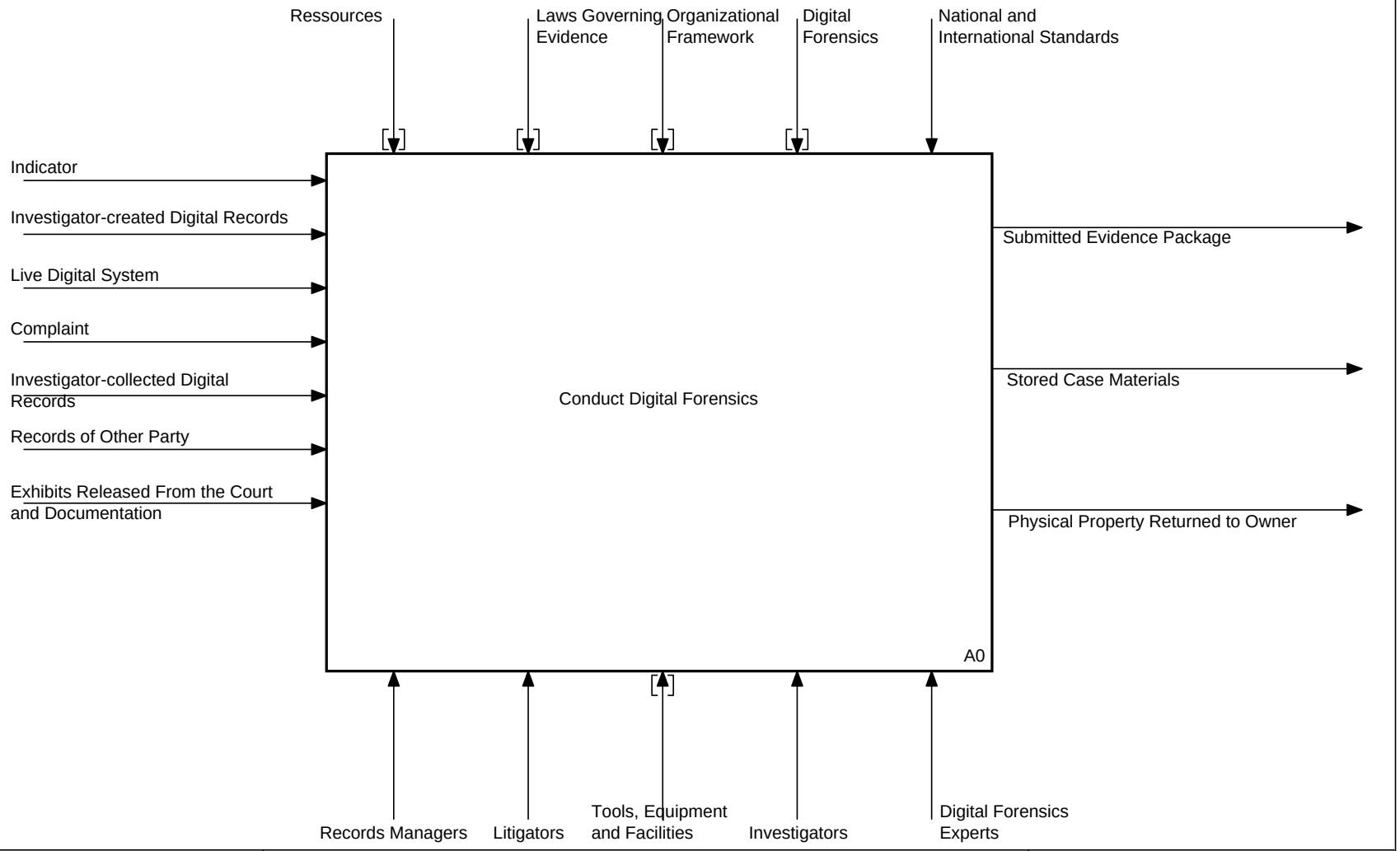
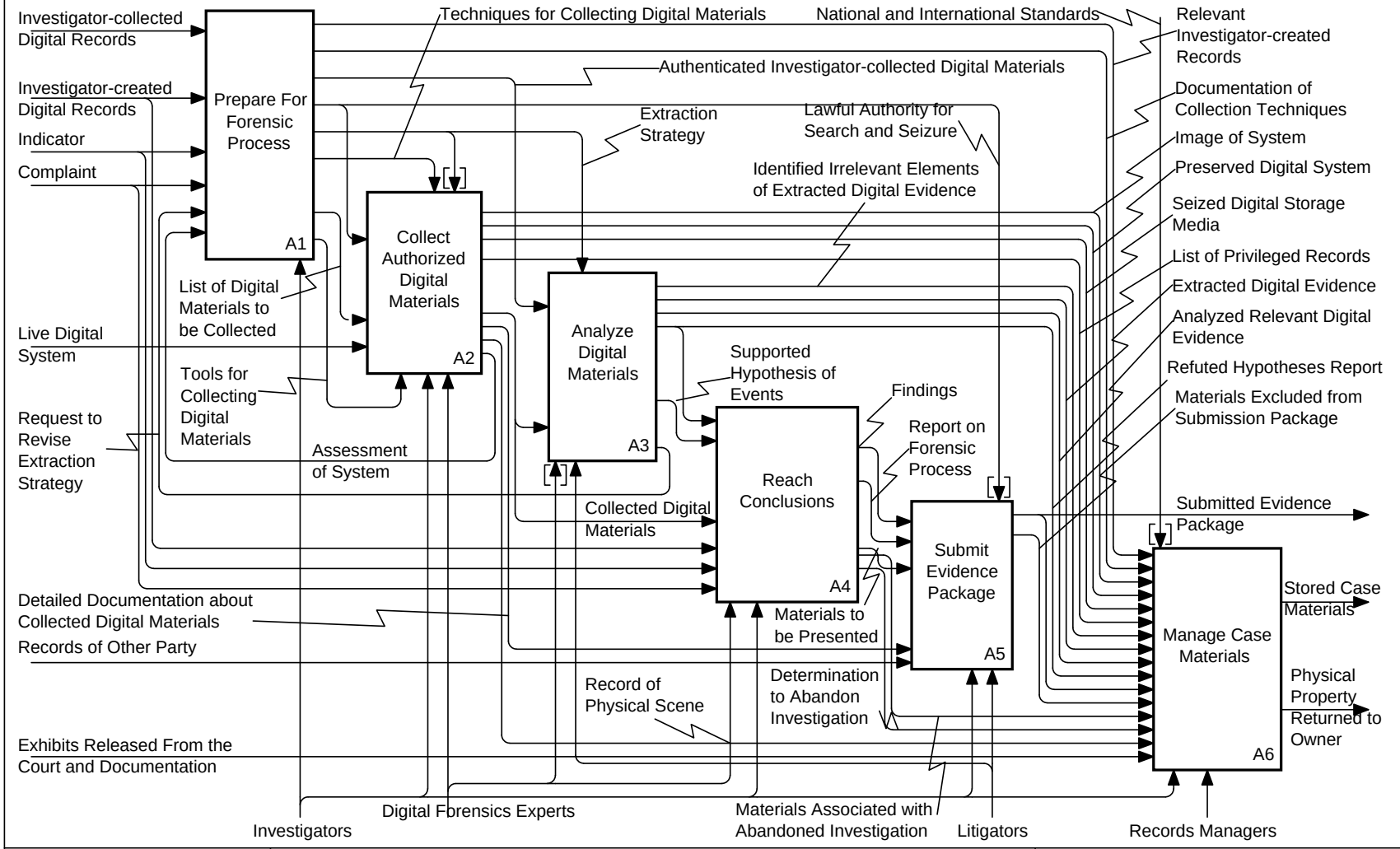
USED AT:	AUTHOR:	DATE: 03/11/2008		WORKING	READER DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2011		DRAFT		TOP
				RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION		



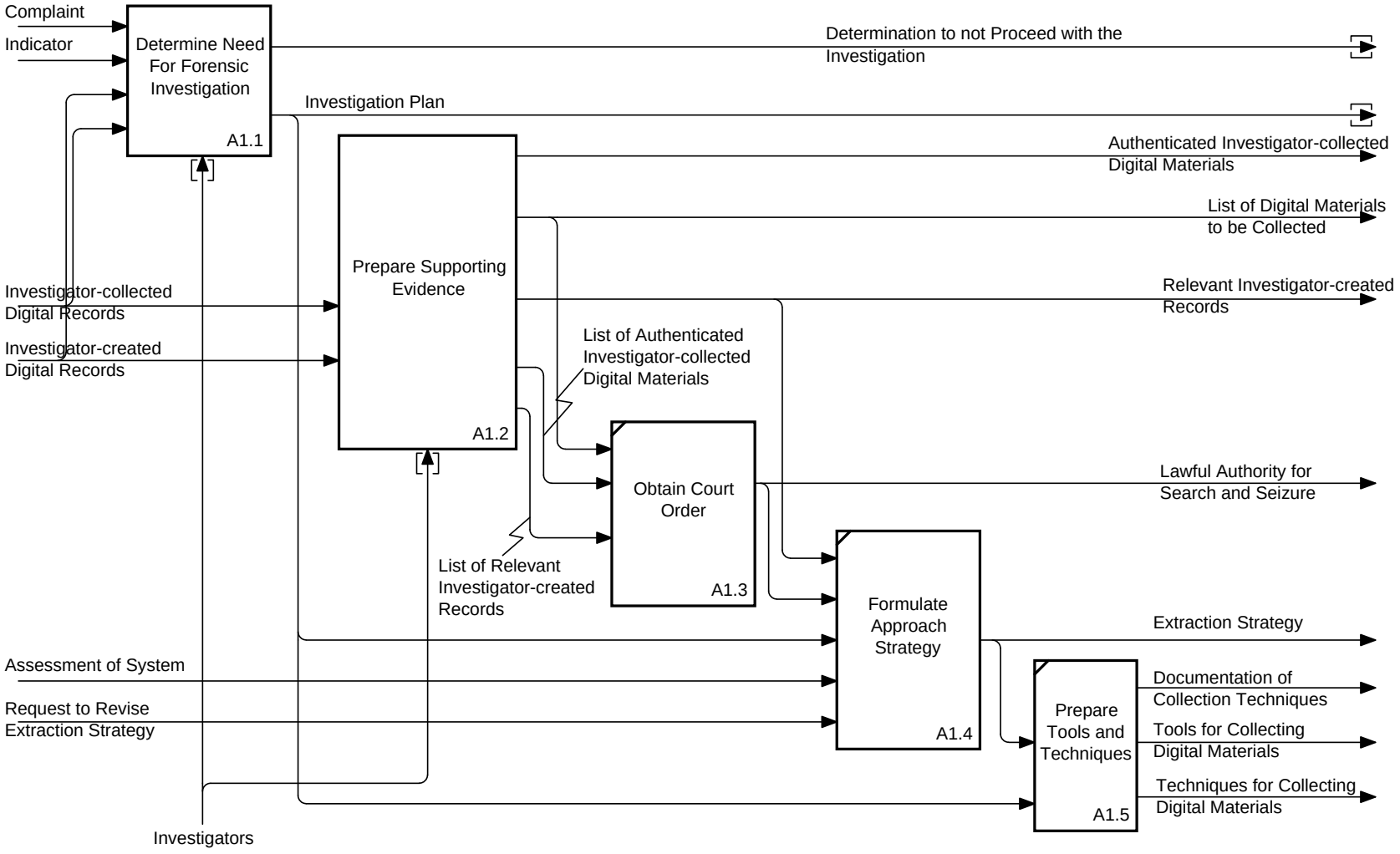
NODE:	TITLE:	NUMBER:
A-0	Conduct Digital Forensics	

USED AT:	AUTHOR:	DATE: 14/11/2008	■	WORKING	READER	DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2011		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			A-0



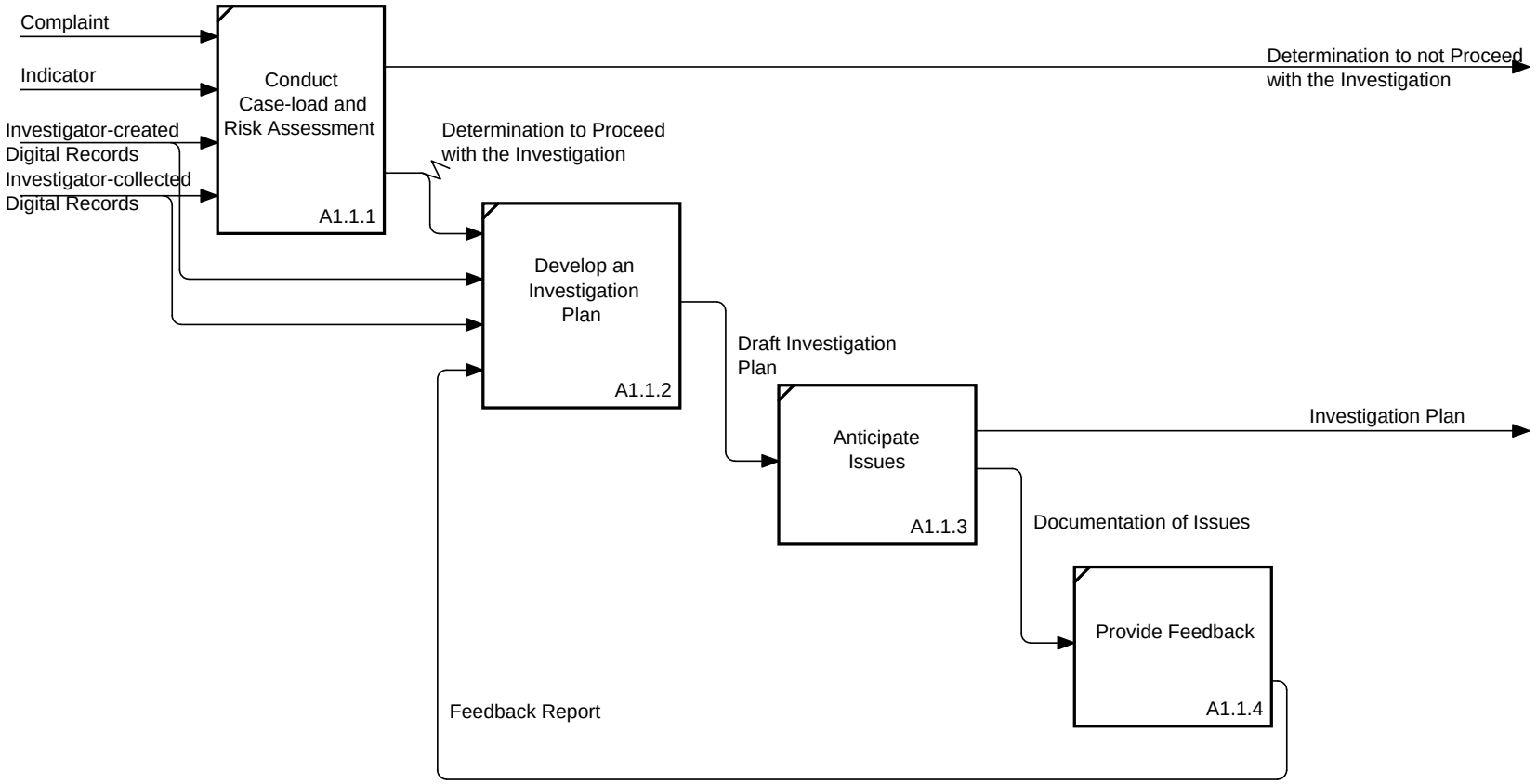
NODE:	TITLE:	NUMBER:
A0	Conduct Digital Forensics	

USED AT:	AUTHOR:	DATE: 14/11/2008	■	WORKING	READER	DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2009		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			A0



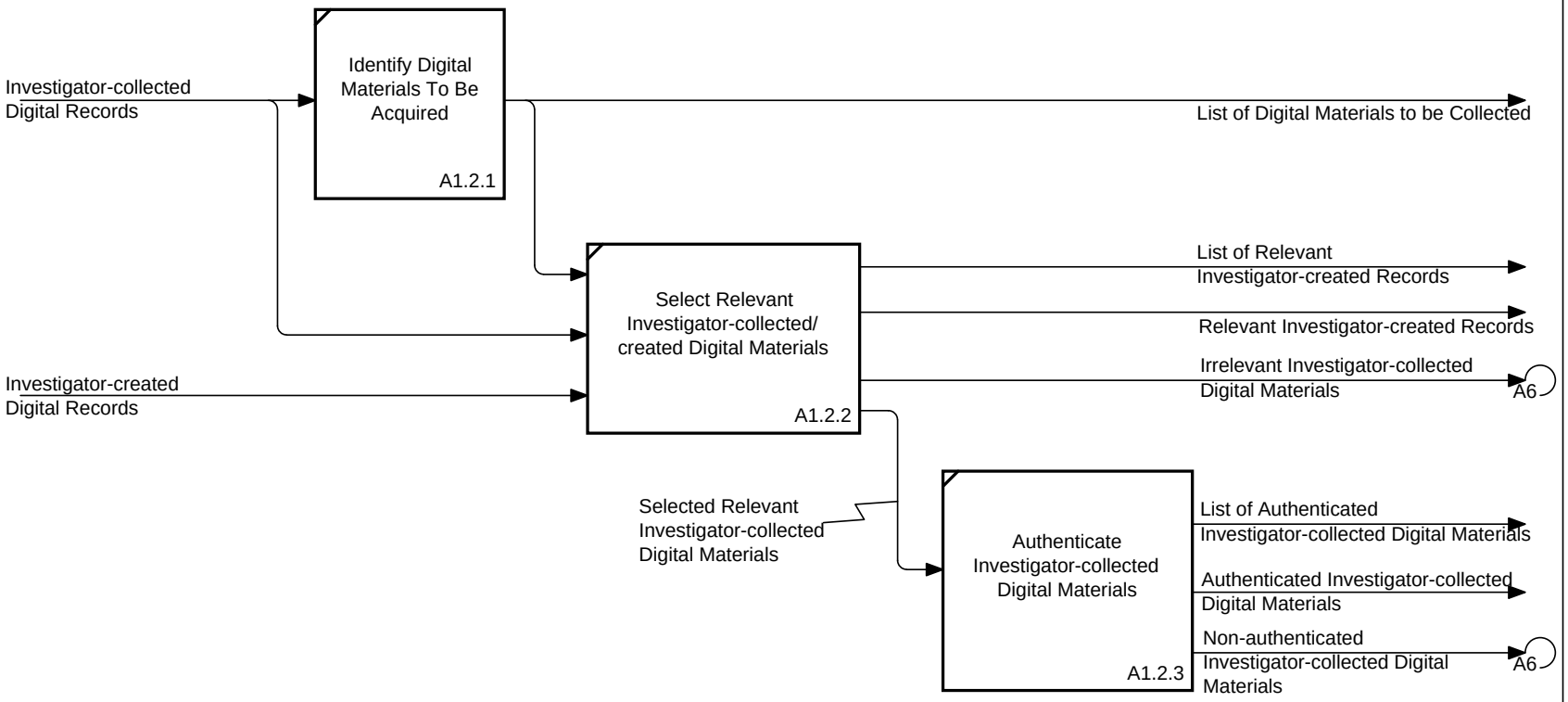
NODE:	TITLE:	NUMBER:
A1	Prepare For Forensic Process	

USED AT:	AUTHOR:	DATE: 13/05/2009		WORKING	READER	DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2009		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			A1



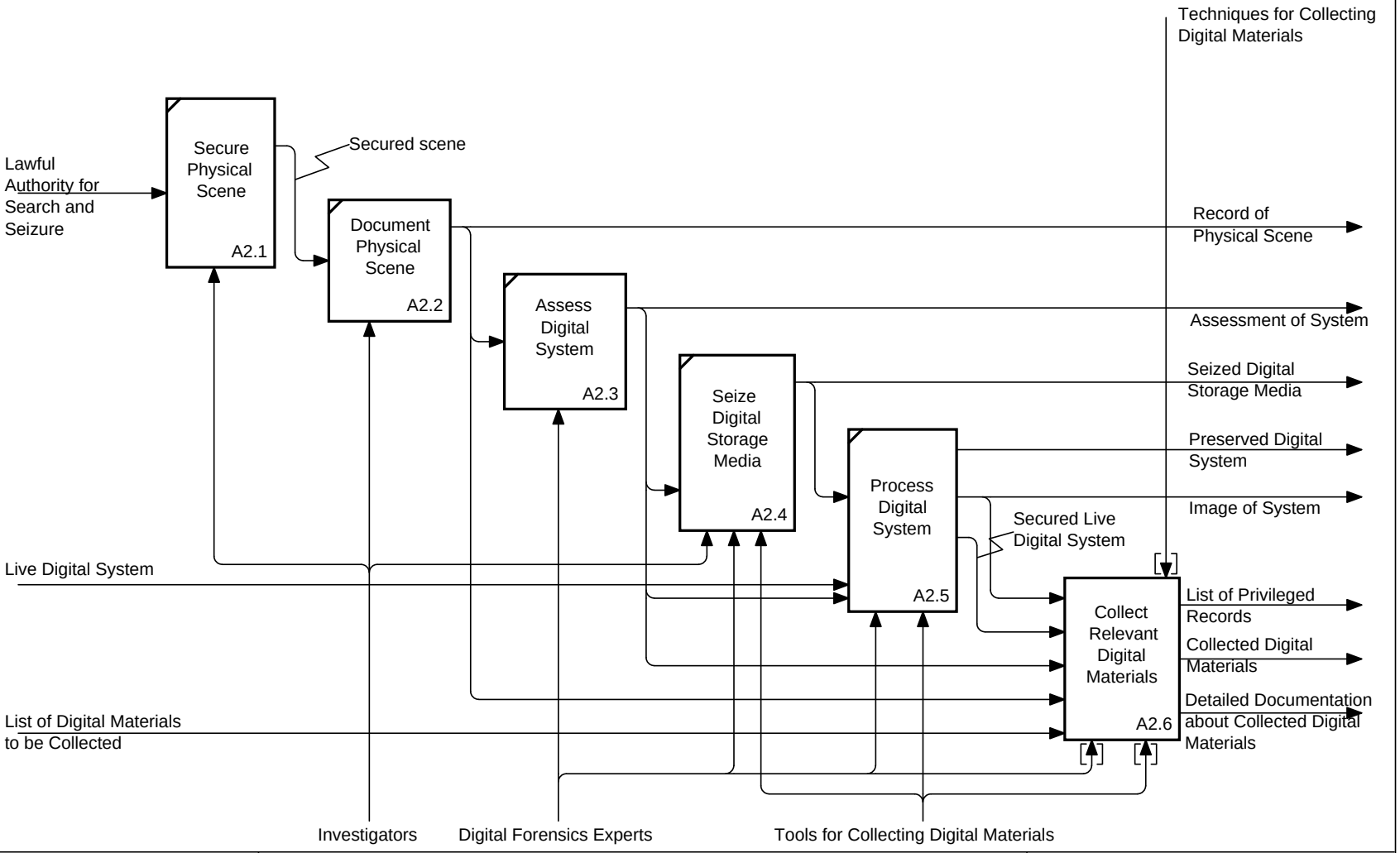
NODE:	TITLE:	NUMBER:
A1.1	Determine Need For Forensic Investigation	

USED AT:	AUTHOR:	DATE: 14/11/2008	■	WORKING	READER	DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2009		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			A1



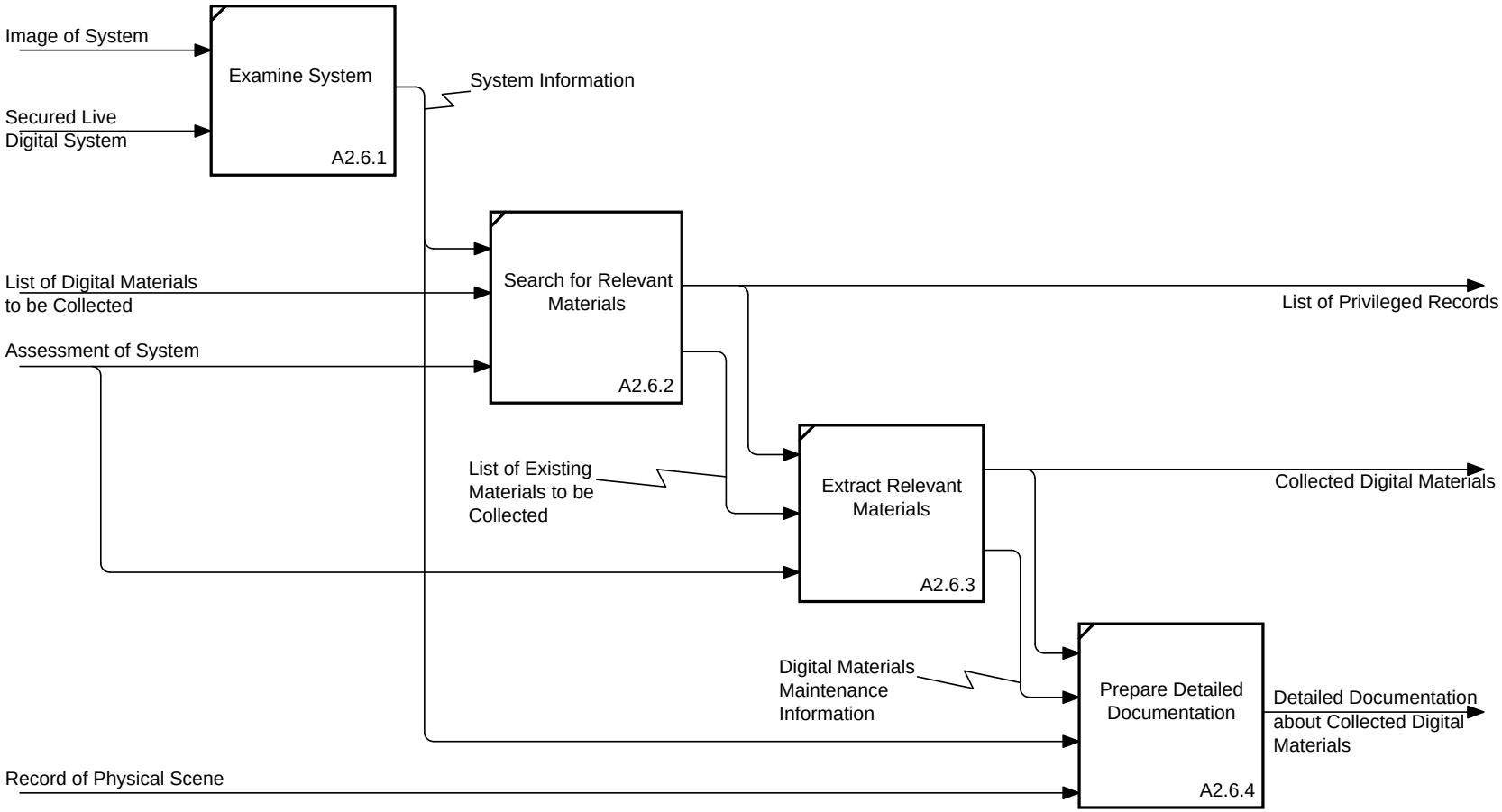
NODE:	TITLE:	NUMBER:
A1.2	Prepare Supporting Evidence	

USED AT:	AUTHOR:	DATE: 14/11/2008		WORKING	READER	DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2009		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			A0



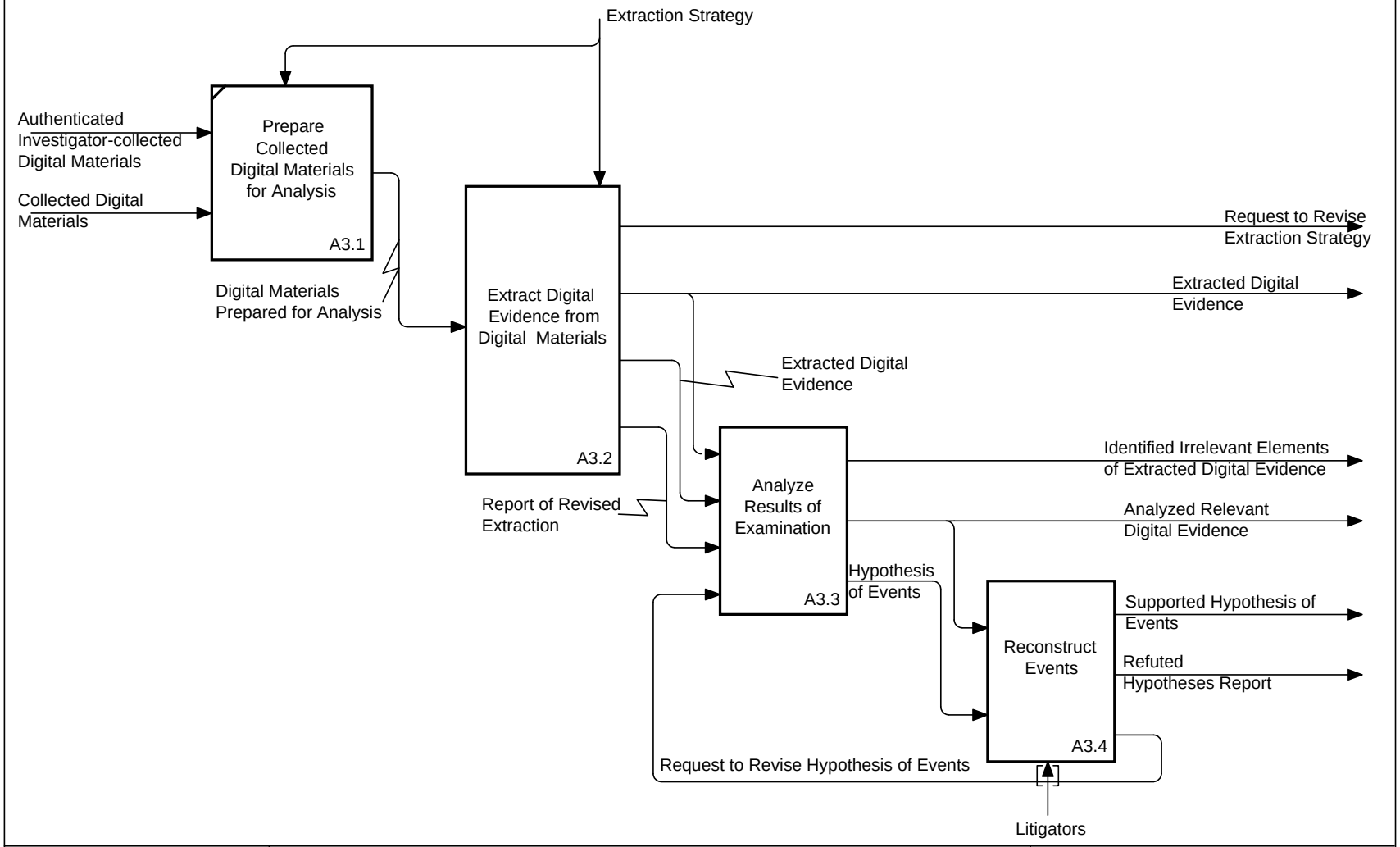
NODE:	TITLE:	NUMBER:
A2	Collect Authorized Digital Materials	

USED AT:	AUTHOR:	DATE: 14/11/2008	■ WORKING	READER DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2011	DRAFT		
			RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10		PUBLICATION		A2



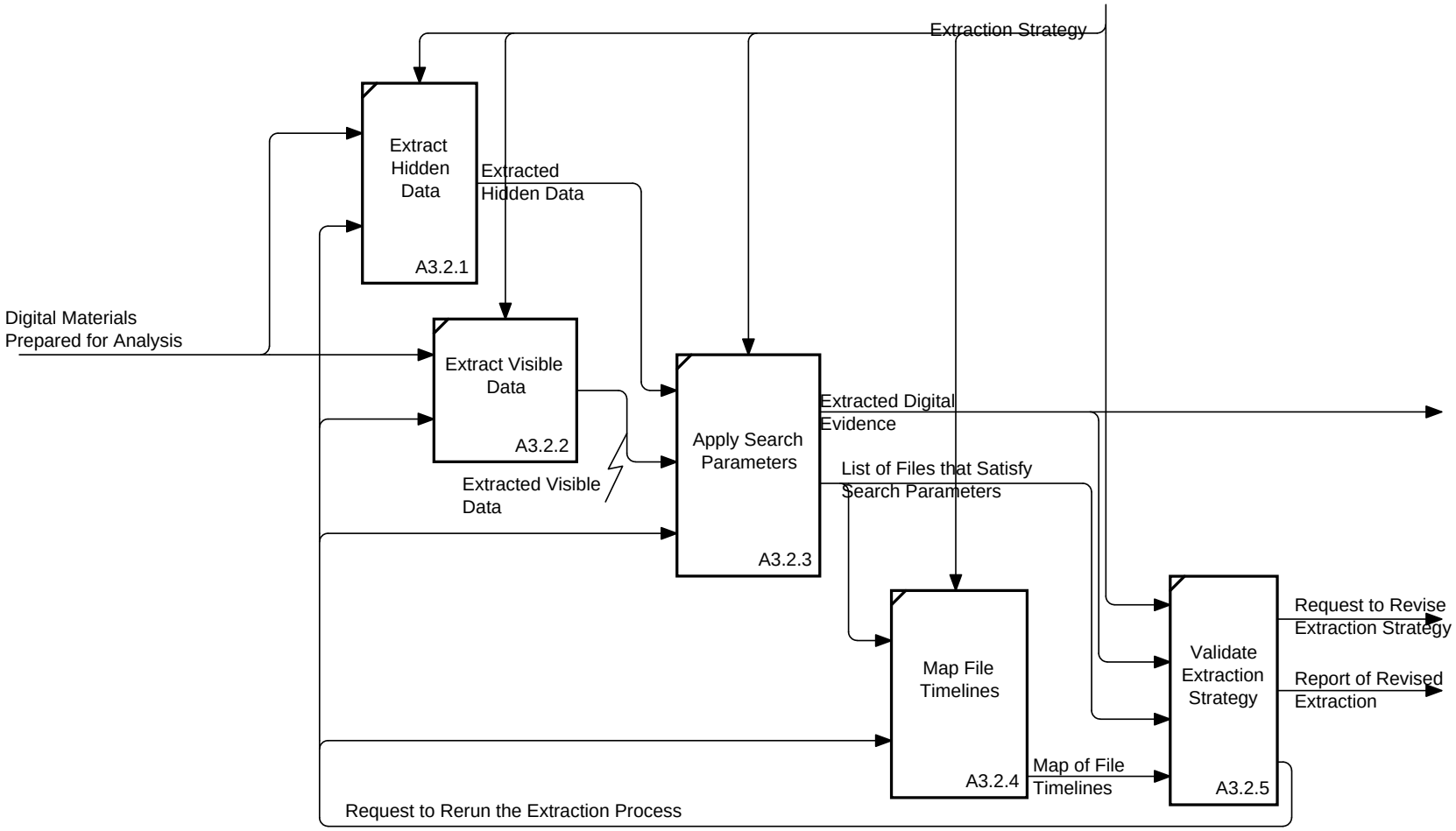
NODE:	TITLE:	NUMBER:
A2.6	Collect Relevant Digital Materials	

USED AT:	AUTHOR:	DATE: 04/06/2010		WORKING	READER DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2011		DRAFT		
				RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION		A0



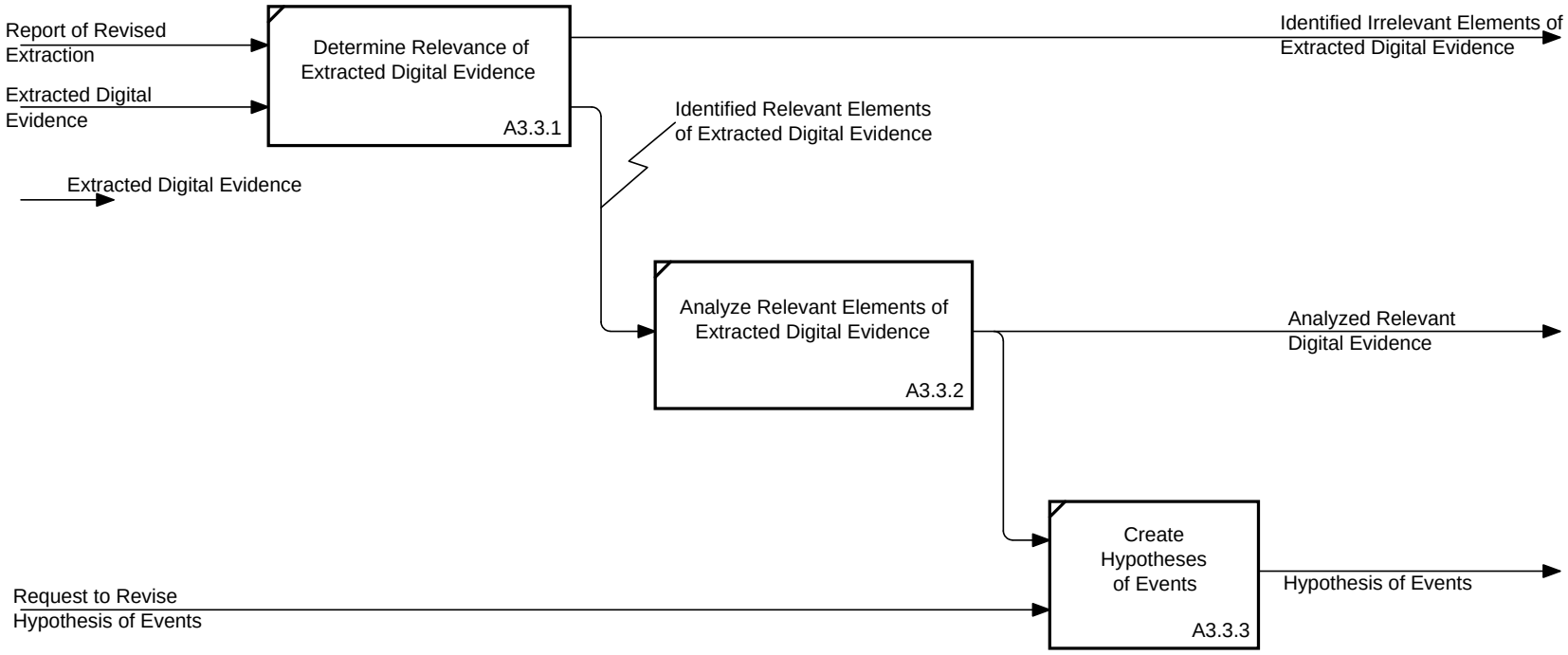
NODE:	TITLE:	NUMBER:
A3	Analyze Digital Materials	

USED AT:	AUTHOR:	DATE: 04/06/2010	WORKING	READER DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2011	DRAFT		
			RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10		PUBLICATION		A3



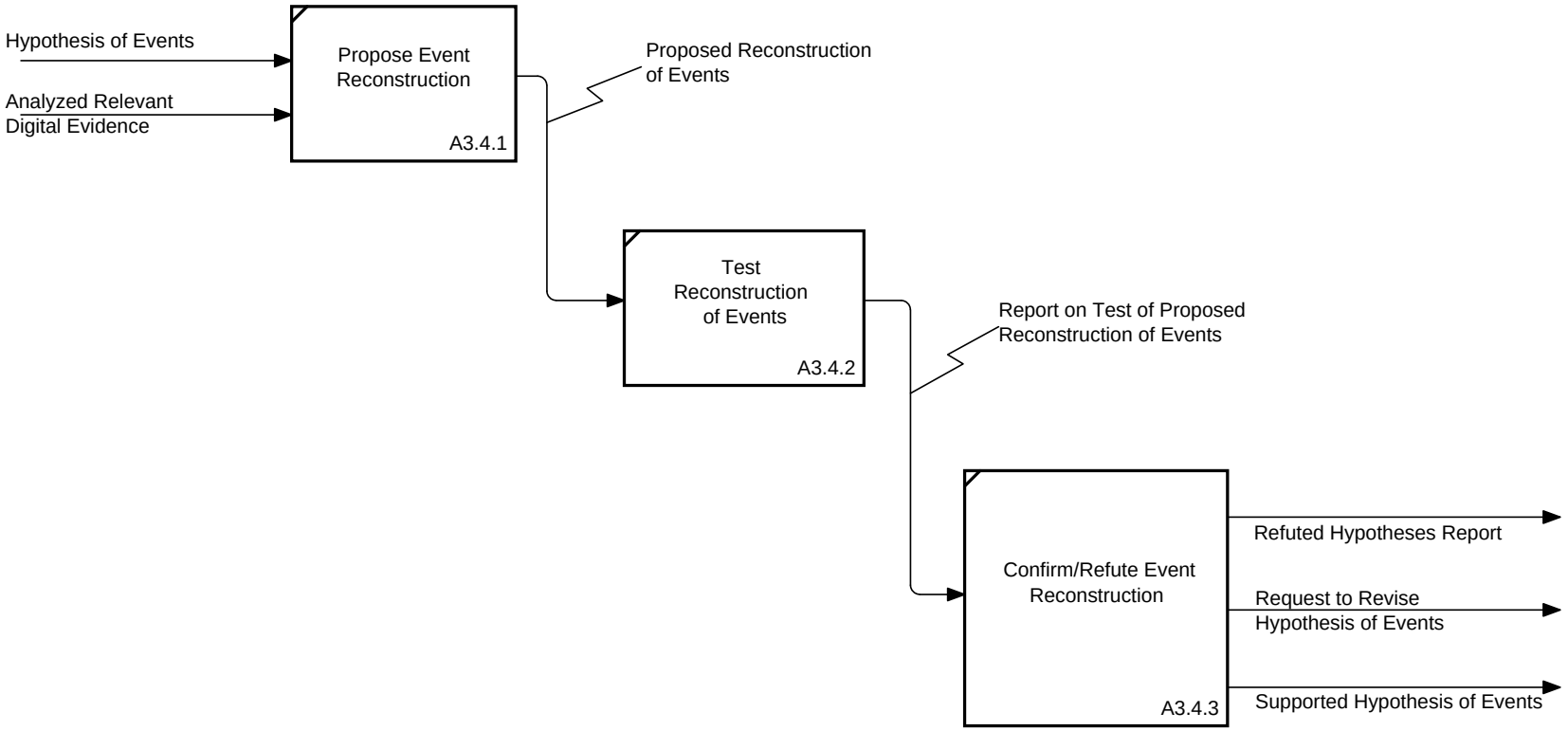
NODE:	TITLE:	NUMBER:
A3.2	Extract Digital Evidence from Digital Materials	

USED AT:	AUTHOR:	DATE: 04/06/2010		WORKING	READER DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2011		DRAFT		
				RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION		A3



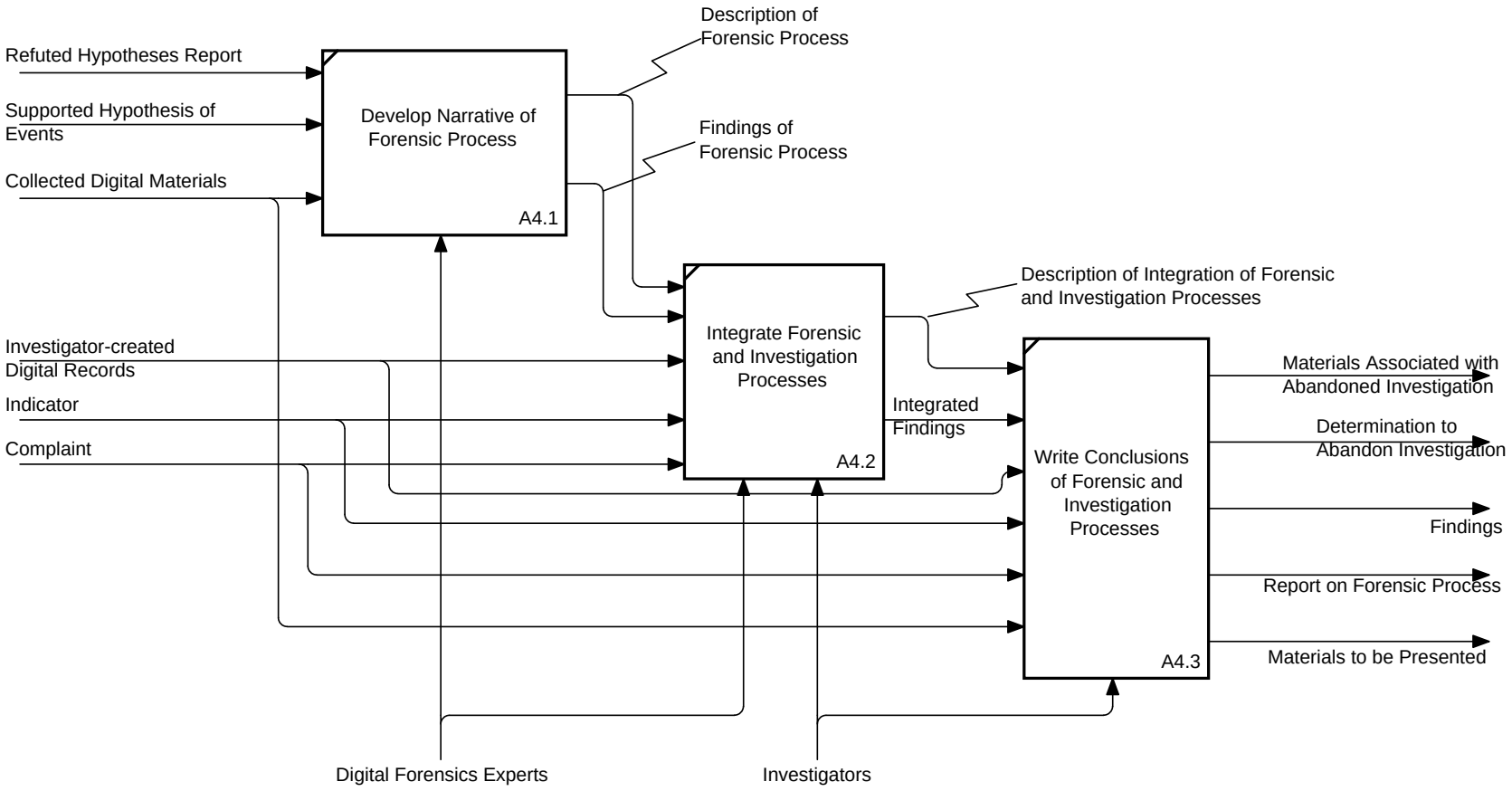
NODE:	TITLE:	NUMBER:
A3.3	Analyze Results of Examination	

USED AT:	AUTHOR:	DATE: 04/06/2010		WORKING	READER DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2011		DRAFT		
				RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION		A3



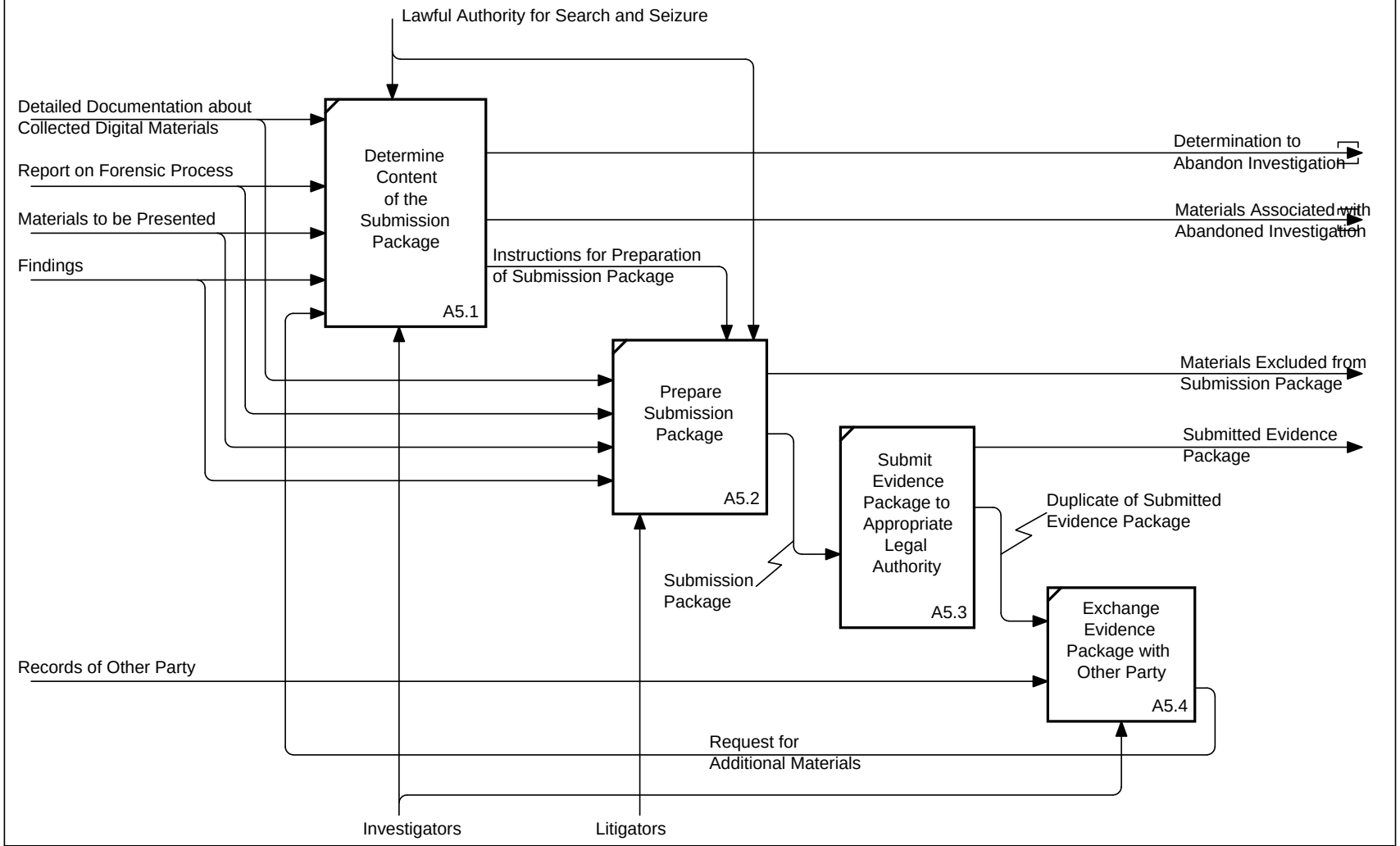
NODE:	TITLE:	NUMBER:
A3.4	Reconstruct Events	

USED AT:	AUTHOR:	DATE: 04/06/2010		WORKING	READER DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2011		DRAFT		
				RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION		A0



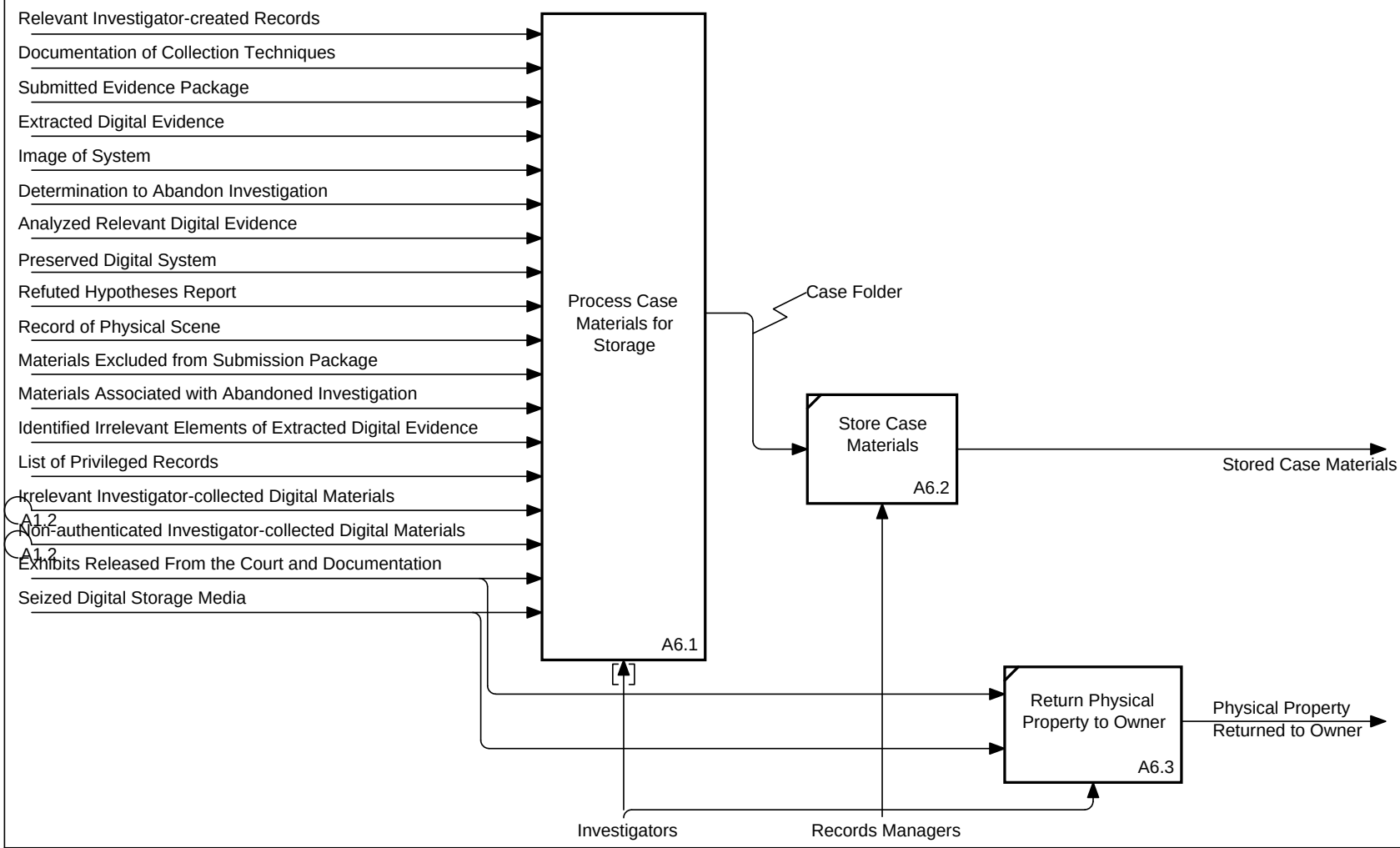
NODE:	TITLE:	NUMBER:
A4	Reach Conclusions	

USED AT:	AUTHOR:	DATE: 14/11/2008	■	WORKING	READER	DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2009		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			A0



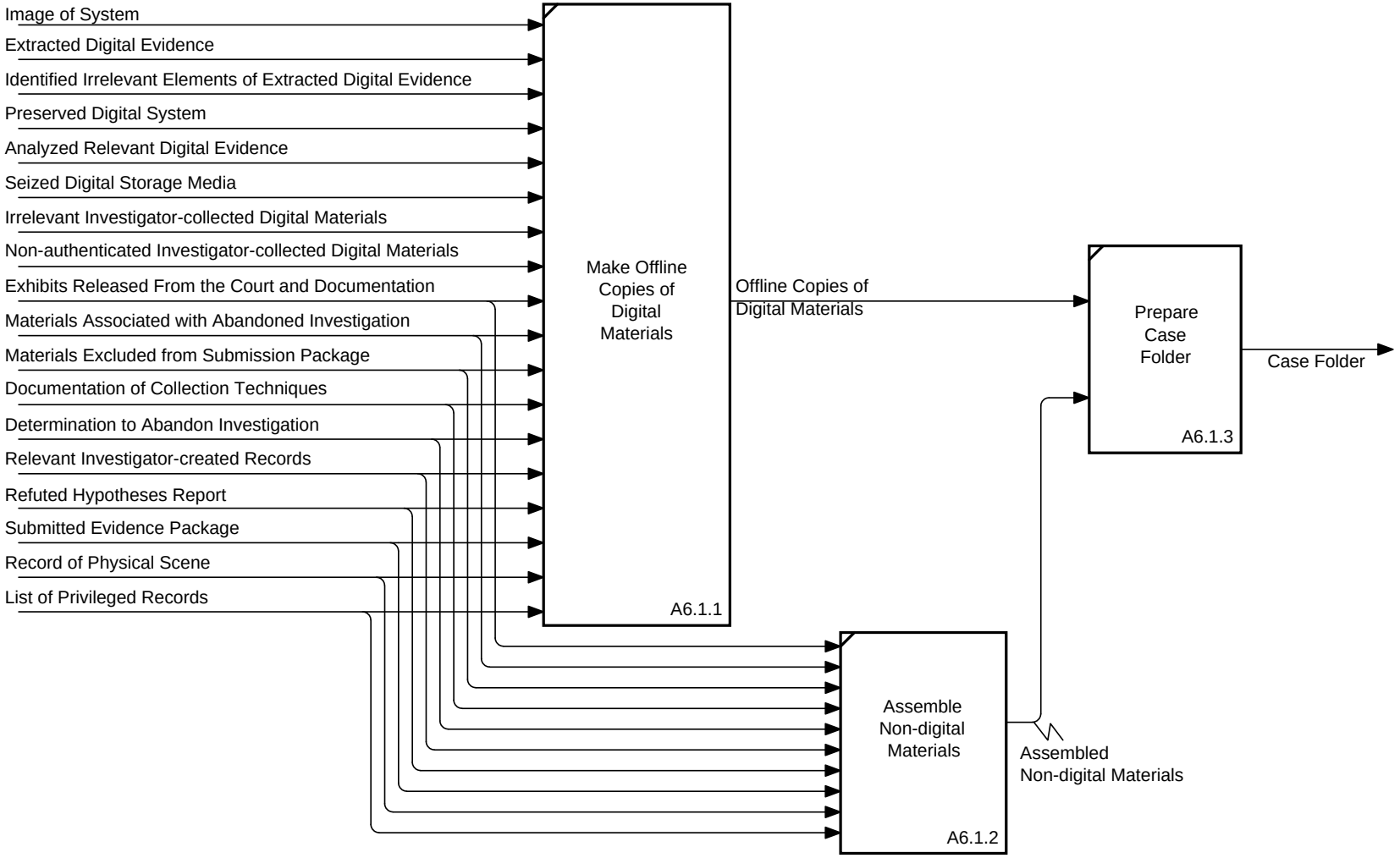
NODE:	TITLE:	NUMBER:
A5	Submit Evidence Package	

USED AT:	AUTHOR:	DATE: 14/11/2008		WORKING	READER	DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2009		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			A0



NODE:	TITLE:	NUMBER:
A6	Manage Case Materials	

USED AT:	AUTHOR:	DATE: 04/06/2010	WORKING	READER DATE	CONTEXT:
	PROJECT: DRF Model	REV: 13/05/2011	DRAFT		
			RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10		PUBLICATION		A6



NODE:	TITLE:	NUMBER:
A6.1	Process Case Materials for Storage	

Digital Records Forensics Model Activity Definitions, May 13, 2011		
Activity Name	Activity Number	Activity Definition
Conduct Digital Forensics	A0	To ensure the creation and/or collection of trustworthy digital records to be used as evidence, their maintenance throughout the judicial process and their preservation over the long term for accountability, reference or further action.
Prepare For Forensic Process	A1	To identify the incident, prepare supporting evidence, obtain a court order, formulate the approach strategy, and prepare tools and techniques.
Determine Need For Forensic Investigation	A1.1	To make decisions about the feasibility of conducting a digital forensic investigation based on material collected and resources available.
Conduct Case-load and Risk Assessment	A1.1.1	To evaluate resources available and establish realistic achievable priorities in light of backlogs and other on-going investigations.
Develop an Investigation Plan	A1.1.2	To identify and allocate adequate resources necessary to conduct each stage of the investigation.
Anticipate Issues	A1.1.3	To predict concerns and problems that might arise during the investigation and analysis.
Provide Feedback	A1.1.4	To report on any improvements to the particular investigation or overall analysis process to ensure that the analysis lifecycle is an effective process from beginning to end.
Prepare Supporting Evidence	A1.2	To collect, create and itemize supporting materials for the investigation and the application for a court order.
Identify Digital Materials To Be Acquired	A1.2.1	To list the types of digital materials that investigators need to collect.
Select Relevant Investigator-collected/ created Digital Materials	A1.2.2	To identify the digital materials that support the issuing of a warrant.
Authenticate Investigator-collected Digital Materials	A1.2.3	To assess the identity and integrity of materials to be used in support of the application for a court order.
Obtain Court Order	A1.3	To prepare an application for a court order, which may include a search warrant or any similar authority; submit the application; obtain the court order
Formulate Approach Strategy	A1.4	To articulate the methods and processes that will be used to acquire custody of the relevant materials.
Prepare Tools and Techniques	A1.5	Self-explanatory.
Collect Authorized Digital Materials	A2	To secure the physical scene, document the physical scene, assess the digital system, seize the physical digital storage medium, or process the digital system.
Secure Physical Scene	A2.1	To protect the incident environment from interference and stop further crimes or damage originating from the impounded items, such as spreading malware.
Document Physical Scene	A2.2	To represent the incident environment as secured by the investigator.
Assess Digital System	A2.3	To identify all the components that will require forensic preservation and analysis, and produce an assessment of the methods and tools that will be required to retrieve the relevant records in a trustworthy way, maintaining the integrity of the system.

Seize Digital Storage Media	A2.4	To remove the physical or virtual digital storage media from the incident environment.
Process Digital System	A2.5	To preserve (isolate and protect) and duplicate the digital system and to secure the live digital system (if required).
Collect Relevant Digital Materials	A2.6	To identify, isolate, extract potential digital evidence from the incident environment.
Examine System	A2.6.1	To identify and document the physical and operational characteristics of a system in support of an investigation.
Search for Relevant Materials	A2.6.2	To use the techniques and tools necessary to locate the potential evidence from the incident environment.
Extract Relevant Materials	A2.6.3	To isolate, collect and protect the potential evidence in the incident environment.
Prepare Detailed Documentation	A2.6.4	To describe the physical scene, system information, magital materials maintenance information and the collected digital materials.
Analyze Digital Materials	A3	To prepare collected digital material for analysis, conduct the initial survey of prepared digital materials, extract digital evidence from digital materials, analyze results of the examination and reconstruct the events.
Prepare Collected Digital Materials for Analysis	A3.1	To conduct activities required to enable, handle and redact the digital materials.
Extract Digital Evidence from Digital Materials	A3.2	To select the data or data sets that will be used as digital evidence.
Extract Hidden Data	A3.2.1	To isolate, protect, and collect digital materials not evident in standard file structures.
Extract Visible Data	A3.2.2	To isolate, protect, and collect digital materials evident in standard file structures.
Apply Search Parameters	A3.2.3	To analysis or examine the extracted data using identified criteria for finding evidence.
Map File Timelines	A3.2.4	To align system clocks in order to account for any discrepancies with the local host.
Validate Extraction Strategy	A3.2.5	Self-explanatory.
Analyze Results of Examination	A3.3	To conduct a detailed assessment of the extracted digital materials with reference to the incident.
Determine Relevance of Extracted Digital Evidence	A3.3.1	To establish the probative value or lack thereof of the digital materials.
Analyze Relevant Elements of Extracted Digital Evidence	A3.3.2	To examine digital material that directly relates to the case
Create Hypotheses of Events	A3.3.3	To propose a sequence of events that align with the evidence.
Reconstruct Events	A3.4	To match the hypothesis which encapsulates an explanation of the incident with the extracted evidence.
Propose Event Reconstruction	A3.4.1	Self-explanatory.
Test Reconstruction of Events	A3.4.2	Self-explanatory.
Confirm/Refute Event Reconstruction	A3.4.3	To determine whether the hypotheses are supported or not by the evidence and its analysis.
Reach Conclusions	A4	To develop narrative of forensic process, integrate forensic and investigation process, and write conclusions of forensic and investigation process.

Develop Narrative of Forensic Process	A4.1	To outline the steps taken throughout the investigation.
Integrate Forensic and Investigation Processes	A4.2	To combine the results of all investigative activities in support of the on-going investigation.
Write Conclusions of Forensic and Investigation Processes	A4.3	Self-explanatory.
Submit Evidence Package	A5	To assess materials and conclusions, prepare submission package, submit the evidence package to appropriate legal authority, and exchange the evidence package with the other party(ies).
Determine Content of the Submission Package	A5.1	To determine whether the materials support the investigation and are sufficient to be included in the submission package.
Prepare Submission Package	A5.2	To gather the relevant material to be sent to the proper parties.
Submit Evidence Package to Appropriate Legal Authority	A5.3	Self-explanatory.
Exchange Evidence Package with Other Party	A5.4	To make disclosure between the parties.
Manage Case Materials	A6	To process case materials for storage, store case materials and return physical property to the owner.
Process Case Materials for Storage	A6.1	To make off-line copies of digital materials, to assemble non-digital materials, and to prepare case folder.
Make Offline Copies of Digital Materials	A6.1.1	To provide secure alternate access to the evidence.
Assemble Non-digital Materials	A6.1.2	To collect non-digital materials for preservation.
Prepare Case Folder	A6.1.3	To compile all investigative materials with indices and descriptions for storage.
Store Case Materials	A6.2	Self-explanatory.
Return Physical Property to Owner	A6.3	Self-explanatory.

Digital Records Forensics Model Arrow Definitions, May 13, 2011		
Arrow Name	Arrow Definition	Arrow Note
Analyzed Relevant Digital Evidence	Extracted materials appropriate for presentation as potential evidence.	
Assembled Non-digital Materials	Self-explanatory.	
Assessment of System	The determination of what needs to be done to extract and obtain custody of the relevant materials in a trustworthy way, maintaining the integrity of the system.	The assessment of the system may lead to the conclusion that there may be other systems to look at.
Authenticated Investigator-collected Digital Materials	These are the third party collected records that are authenticated by digital records forensics experts for submission to the courts.	
Case Folder	The aggregation of the evidence and supporting materials, created or collected in relation to a case.	
Collected Digital Materials	Relevant digital materials removed from the system.	
Complaint	Oral or written request to investigate an indicator.	
Description of Forensic Process	The articulation of the steps involved in carrying out the forensic component of the investigation.	
Description of Integration of Forensic and Investigation Processes	A representation of the combined results of all investigative activities in support of the on-going investigation.	
Detailed Documentation about Collected Digital Materials	Description of the process of searching the digital media, and collecting and securing the relevant digital materials.	Includes documentation about the digital materials' authentication and relevance (e.g., what has been done to collect the materials how the collected records have been modified (if relevant), etc.).
Determination to Abandon Investigation	Self-explanatory.	
Determination to not Proceed with the Investigation	A report indicating the reasons and decisions to terminate the investigation.	
Determination to Proceed with the Investigation	A report confirming the resources and indicating the grounds for continuing the investigation.	
Digital Forensics	The body of theory, methods and practice, developed and applied in the course of investigating digital evidence.	

Digital Forensics Experts	Professionals who have the knowledge and the qualifications to conduct digital forensic work.	Professionals who have knowledge in evidence law and procedure, digital recordkeeping systems, diplomatics, archival science, digital forensics and e-discovery systems. [this definition applies more directly to digital records forensics experts]
Digital Materials Maintenance Information	Documentation of any alterations made to the original format of the collected relevant materials.	
Digital Materials Prepared for Analysis	The product of preparation activities.	
Documentation of Collection Techniques	Description of the technologies and methods that will be employed in the extraction of digital materials.	
Documentation of Issues	A report on the potential problems and their mitigation areas in the forensic investigation of digital materials.	
Draft Investigation Plan	The identification of the stages of the investigation and of the resources needed for each in draft form.	
Duplicate of Submitted Evidence Package	Self-explanatory.	
Exhibits Released From the Court and Documentation	The records that have been used as exhibits in the court and the information about their technological characteristics and changes during the trial.	
Extracted Digital Evidence	The digital materials resulting from a successful extraction of potential evidence.	
Extracted Hidden Data	The isolated, protected, and collected digital materials not evident in standard file structures.	
Extracted Visible Data	The isolated, protected, and collected digital materials evident in standard file structures.	
Extraction Strategy	The methods and processes that will be used to obtain custody of the materials listed in the court order.	
Feedback Report	Comments and/or recommendations relevant the particular investigation or the overall analysis process to ensure that the analysis lifecycle is an effective beginning to end process.	
Findings	The outcomes of the investigation and analysis which maybe be conclusive, inconclusive.	

Findings of Forensic Process	Self-explanatory.	
Hypothesis of Events	A proposed reconstruction of the incident based on the evidence extracted.	The hypothesis might have been suggested from the investigator directly, from other persons or based on the physical evidence earlier.
Identified Irrelevant Elements of Extracted Digital Evidence	Extracted materials not appropriate for further analysis or presentation.	
Identified Relevant Elements of Extracted Digital Evidence	Self-explanatory.	
Image of System	The bit copy of all the digital media in the incident environment.	includes digital materials and applications
Indicator	Information about an unusual or suspicious activity.	
Instructions for Preparation of Submission Package	Self-explanatory.	
Integrated Findings	Self-explanatory.	
Investigation Plan	The identification of the stages of the investigation and of the resources needed for each.	
Investigator-collected Digital Records	The digital materials that have been acquired by the investigators from the third party in the initiation of an investigation.	
Investigator-created Digital Records	Supporting digital materials produced by the investigators in the course of the investigation within which the digital forensics process occurs.	
Investigators	Public or private individuals responsible for gathering evidence in regard to an occurrence as a result of a complaint or other indicator.	This includes investigators studying the physical as well as the digital crime scene.
Irrelevant Investigator-collected Digital Materials	The subset of digital materials that have been acquired by the investigators from a third party in the initiation of an investigation and will not be used in the application for a court order and in the remainder of the investigation.	This material may be returned to the third party.
Lawful Authority for Search and Seizure	The permission to secure the scene and search and remove evidence as given by the pertinent authority.	The authority maybe given by the courts, one of the parties, or other relevant persons as required.
Laws Governing Evidence	The concepts, rules and procedures that regulate proof of facts in a legal process.	
List of Authenticated Investigator-collected Digital Materials	Itemization of the materials collected from third parties that are authenticated by the investigators which support the application for a court order.	

List of Digital Materials to be Collected	An itemization of the relevant digital materials identified by the investigator to be collected for the purposes of supporting an investigation.	
List of Existing Materials to be Collected	Itemization of digital materials that will be extracted and presented as potential evidence.	
List of Files that Satisfy Search Parameters	A report of the extracted data satisfying the criteria.	
List of Privileged Records	An itemization of documents protected by legal-professional privilege from disclosure.	For example, correspondence passing between lawyers and clients relating to legal advice.
List of Relevant Investigator-created Records	An itemization of documentation created to support the investigation and application for the court order.	
Litigators	Lawyers, paralegals and other legal personnel who are involved in the conduct and presentation of disputes to court or other appropriate decision-making body.	This would include professional disciplinary bodies, tribunals, etc. who may be receiving this information (the result of the investigation)
Live Digital System	Running digital applications in the incident environment.	
Map of File Timelines	A report of clock synchronizations.	
Materials Associated with Abandoned Investigation	Self-explanatory.	
Materials Excluded from Submission Package	Self-explanatory.	
Materials to be Presented	Self-explanatory.	
National and International Standards	The de jure and de facto professional rules, guidelines and best practices that are relevant to the environment in which digital forensics is conducted.	This includes accepted principles, codes, models, ethics, habits, customs considered as authoritative, that digital investigators apply in the course of their work.
Non-authenticated Investigator-collected Digital Materials	The materials collected from third parties that could not be authenticated by the investigators.	
Offline Copies of Digital Materials	Self-explanatory.	
Organizational Framework	The organizational mandate, policies and regulations of the body responsible for conducting the digital forensics process.	

Physical Property Returned to Owner	Self-explanatory.	
Preserved Digital System	The isolated and protected digital system.	
Proposed Reconstruction of Events	Self-explanatory.	
Record of Physical Scene	Description of the incident environment as secured by the investigator.	An itemization and description of the computers, storage devices, peripherals, cabling, and their connection in the context in which they were found at the scene and other relevant materials.
Records Managers	Professionals responsible for the control and management of the creation, maintenance and record-keeping processes.	
Records of Other Party	Self-explanatory.	
Refuted Hypotheses Report	The description of the narrative chain of events inconsistent with the extracted digital evidence.	
Relevant Investigator-created Records	Documentation created to support the investigation and application for the court order.	
Report of Revised Extraction	Self-explanatory.	
Report on Forensic Process	Self-explanatory.	
Report on Test of Proposed Reconstruction of Events	Self-explanatory.	
Request for Additional Materials	Self-explanatory.	
Request to Rerun the Extraction Process	Self-explanatory.	
Request to Revise Extraction Strategy	Result of the evaluation of an unsuccessful extraction.	
Request to Revise Hypothesis of Events	The refuted hypothesis returned to the analysis phase for review and revision.	
Ressources	This includes personnel, financial, technological, and knowledge resources.	
Secured Live Digital System	Protected running digital applications in the incident environment.	
Secured scene	The incident environment after it has been protected from interference.	

Seized Digital Storage Media	The physical or virtual digital storage media which have been removed from the incident environment.	
Selected Relevant Investigator-collected Digital Materials	The subset of digital materials that have been acquired by the investigators from a third party in the initiation of an investigation and will be used in the application for a court order.	
Stored Case Materials	Self-explanatory.	
Submission Package	The collected evidence and supporting materials presented to the appropriate parties.	
Submitted Evidence Package	The collected evidence presented to the appropriate parties.	
Supported Hypothesis of Events	Self-explanatory.	
System Information	Information about the physical and operational characteristics of the system examined in support of an investigation.	
Techniques for Collecting Digital Materials	Self-explanatory.	
Tools for Collecting Digital Materials	The technologies that may be used to extract digital materials.	The technologies chosen will be refined in subsequent steps - see A1.2.3
Tools, Equipment and Facilities	The technologies and environment required to carry out all the activities involved in conducting digital forensics.	