence” also adds to the ambiguity. It is not easy to make a determination on the relevancy of evidence during identification. Any digital storage media is collected, then later after acquisition; one determines the relevancy of evidence.address or location where digital data is stored, e.g. on a hard disk.identification process should identify digital storage media which may contain digital data. Potential digital evidence may be changed to digital data storage with potential evidence or any shortened word	Accepted in principle – Incorporate with US 22. Section 5.1 is renumbered to 4.3.1.
ZA 44	5.1		Ed	Spelling mistake: occurred	Change to: occurred	Accepted. Section 5.1 is renumbered to 4.3.1.
ZA 45	5.1	After Paragraph 5.1	Ed	Remove full stop before the new heading.	Remove . before the new heading.	Accepted. Section 5.1 is renumbered to 4.3.1.
ZA 46	5.1	Par 3	Ed	Grammatical error	This process should also identify the possibility of potentially hidden digital evidence.	Accepted. Section 5.1 is renumbered to 4.3.1.
ZA 47	5.1	Par 4	Ed	The sentence seems difficult to read. Consider rewriting.	Rewrite and consider splitting the sentence into two separate sentences.	Accepted. Section 5.1 is renumbered to 4.3.1.
ZA 48	5.2	Par 2	Te	The two situations are mentioned, but never followed up upon. Surely the approach will differ with regards to the	Please clarify.	Accepted in principle – Text should be enhanced to clarify that the two

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				situation?		situations referred to is dead and live forensics. This section will be split into two sections for separate discussion on acquisition and collection. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition.
ZA 49	5.2	Paragraph 1	Te	Add word: 'with'. Change 'implied' to 'applied'.	Change to: <i>"Remember that digital data may be tampered with or easily spoiled if proper due care is not applied."</i>	Accepted. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition.
ZA 50	5.2	a)	Ed	Misspelled e.g	Change to e.g.	Accepted. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition.
ZA 51	5.2	a)	Te	Unallocated and slack space	Define these two terms in the definition of terms clause.	Accepted – ZA to provide content. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition..
ZA 52	5.2	Paragraph 2	Te	Logical order of events: first list real time, and then after the incident.	Change to: <i>"In doing acquisition, potential digital evidence can exist in two conditions: when the incident is in progress or when the incident already happened."</i>	Accepted. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition.
ZA 53	5.2	a, b, c, d	Te	The definitions do not really provide distinction between the types of acquisition.	Elaborate more to distinct between the types of acquisition, or combine the explanation and only list the types.	Accepted – Incorporate with UK 7. Section 5.2 is renumbered and split into 4.3.2 Collection and 4.3.3 Acquisition.
ZA 54	5.3		Te	The section on the preservation of digital evidence is not sufficient. No mention is made of chain of evidence, bagging and tagging evidence, etc.	Consider amalgamating section 7 and section 5.1 as they deal with the same thing.	Accepted in principle - Extend text on identification to include chain of custody, bagging and tagging. Make use of cross reference from current 5.2 and chain of custody, but keep sections

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

						separate. Section 5.3 is renumbered to 4.3.4.
ZA 55	5.3	Paragraph 1	Ed	Spelling mistake: admissable	Change to: admissible	Duplicate – Addressed in FIRST 13.
ZA 56	5.5		Te	Add examples of different presentation types for different audiences.	Presentation will differ if the evidence serves in a criminal proceeding or in an organisational disciplinary hearing. Evidence for court may be more formal, both reports and verbal explanation. Disciplinary hearings may consist of screenshots and perhaps slideshows presenting graphs and other relevant data.	Not applicable since section is deleted – JP 15.
ZA 57	6		Te	Before digital evidence (Section 5) is discussed, I would think that the principles of care of evidence (Section 6) should be discussed. Also, the subsections in section 5 should link back to the relevant sections in the current section 6 in order to provide a proper holistic approach to evidence gathering.	Swap the order of Sections 5 and 6. Shouldn't sections 5 & 6 be combined? These sections overlap hugely.	Accepted in principle – In the new structure clause 5.1 (current section 5) will be swapped with clause 5.2 (current section 6). Reject combining of sections, rather rewrite to diminish overlap. Section 6 is renumbered and split into 4.1 and 4.2.
ZA 58	6.2 & 6.3		Te	In the audit world, the word “re-performance” is often used. It is key that any person reading the case notes should be able to re-perform the entire investigation from the original notes. It is therefore extremely important that the notes should be detailed and exact and should be written in a non-technical language so that any reader should be able to understand the process.	Consider the use of the term re-performance instead of repeatability.	Rejected – The introduction of re-performance may complicate the document.
ZA 59	6.2		Te	Proper word usage should be used in reports. Investigate the use of the classes of evidence from the audit world	Extend the current section on auditability by including mentioned	Rejected – Content is out of scope of the standard.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				(listed here from weakest to strongest): Evidence by discussion (documented as: "It was noted that x through discussion with y (title) on <i>date</i> ."). Evidence by observation (documented as: "Observed with <i>person</i> on <i>date</i> that x"). Evidence by inspection (documented as: "Inspected x on <i>date</i> and noted that y"). Evidence by re-performance (documented as "Re-performed x by means of procedure y on <i>date</i> and noted that z").	jargon as examples of making an investigation (and subsequent report) auditable by auditing standards.	
ZA 60	6.3	B	Te	Shouldn't repeatability extend to different operators as well? What happens if the original operator is not available or doesn't work for the organisation anymore?	Remove bullet point.	Accepted. Section 6.3 is renumbered to 4.1.2.
ZA 61	6.4	Paragraph 2	Ed	Change 'defensible' to 'defensibility'.	Change 'defensible' to 'defensibility'.	Not applicable since sentence is removed – US 38.
ZA 62	7	Paragraph 1	Te	Definition is not accurate.	Change to: " <i>Chain of custody is a record of who had the responsibility of handling collected digital device(s) and/or acquired digital data at a specific point in time.</i> "	Accepted. Section 7 is renumbered to 5.1.
ZA 63	7	Par 1	Ed	Grammatical error.	Consider replacing weightage with weight.	Rejected - AU 31 replaces evidentiary weightage' with 'evidential weighting'.
ZA 64	8.1	Par 1	Ed	Typographical error	Use premises instead of premise.	Accepted. Section 8.1 is renumbered to 5.3.1.
ZA 65	8.1		Ed	"Note: Competence of a DEFR varies from from one.... another. However,it is utmost important for" Double use of the word 'from' and spacing is a problem after 'however'.	"Note: Competence of a DEFR varies from one.... another. However, it is utmost important for..."	Accepted – Will be incorporated into the new text. Section 8.1 is renumbered to 5.3.1.1.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

ZA 66	8.3	Bullets	Te	Consistency in presentation. Some aspects are listed as questions, and others as sentence fragments.	Be consistent in presenting lists: either all fragments or all questions.	Accepted. Section 8.3 is renumbered to 5.2.
ZA 67	9		Ed	Spelling mistake: 'briefng'	Change to: briefing.	Duplicate – Addressed in FIRST 36.
ZA 68	10.1		Te	Refrain from using Latin expressions such as "in situ"	Use the correct English phrase, such as "in its original position".	Accepted. Section 10.1 is renumbered to 5.3.3.1.
ZA 69	11	3	Ed	General written practice: write out all numbers less than twenty.	Change '2' to 'two'.	Accepted. Section 11 is renumbered to 5.8.
ZA 70	11	3	Ed	Spelling mistake: 'prioritze'	Change to: prioritize	Duplicate – Addressed in FIRST 39.
ZA 71	11	Note 2	Ed	Spelling mistake: 'pyhsical'	Change to: physical	Duplicate – Addressed in FIRST 40.
ZA 72	11 or 12.1.1.		Te	When the strategy for first steps to be taken after the DEFR arrival on an incident scene is discussed, the warning in 14.1 a) should be included. It is of crucial importance to recover all devices from an incident scene.	Include comment similar to 14.1 a).	Accept in principle – Content will be drafted to prevent redundancy. Section 11 is renumbered to 5.8.
ZA 73	12.1.1 a)		Ed	Typographical error	... the peripheral devices. The ...	Accepted. Section 12.1.1 is renumbered to 6.1.1.1.
ZA 74	12.1.1	1	Ed	Full stop too many.	Change to: <i>"The first step of identification is to secure the incident scene and move people away from computers and the peripheral devices. The DEFR must ensure that no unauthorized person has access to any devices at the premise."</i>	Accepted. Section 12.1.1 is renumbered to 6.1.1.1.
ZA 75	12.1.2	Par 2	Te	Consider adding the requirement that such conversations should be recorded in order to ensure that the details are accurate and that the witness cannot change his/her statement.	Consider adding the requirement that such conversations should be recorded in order to ensure that the details are accurate and that the witness cannot change his/her statement.	Accepted – ZA to provide content. Section 12.1.2 is renumbered to 6.1.1.2.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

ZA 76	12.2.	Par 1	Ed	Typographical errors	...potential digital evidences from them. The choice ... (a) when the computers are powered on, (b) when the ...	Accepted. Section 12.2 is renumbered and split into 6.1.2 and 6.1.3.
ZA 77	12.2	1	Ed	Comma too many.	Change to: "...(a) when the computers are powered on, (b) when the computers are powered off and..."	Accepted. Section 12.2 is renumbered and split into 6.1.2 and 6.1.3.
ZA 78	12.2.1	b	Ed	UPS is written out incorrectly.	It should be: uninterruptible power supply (UPS)	Accepted. Section 12.2.1 is renumbered to 6.1.2.1.
ZA 79	12.2.1	c	Te	Consider adding the information that the action of depressing the power button on a computer may be configured to kick off a script that may alter information and/or delete information from the system before shutting down.		Accepted in principle – Include a warning or general note. Section 12.2.1 is renumbered and split into 6.1.2.1 and 6.1.3.1.
ZA 80	12.2.1 f) 12.2.2 c)		Te	Is it <i>really</i> necessary to tape up the floppy disk drive?	Consider removing the requirement. Floppy drives are mostly obsolete anyways.	Rejected – Floppy disk drive may still be relevant in legacy systems. Incorporate as Desirable (see UK 18).
ZA 81	12.2.4	c	Ed	Spelling mistake: 'identified'	Change to: identified	Duplicate – addressed in FIRST 50.
ZA 82	12.3	c	Te	Typographical error	... first responder or personnel ...	Accepted. Section 12.3 is incorporated into 5.7.
ZA 83	13		Te	Should sections 12 and 13 not be amalgamated with the differences merely referred to in the text? It feels like an unnecessary duplication of data with very few real differences.		Superseded by new structure suggested in JP10.
ZA 84	13.1.1	a	Te	How should the DEFR ensure that no unauthorised person has access to the device via a network connection? It is quite possible for a suspect to remotely access a networked resource and tamper with the	Specify specific actions regarding prohibiting remote network access.	Superseded by SE 24.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				evidence.		
ZA 85	13.3	a	Ed	Spelling mistake: 'involces'	Change to: involves	Duplicate – Addressed in FIRST 53.
ZA 86	13.3	c	Ed	“first responder or o personnel”	Typing error, delete the 'o'	Accepted.
ZA 87	14.1.1	1	Ed	Spelling mistake: 'craddles'	Change to: cradles	Duplicate – Addressed in FIRST 55.
ZA 88	14.2	2	Ed	Spelling mistake: 'evironment'	Change to: environment	Accepted.
ZA 89	14.2	3	Ed	Spelling mistake: 'spoilling'	Change to: spoiling	Accepted.
ZA 90	14.2.1	b	Ed	Sentence construction	Therefore, it is highly recommended that the mobile devices should be delivered to the lab as soon as possible for investigation.	Not applicable since section has been deleted – AU 76.
ZA 91	14.2.2	b	Ed	Spelling mistake: 'craddles'	Change to: cradles	Duplicate – Addressed in FIRST 55.
ZA 92	14.3	d	Ed	Spelling mistake: 'shilded'	Change to: shielded	Duplicate – Addressed in FIRST 62.
ZA 93	15	1	Ed	Spelling mistake: 'propreitary'	Change to: proprietary	Accepted.
ZA 94	15	1	Ed	CCTV should always be capitalized	Change to CCTV	Accepted.
ZA 95	15.1	1	Ed	Spelling mistake: 'necessary'	Change to: necessary	Duplicate – Addressed in FIRST 63.
ZA 96	15.2	k	Ed	Spelling mistake: 'circumtsances'	Change to: circumstances	Accepted.
ZA 97	16.1	1	Te	Add more “modern” media types. Currently most focus is on magnetic media. Also include flash and optical media.	Include flash and optical media.	Accepted in principle – ZA to provide content. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
ZA 98	16.1	f	Ed	Spelling mistake: 'electricy'	Change to: electricity	Accepted. Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
ZA 99	16.1	i	Te	Investigators should label evidence with ink	“Investigators” is a correct word but I	Accepted.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on ISO/IEC 1st WD 27037

Date: 2009-11-11

Document: **SC 27 N7570**

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

					feel it would be more appropriate and consistent to use the word "DEFER"	Sections 16.1 and 16.2 are renumbered to 5.5 and 5.6.
ZA 100	Annex	A and B	Ed	Fonts in Annex A and B are not the same.	Use fonts and font sizes consistently.	Accepted.

SD6 editor	3		Ge	<p>ISO/IEC Directives, Part 2: Rules for the structure and drafting of International Standards states how to write the "Terms and definitions" as follows.</p> <p>D.1.5.3 The form of a definition shall be such that it can replace the term in context. Additional information shall be given only in the form of examples or notes (see D.3.9).</p> <p>D.3.2 Layout</p> <p>The preferred term (set in bold type in the printed publication) shall be placed on a new line, after its reference number, starting with a lower case letter except for any capital letters required by the normal written form in running text. The definition shall be placed on a new line, starting with a lower case letter, except for any capital letters required by the normal written form in running text, and shall not be followed by a full-stop.</p> <p>Following is a good example.</p> <p>3.13</p> <p>encryption</p> <p>reversible operation by a cryptographic algorithm converting data into ciphertext, so as to hide the information content of the data</p> <p>NOTE Encryption and encipherment are equivalent terms.</p>	Apply directives.	Accepted – Editors need to check which terms defined are used in the text itself and remove redundant definitions.
------------	---	--	----	---	-------------------	--

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<p>[ISO/IEC 9798-1:1997]</p> <p>Based on the above rules, following errors are found in the "Terms and definitions" of the N7570 1st WD 27037:</p> <ol style="list-style-type: none"> Terms and/or definitions should be all in Arial font with font size 10. (But 3.8 and 3.9 are size 9.) Terms and/or definitions should be in lower case characters except usual usage is in capital letter(s). Some definitions are starting with article of "a" or "an" or "the", they should be removed. Definitions should not be explanation but be words which can replace the term in the main texts. Definitions should be one sentence, other sentence(s) should be put into NOTE or EXAMPLE. Full-stops (periods) at the end of definitions should be removed. <p>Following are bad examples.</p> <p>3.6 digital evidence copy a copy of digital data obtained in a forensically sound manner. Also called a forensic imae.</p> <p>3.7 Digital Evidence First Responder person(s) at a scene containing digital evidence who is authorized, qualified and/or trained in digital forensics with responsibility for handling that evidence</p> <p>3.20</p>		
--	--	--	--	--	--	--

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<p>volatile data data that is easily spoiled for example by switching off the power or passing through a magnetic field. Volatile data also includes data that changes as the system state changes. Examples include data stored in RAM and dynamic IP addresses</p>		
--	--	--	--	--	--	--

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.