Framework Penyidikan Forensik Digital

Definisi *forensics*

- “belonging to, used in, or suitable to courts of judicature or to public discussion and debate a lawyer's forensic skills” (Merriam Webster)
- “relating to or dealing with the application of scientific knowledge to legal problems” (Merriam Webster)
- — **forensically** adverb
- Forensically sound

Locard's Exchange Principle:

"Every contact leaves a trace"

(Prof. Edmond Locard, 1910)

Apa itu “Digital”

- Perangkat digital adalah perangkat binary yang menyimpan informasi sebagai kombinasi 0 dan 1
- Komputer adalah istilah umum
  - Laptop, desktop, server
  - Router, switch, perangkat jaringan lainnya
  - Mobile devices, kamera digital, iPOD, tablet
  - Printer

Apa itu Science?

- Scientific method: *“principles and procedures for the systematic pursuit of knowledge involving the recognition and formulation of a* ***problem****, the* ***collection*** *of data through* ***observation*** *and* ***experiment****, and the formulation and* ***testing*** *of hypotheses”* (Merriam Webster)
- Digital forensics menggunakan scientific method sebagai pedoman untuk:
  - Menemukan informasi
  - Menganalisis informasi

Permainan simpan angka

- $x<>0$; x elemen bilangan Real

Proses Forensik

- Proses dasar dalam forensics:
  - Identification
  - Preservation
  - Analysis
  - Presentation
- Hubungan antara penyidikan digital dan penyidikan physical
- Istilah bukti digital:
  - Barang bukti
  - Alat bukti
  - Bukti digital **potensial**

Isu Hukum dan Etika

- Admissibility of scientific evidence
- Locard Exchange principle (1910)
- Frye v. U.S (1923) adalah acuan pertama untuk penerimaan scientific evidence di pengadilan U.S.
  - *"Where novel scientific evidence is at issue, the Frye inquiry allows the judiciary to defer to scientific expertise precisely as to whether or not it has gained "general acceptance" in the relevant field. The trial courts' gatekeeper role in this respect is conservative, thus helping to keep "pseudoscience" out if the courtroom"*

- Daubert v. Merrell Dow (1993) – Daubert Test
  - Acuan baru untuk menentukan standar untuk menerima scientific evidence: evidentiary reliability
  - Empat panduan:
    - ***Testing***: Dapatkan dan sudahkan prosedur tersebut ditest?
    - ***Publication***: Sudahkan prosedur tersebut dipublikasikan dan direview?
    - ***Error Rate***: Apakah error rate dari prosedur tersebut dapat diketahui?
    - ***Acceptance***: Apakah prosedur tersebut telah secara umum diterima oleh komunitas science?

ACPO Good Practice Guide for Digital Evidence

THE PRINCIPLES OF DIGITAL EVIDENCE

Principle 1: ***No*** action taken by law enforcement agencies, persons employed within those agencies or their agents should ***change data*** which may subsequently be relied upon in court.

Principle 2: In circumstances where a person finds it necessary to access original data, that ***person*** must be ***competent*** to do so and be able to give evidence ***explaining*** the relevance and the implications of their ***actions***.

Principle 3: An audit trail or other ***record*** of all processes applied to digital evidence should be created and preserved. An independent ***third party*** should be able to ***examine*** those processes and achieve ***the same result***.

Principle 4: The person in charge of the investigation has overall ***responsibility*** for ensuring that the ***law*** and these principles are adhered to.

Frameworks and process models

- A framework for digital forensic investigations is needed to manage the investigation process and to ensure that the process is conducted in a forensically-sound manner

- This is needed to ensure the digital forensic process transparent and to maintain the original data for trial in a court (McKemmish 2008)

- This forensically-sound process is also required to ensure that results are reproducible by other parties if they have doubts.

Frameworks of digital forensic investigations

No	Model	Proposed by	Computer forensics	Network forensics	Mobile forensics	Cloud forensics
1	Computer forensics process	Pollitt (1995)	√			
2	Four key elements of forensic computing Identification, Preservation, Analysis, Presentation	McKemmish (1999)	√	√	√	
3	Electronic crime scene investigation: a guide for first responders Preparation, Recognition and Identification, Documentation of the crime scene, Collection and Preservation, Packaging and Transportation, Examination, Analysis, and Reporting	National Institute of Justice (2001)	√	√	√	
4	Investigative process for digital forensic science	Palmer (2001)	√	√		
5	An abstract digital forensics model Identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence.	Reith, Carr and Gunsch (2002)	√	√	√	√

No	Model	Proposed by	Computer forensics	Network forensics	Mobile forensics	Cloud forensics
6	An integrated digital investigation process 17 processes organized into the following five groups: Readiness processes, Deployment processes, Physical crime scene investigation processes, Digital crime scene investigation processes, and Review process	Carrier and Spafford (2003)	√	√	√	
7	Incident response methodology	Prosise and Mandia (2003)	√	√		
8	End-to-end digital investigation	Stephenson (2003)	√	√		
9	Investigative process model Iterative processes	Casey and Palmer (2004)	√	√		
10	An extended model of cybercrime investigations	Ciardhuáin (2004)	√	√		
11	The enhanced digital investigation process model	Baryamureeba and Tushabe (2004)	√	√	√	
12	The general process of network forensics	Ren and Jin (2005)		√		
13	A hierarchical, objectives-based framework for the digital investigations process	Beebe and Clark (2005)	√	√		

No	Model	Proposed by	Computer forensics	Network forensics	Mobile forensics	Cloud forensics
14	Computer forensics field triage process model	Rogers et al. (2006)	√	√	√	
15	Forensic process	Kent et al. (2006)	√	√	√	
16	Framework for a digital forensic investigation	Köhn, Olivier and Eloff (2006)	√			
17	Digital forensics investigation framework	Ieong (2006)	√	√		
18	A common process model for incident response and digital forensics	Freiling and Schwittay (2007)	√			
19	Windows mobile forensic process model	Ramabhadran (2007)			√	
20	Digital forensic investigation framework	Selamat, Yusof and Sahib (2008)	√	√	√	
21	Two-dimensional evidence reliability amplification process	Khatir, Hejazi and Sneiders (2008)	√	√		
22	A new forensic model of a memory dump	Kiltz, Hoppe and Dittmann (2009)	√	√		
23	Digital forensic model based on Malaysian investigation process	Perumal (2009)	√	√		
24	Cellular phone evidence extraction process	Murphy (2009)			√	

No	Model	Proposed by	Computer forensics	Network forensics	Mobile forensics	Cloud forensics
25	Symbian smartphones forensic process model	Yu et al. (2009)			√	
26	The generic process model for network forensics	Pilli, Joshi and Niyogi (2010)		√		
27	The cybercrime investigations	Hunton (2010)	√	√		
28	Framework for iPhone forensic analysis	Husain, Baggili and Sridhar (2011)			√	
29	Triaging in mobile forensics	Marturana et al. (2011)			√	
30	Digital evidence forensics standard operating procedure	Lin, Chao and Peng (2011)			√	
31	Systematic digital forensic investigation model	Agarwal et al. (2011)	√	√	√	
32	Digital forensic model for digital forensic investigation	Ademu, Imafidon and Preston (2011)	√	√	√	
33	Generic computer forensic investigation model	Yusoff, Y, Ismail and Hassan (2011)	√			
34	Framework of digital forensics for the Samsung star series phone	Parvez, Dehghantanha and Broujerdi (2011)			√	
35	Digital forensics process of smartphone devices	Alghafli, Jones and Martin (2011)			√	
36	Cybercrime investigation procedure	Shin (2011)	√	√		

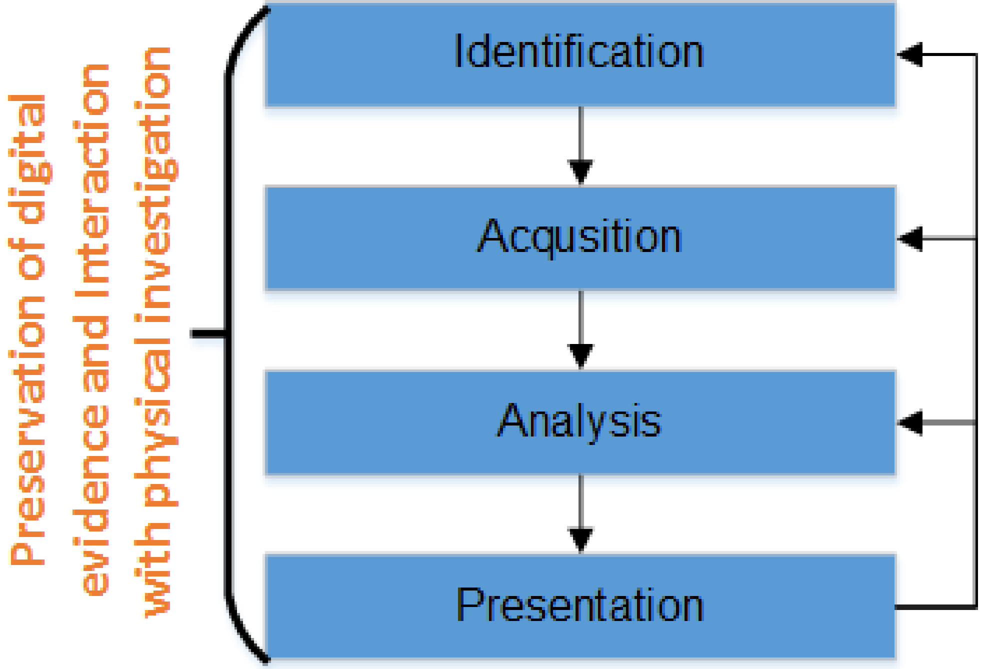
No	Model	Proposed by	Computer forensics	Network forensics	Mobile forensics	Cloud forensics
37	An integrated conceptual digital forensic framework for cloud computing	Martini and Choo (2012)				√
38	A proactive investigation scheme For evidence acquisition	Mylonas et al. (2012)			√	
39	Improved mobile forensics model	Shah and Bansal (2012)			√	
40	Smartphone forensic investigation process model	Goel, Tyagi and Agarwal (2012)			√	√
41	Platform independent process model for smartphones	Dancer et al. (2013)			√	
42	Advances of mobile forensic procedures in Firefox OS	Yusoff, MN et al. (2014)			√	
43	Guidelines on mobile device forensics Identification, Preservation, Acquisition, Examination and Analysis, Reporting	Ayers, Brothers and Jansen (2014)			√	
44	The extended abstract digital forensic model with 2pasu	Saleem, Popov and Bagilli (2014)	√	√	√	√
45	Harmonized digital investigation process Readiness, Initialization, Acquisition, Investigative	ISO/IEC (2015)	√	√	√	√
46	Digital forensics laboratory process model	Hájek et al. (2015)	√			

No	Model	Proposed by	Computer forensics	Network forensics	Mobile forensics	Cloud forensics
47	Domain specific cyber forensics investigation process model	Satti and Jafari (2015)	√	√		
48	Android cache taxonomy and forensic process	Immanuel, Martini and Choo (2015)			√	
49	Evidence collection and analysis methodology for android devices	Martini, Do and Choo (2015b)			√	
50	ANDROPHSY - forensic framework for Android	Akarawita, Perera and Atukorale (2015)			√	
51	Mobile forensic investigation	Rajendran and Gopalan (2016)			√	
52	Mobile forensics model	Sadiq et al. (2016)			√	
53	Tiered forensic methodology model for digital field triage by non-digital evidence specialists	Hitchcock, Le-Khac and Scanlon (2016)	√	√	√	
54	Multidisciplinary digital forensic investigation process model	Lutui (2016)	√	√	√	√
55	Integrated digital forensics investigation framework	Ruuhwan and Prayudi (2017)	√		√	

Tahapan Umum dalam Forensik Digital

- Identification
- Preservation
- Analysis
- Presentation

Case Specific Process Model



Preservation of digital evidence and Interaction with physical investigation

Identification

Acqusition

Analysis

Presentation

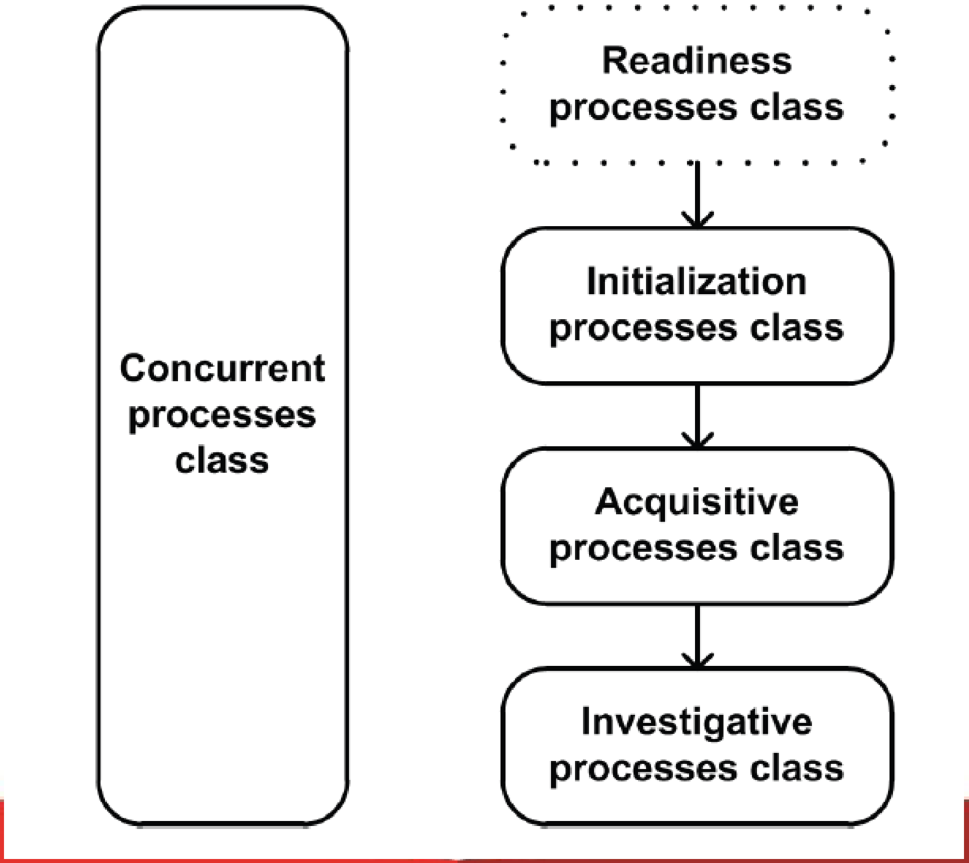
The high-level abstraction of the proposed process model for Windows Phone 8 forensics

Comparison with other Frameworks

WP Process Model	McKemmish framework	ISO/IEC 27043:2015	NIST guidelines on mobile device forensics
–	–	1. Readiness	–
1. Identification	1. Identification	2. Initialization	1. Identification of mobile device and mobile forensic tools*)
2. Acquisition	2. Preservation 3. Analysis	3. Acquisitive	2. Preservation 3. Acquisition
3. Analysis		4. Investigative	4. Examination and analysis
4. Presentation	4. Presentation		5. Reporting

ISO-IEC 27043:2015

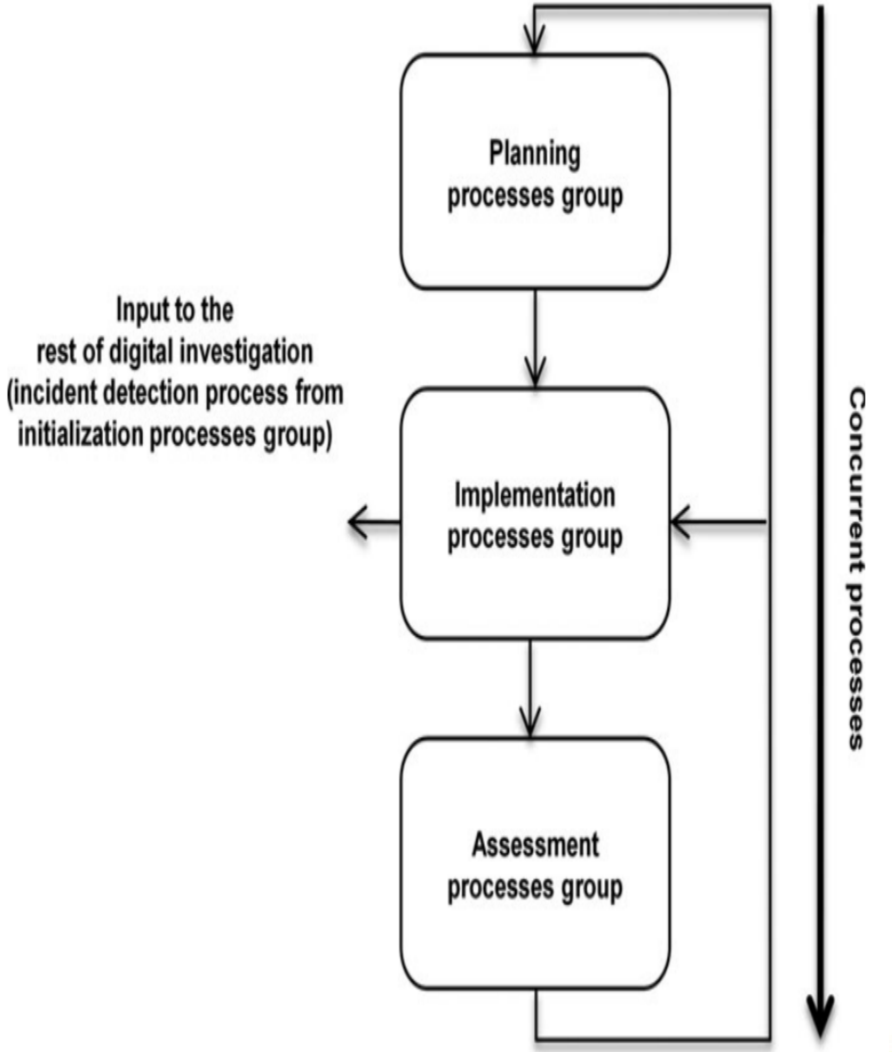
The various classes of digital investigation processes


Concurrent processes class
Readiness processes class
Initialization processes class
Acquisitive processes class
Investigative processes class

Valjarevic & Venter (2015), p.1470

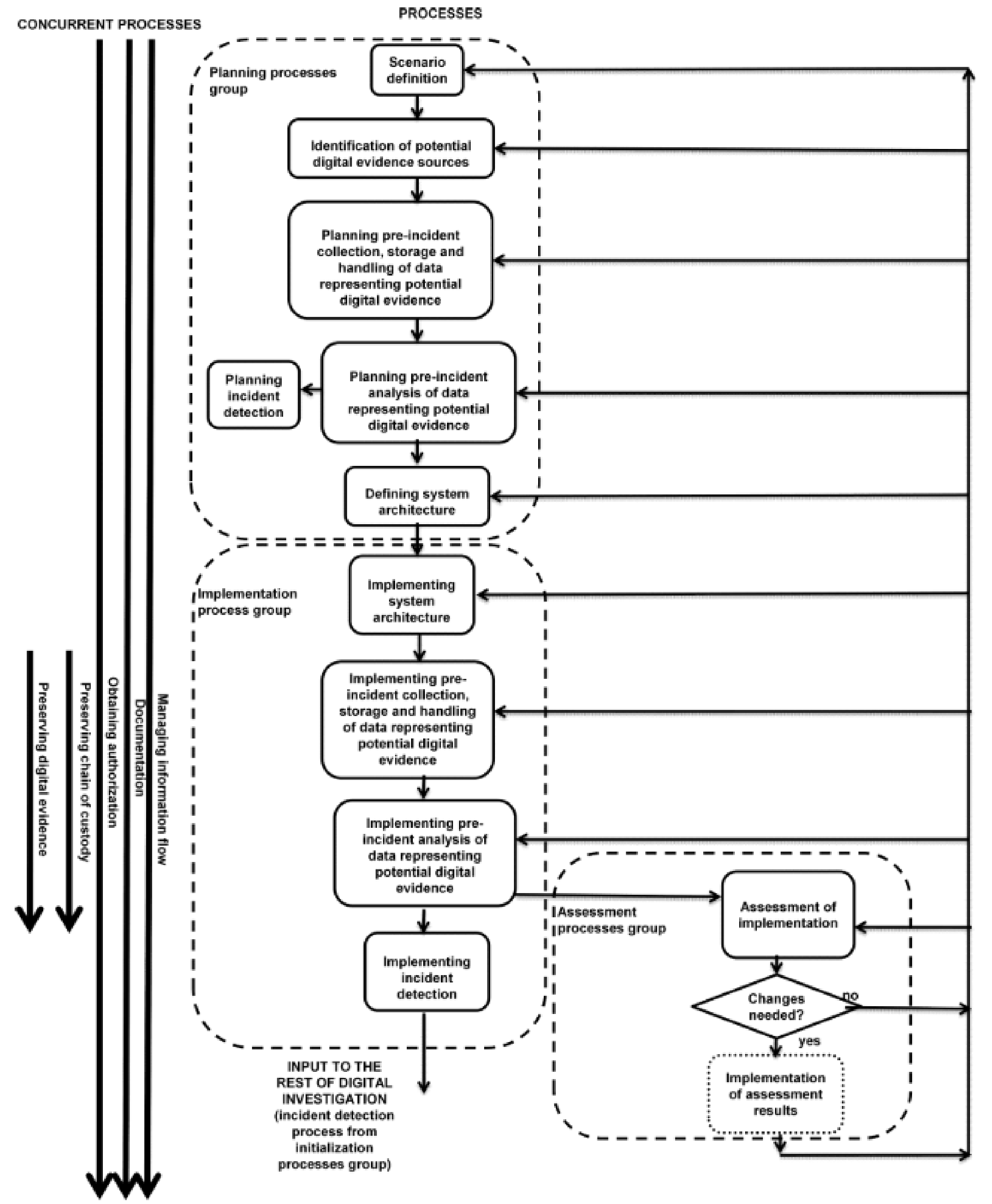
Readiness Proces

- Optional
- Setting up an organization
- In the case that a digital investigation is required
- The aims:
  - maximize the potential use of potential digital evidence,
  - minimize the costs of the investigation
  - minimize interference with and prevent the interruption of business processes
  - preserve or improve the current level of information systems security.
- Consist of 3 iterative processes



Valjarevic & Venter (2015), p.1471

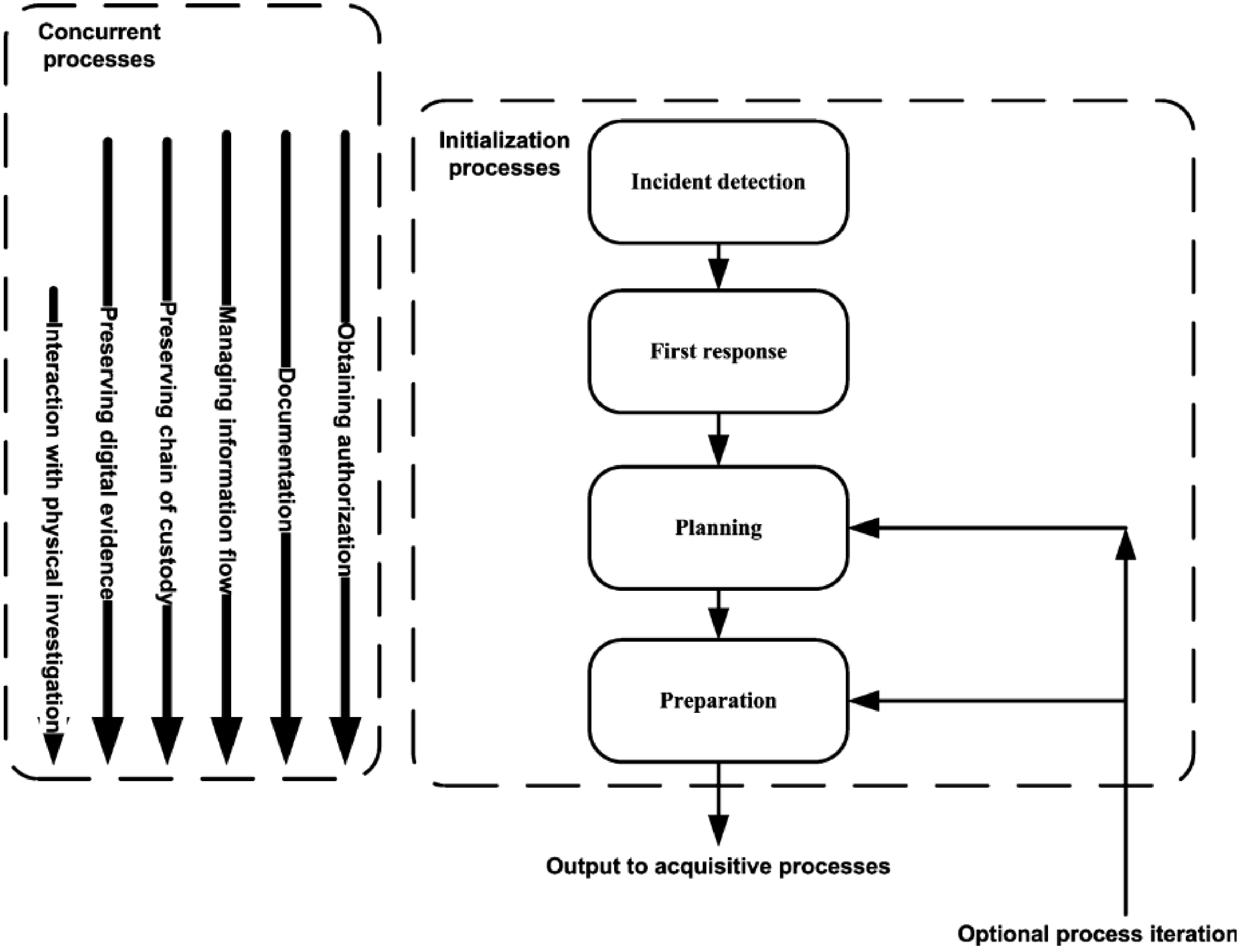
- Planning activities:
  - Scenario definition – Risk Assessment
  - Identification of potential digital evidence
  - Planning pre-incident gathering
  - Storage and handling of data representing potential digital evidence
  - Planning incident detection
  - Defining system architecture
- Implementing activities: Implementation of the plan
- Assessment activities:
  - Assessment of the implementation
  - Implementation of the assessment results


CONCURRENT PROCESSES
PROCESSES
Planning processes group
Scenario definition
Identification of potential digital evidence sources
Planning pre-incident collection, storage and handling of data representing potential digital evidence
Planning incident detection
Planning pre-incident analysis of data representing potential digital evidence
Defining system architecture
Implementation process group
Implementing system architecture
Implementing pre-incident collection, storage and handling of data representing potential digital evidence
Implementing pre-incident analysis of data representing potential digital evidence
Implementing incident detection
Assessment processes group
Assessment of implementation
Changes needed?
no
yes
Implementation of assessment results
INPUT TO THE REST OF DIGITAL INVESTIGATION (incident detection process from initialization processes group)
Preserving digital evidence
Preserving chain of custody
Obtaining authorization
Documentation
Managing information flow

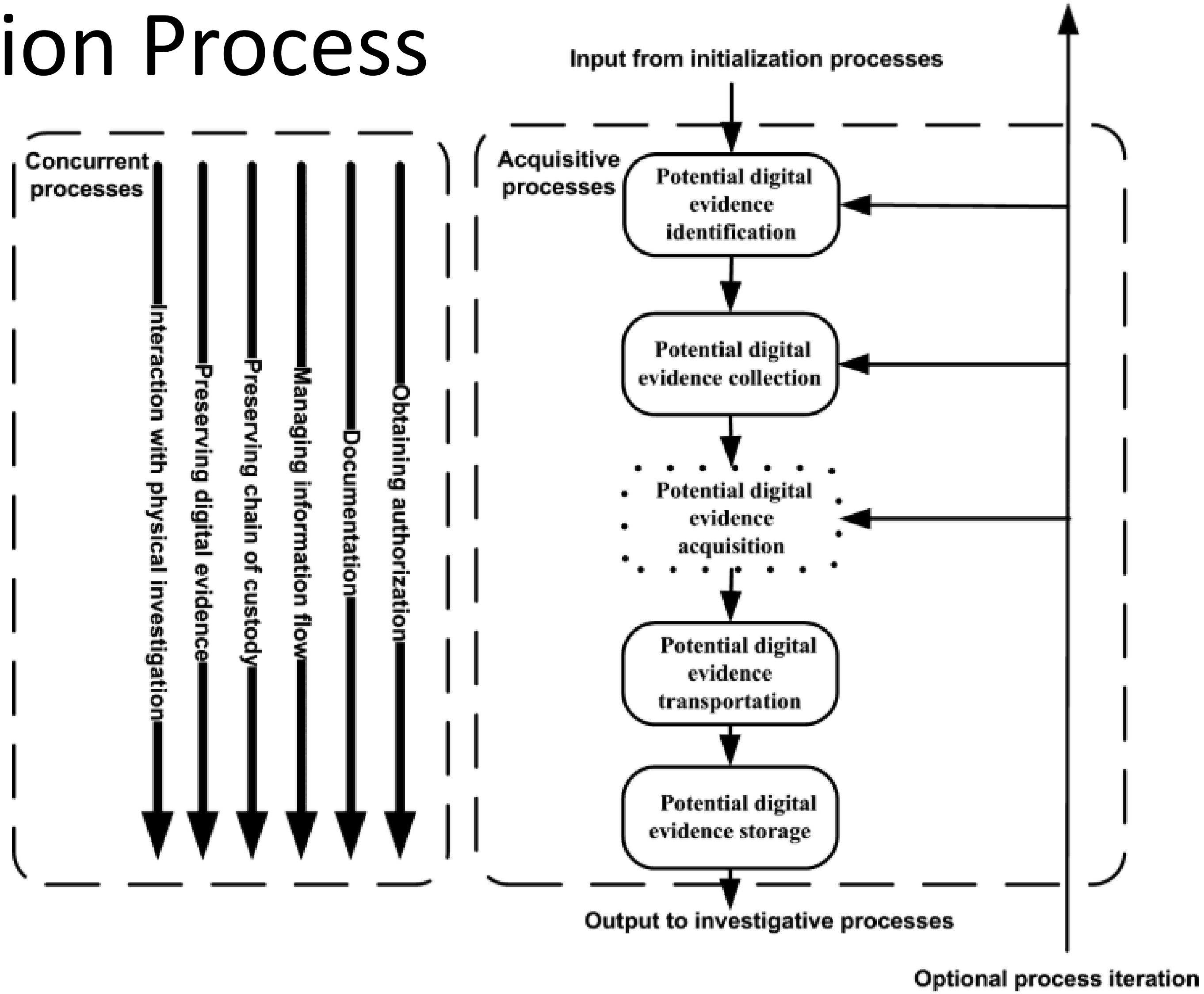
Valjarevic & Venter (2015), p.1472

Initialization Process

- Incident detection
  - Detection
  - Classification
  - Description
  - This process will have a significant influence on the rest of the process
    - ‘unauthorized access to the root account of the operating system’, versus ‘using the computer to distribute abusive images’
- First response
  - To ensure integrity of digital evidence
- Planning and preparation processes
  - To determines the efficiency and success of all the other processes


Concurrent processes
Interaction with physical investigation
Preserving digital evidence
Preserving chain of custody
Managing information flow
Documentation
Obtaining authorization
Initialization processes
Incident detection
First response
Planning
Preparation
Output to acquisitive processes
Optional process iteration

Acquisition Process



Input from initialization processes

Concurrent processes

Interaction with physical investigation

Preserving digital evidence

Preserving chain of custody

Managing information flow

Documentation

Obtaining authorization

Acquisitive processes

Potential digital evidence identification

Potential digital evidence collection

Potential digital evidence acquisition

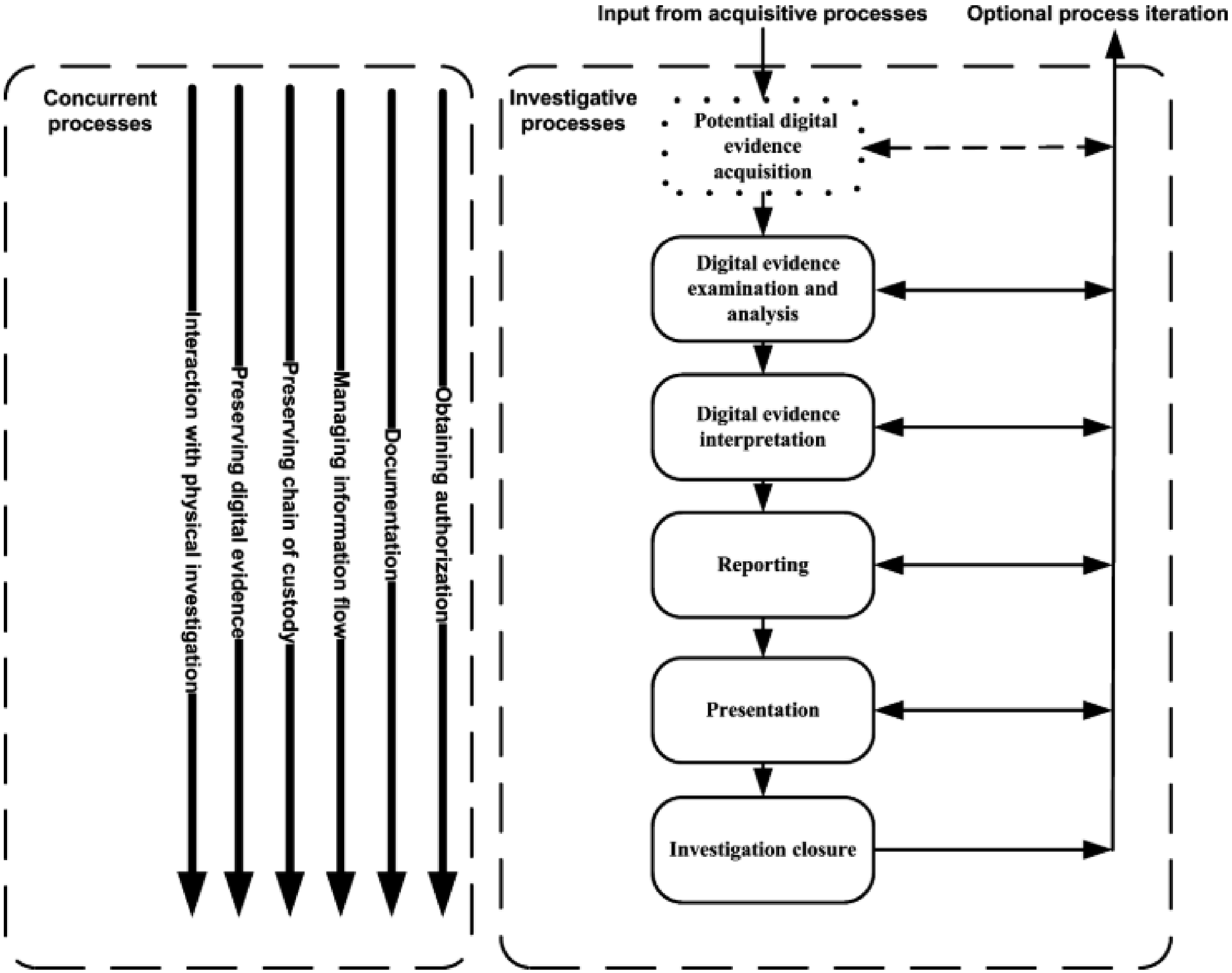
Potential digital evidence transportation

Potential digital evidence storage

Output to investigative processes

Optional process iteration

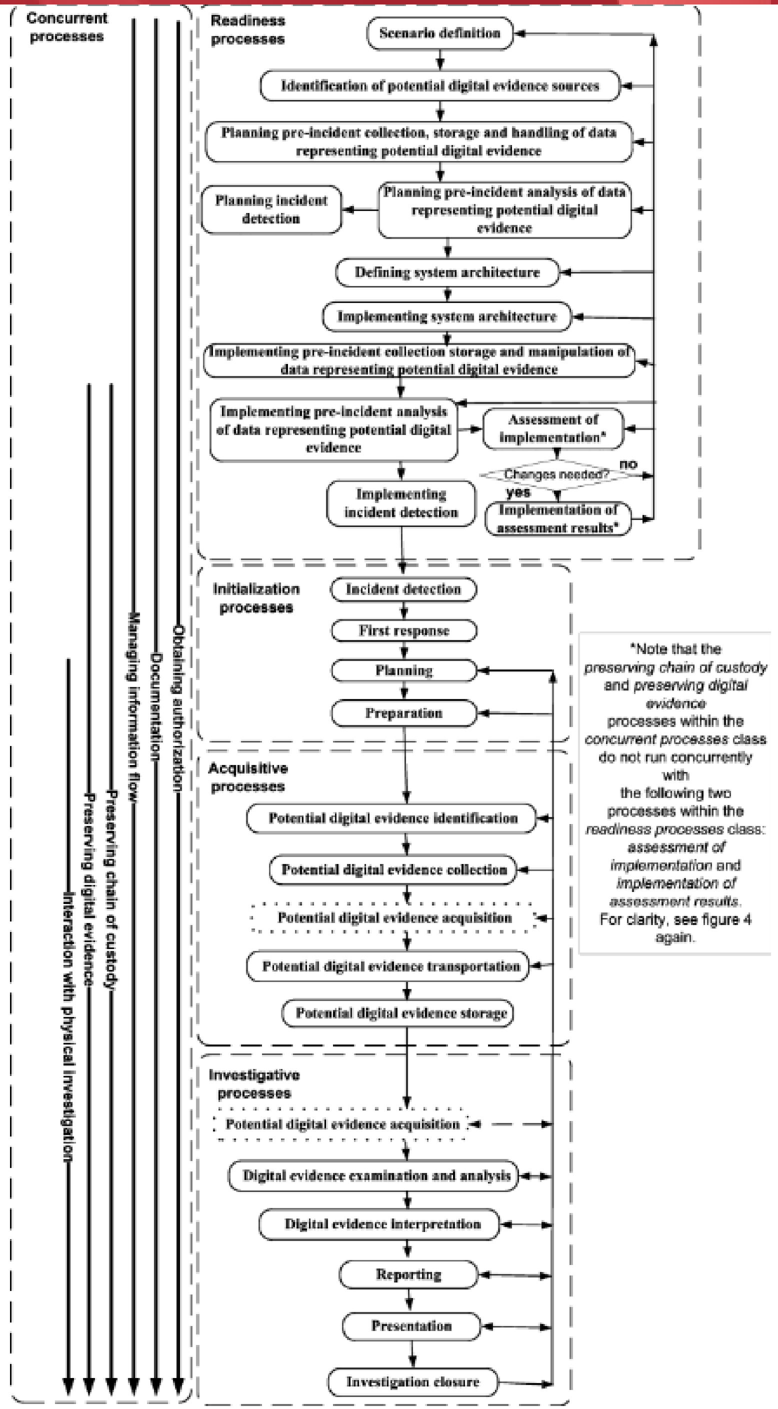
Investigative Process


Input from acquisitive processes
Optional process iteration
Concurrent processes
Interaction with physical investigation
Preserving digital evidence
Preserving chain of custody
Managing information flow
Documentation
Obtaining authorization
Investigative processes
Potential digital evidence acquisition
Digital evidence examination and analysis
Digital evidence interpretation
Reporting
Presentation
Investigation closure

Concurrent Processes

- Obtaining authorization
  - From government authorities, system owners, system custodians, principals, users, etc
  - Not to infringe on rights and legal rules
- Documentation
  - Proper documentation in the
  - Preserve the chain of custody
- Defining the information flow
  - Information exchange between two investigators?
  - Using digital signature?
- Preserving the chain of custody
- Preserving digital evidence
  - Strict procedures from the incident is detected until the investigation is closed
- Interaction with the physical investigation

The Completed Processes



Concurrent processes

Obtaining authorization

Documentation

Managing information flow

Preserving chain of custody

Preserving digital evidence

Interaction with physical investigation

Readiness processes

Scenario definition

Identification of potential digital evidence sources

Planning pre-incident collection, storage and handling of data representing potential digital evidence

Planning incident detection

Planning pre-incident analysis of data representing potential digital evidence

Defining system architecture

Implementing system architecture

Implementing pre-incident collection storage and manipulation of data representing potential digital evidence

Implementing pre-incident analysis of data representing potential digital evidence

Assessment of implementation*

Changes needed?

no

yes

Implementing incident detection

Implementation of assessment results*

Initialization processes

Incident detection

First response

Planning

Preparation

Acquisitive processes

Potential digital evidence identification

Potential digital evidence collection

Potential digital evidence acquisition

Potential digital evidence transportation

Potential digital evidence storage

Investigative processes

Potential digital evidence acquisition

Digital evidence examination and analysis

Digital evidence interpretation

Reporting

Presentation

Investigation closure

*Note that the *preserving chain of custody* and *preserving digital evidence* processes within the *concurrent processes* class do not run concurrently with the following two processes within the *readiness processes* class: *assessment of implementation* and *implementation of assessment results*. For clarity, see figure 4 again.

Valjarevic & Venter (2015), p.1480

References

- Handbook of Digital Forensics and Investigation, Eoghan Casey
- File System Forensic Analysis, Brian Carrier
- ISO-IEC 27043:2015
- NIST guidelines on mobile device forensics
- McKemmish, “What is forensic computing?”, 1999.

THANK YOU