

Lampiran 1: Tahapan IDFIF dan DFIF untuk *smartphone investigation*

No.	Nama Framework	Tahapan Utama		Sub Tahapan		Σ Tahapan
		Urutan	Nama Tahapan	Urutan	Nama Tahapan	
1	<i>Windows Mobile Device Forensics Model (WMDFM)</i>	1	<i>Preparation</i>	-	-	12
		2	<i>Securing the scene</i>	-	-	
		3	<i>Survey and Recognition</i>	-	-	
		4	<i>Documenting the scene</i>	-	-	
		5	<i>Communication shielding</i>	-	-	
		6	<i>Volatile Evidence Collection</i>	-	-	
		7	<i>Non-Volatile Evidence Collection</i>	-	-	
		8	<i>Preservation</i>	-	-	
		9	<i>Examination</i>	-	-	
		10	<i>Analysis</i>	-	-	
		11	<i>Presentation</i>	-	-	
		12	<i>Review</i>	-	-	
2	<i>Symbian Smartphones Forensics Process Model (SSFPM)</i>	1	<i>Preparation and identification</i>	-	-	6
		2	<i>Acquicition</i>	2.1	<i>Remote evidence acquisition</i>	
				2.2	<i>Internal evidence acquisition</i>	
		3	<i>Analysis</i>	-	-	
		4	<i>Presentation and review</i>	-	-	

Lanjutan lampiran 1: Tahapan IDFIF dan DFIF untuk *smartphone investigation*

No.	Nama Framework	Tahapan Utama		Sub Tahapan		Σ Tahapan		
		Urutan	Nama Tahapan	Urutan	Nama Tahapan			
3	ACPO <i>Smartphone Forensic Investigation</i>	1	<i>Preparation</i>	-	-	10		
		2	<i>Securing the scene</i>	-	-			
		3	<i>PDA mode</i>	-	-			
		4	<i>Documentation</i>	-	-			
		5	<i>Report writing</i>	-	-			
		6	<i>Communication shielding</i>	-	-			
		7	<i>Package</i>	-	-			
		8	<i>Seize</i>	-	-			
		9	<i>Plug in portable power supply</i>	-	-			
		10	<i>examination</i>	-	-			
4	<i>Smartphone Forensics Investigation Process Model (SFIPM)</i>	1	<i>Preparation and securing the scene</i>	-	-	13		
		2	<i>Documentation</i>	-	-			
		3	<i>PDA mode</i>	-	-			
		4	<i>Communication shielding</i>	-	-			
		5	<i>Evidence collcetion</i>	5.1	<i>Volatile memory</i>			
				5.2	<i>Non-Volatile memory</i>			
				5.2	<i>Off-Set/Cloud memory</i>			
		6	<i>Preservation</i>	-	-			
		7	<i>Examination</i>	-	-			
		8	<i>Analysis</i>	-	-			
9	<i>Presentation</i>	-	-					
10	<i>Review</i>	-	-					

Lanjutan lampiran 1: Tahapan IDFIF dan DFIF untuk *smartphone investigation*

No.	Nama Framework	Tahapan Utama		Sub Tahapan		Σ Tahapan
		Urutan	Nama Tahapan	Urutan	Nama Tahapan	
5	ISO/IEC 27041 <i>Smartphone Investigation</i>	1	<i>Incident detection</i>	-	-	12
		2	<i>First response</i>	-	-	
		3	<i>Planning</i>	-	-	
		4	<i>Preparation</i>	-	-	
		5	<i>Incident scene documentation</i>	-	-	
		6	<i>Potential digital evidence identification</i>	-	-	
		7	<i>Communication shielding</i>	-	-	
		8	<i>Digital evidence acquisition</i>	-	-	
		9	<i>Digital evidence transportation</i>	-	-	
		10	<i>Digital evidence storage</i>	-	-	
		11	<i>Digital evidence analysis</i>	-	-	
		12	<i>Report writing</i>	-	-	
6	NIST <i>Smartphone Forensic Investigation</i>	1	<i>Preservation</i>	1.1	<i>Securing and evaluation the scene</i>	9
				1.2	<i>Documentation the scene</i>	
				1.3	<i>Isolation</i>	
				1.4	<i>Packaging, transportation and storing evidence</i>	
				1.5	<i>Triage processing</i>	

Lanjutan lampiran 1: Tahapan IDFIF dan DFIF untuk *smartphone investigation*

No.	Nama Framework	Tahapan Utama		Sub Tahapan		Σ Tahapan
		Urutan	Nama Tahapan	Urutan	Nama Tahapan	
		2	<i>Acquicition</i>	-	-	
		3	<i>Examination and analysis</i>	-	-	
		4	<i>Reporting</i>	-	-	
7	<i>Harmonised Digital Forensic Investigation Process (HDFIP)</i>	1	<i>Initialization processes</i>	1.1	<i>Incident Detection</i>	18
				1.2	<i>First Response</i>	
				1.3	<i>Planning</i>	
				1.4	<i>Preparation</i>	
		2	<i>Acquicition processes</i>	2.1	<i>Potential digital evidence identification</i>	
				2.2	<i>Potential digital evidence collection</i>	
				2.3	<i>Potrntial digital evidence acquicition</i>	
				2.4	<i>Potential digital evidence transportation</i>	
				2.5	<i>Potential digital evidence storage and preservation</i>	
		3	<i>Investigation processes</i>	3.1	<i>Potential digital evidence acquicition</i>	
				3.2	<i>Digital evidence examination and analysis</i>	

Lanjutan lampiran 1: Tahapan IDFIF dan DFIF untuk *smartphone investigation*

No.	Nama Framework	Tahapan Utama		Sub Tahapan		Σ Tahapan
		Urutan	Nama Tahapan	Urutan	Nama Tahapan	
				3.3	<i>Digital evidence interpretation</i>	
				3.4	<i>Reporting</i>	
				3.5	<i>Presentation</i>	
				3.6	<i>Investigation closure</i>	
8	<i>Integrated Digital Forensic Investigation Framework (IDFIF)</i>	1	<i>Pre-Process</i>	1.1	<i>Notification</i>	30
				1.2	<i>Authorization</i>	
				1.3	<i>Preparation</i>	
		2	<i>Proactive Process</i>	2.1	<i>Proactive collection</i>	
				2.1.1	<i>Incident response volatile collection and collection of network traces</i>	
				2.2	<i>Crime scene investigation</i>	
				2.2.1	<i>Event triggering function and communication shielding</i>	
				2.2.2	<i>Documenting the scene</i>	
				2.3	<i>Proactive preservation</i>	
				2.4	<i>Proactive analysis</i>	

Lanjutan lampiran 1: Tahapan IDFIF dan DFIF untuk *smartphone investigation*

No.	Nama Framework	Tahapan Utama		Sub Tahapan		Σ Tahapan
		Urutan	Nama Tahapan	Urutan	Nama Tahapan	
				2.5	<i>Preminary report</i>	
				2.6	<i>Securing the scene</i>	
				2.7	<i>Detection of incident/ crime</i>	
		3	<i>Reactive Process</i>	3.1	<i>Identification</i>	
				3.1.1	<i>Survey</i>	
				3.1.2	<i>Recognition</i>	
				3.2	<i>Colection and acqicition</i>	
				3.3	<i>Preservation</i>	
				3.3.1	<i>Transportation</i>	
				3.3.2	<i>Storage</i>	
				3.4	<i>Examination</i>	
				3.5	<i>Analysis</i>	
				3.6	<i>Presentation</i>	
		4	<i>Post-Process</i>	4.1	<i>Conclusion</i>	
				4.2	<i>Recontruction</i>	
				4.3	<i>Dissemination</i>	

Lampiran 2: Pemberian ID pada setiap tahapan IDFIF dan DFIF untuk *smartphone investigation*

No.	Nama Framework	Nama Tahapan	ID
1	WMDFM	<i>Preparation</i>	1
		<i>Securing the scene</i>	2
		<i>Survey</i>	3
		<i>Recognition</i>	4
		<i>Documenting the scene</i>	5
		<i>Communication shielding</i>	6
		<i>Volatile Evidence Collection</i>	7
		<i>Non-Volatile Evidence Collection</i>	8
		<i>Preservation</i>	9
		<i>Examination</i>	10
		<i>Analysis</i>	11
		<i>Presentation</i>	12
		<i>Review</i>	13
2	SSFPM	<i>Preparation</i>	1
		<i>Identification</i>	14
		<i>Acquicition</i>	15
		<i>Remote evidence acquicition</i>	16
		<i>Internal evidence acquicition</i>	17
		<i>Analysis</i>	11
		<i>Presentation</i>	12
		<i>Review</i>	13
3	ACPO	<i>Preparation</i>	1
		<i>Securing the scene</i>	2
		<i>PDA mode</i>	18
		<i>Documentation</i>	19
		<i>Report writing</i>	20
		<i>Communication shielding</i>	6
		<i>Package</i>	21
		<i>Seize</i>	22
		<i>Plug in portable power supply</i>	23
		<i>Examination</i>	10
4	SFIPM	<i>Preparation</i>	1
		<i>Securing the scene</i>	2
		<i>Documentation</i>	19
		<i>PDA mode</i>	18
		<i>Communication shielding</i>	6
		<i>Evidence collction</i>	24
		<i>Volatile memory</i>	25
		<i>Non-Volatile memory</i>	26
		<i>Off-Set/Cloud memory</i>	27
		<i>Preservation</i>	9
		<i>Examination</i>	10
		<i>Analysis</i>	11
		<i>Presentation</i>	12
<i>Review</i>	13		

Lanjutan lampiran 2: Pemberian ID pada setiap tahapan IDFIF dan DFIF untuk *smartphone investigation*

<b>No.</b>	<b>Nama Framework</b>	<b>Nama Tahapan</b>	<b>ID</b>
5	ISO/IEC 27041	<i>Incident detection</i>	28
		<i>First response</i>	29
		<i>Planning</i>	30
		<i>Preparation</i>	1
		<i>Incident scene documentation</i>	31
		<i>Potential digital evidence identification</i>	32
		<i>Communication shielding</i>	6
		<i>Digital evidence acquisition</i>	33
		<i>Digital evidence transportation</i>	34
		<i>Digital evidence storage</i>	35
		<i>Digital evidence analysis</i>	36
		<i>Report writing</i>	20
6	NIST	<i>Preservation</i>	9
		<i>Securing the scene</i>	2
		<i>Evaluation the scene</i>	37
		<i>Documentation the scene</i>	5
		<i>Isolation</i>	38
		<i>Packaging</i>	39
		<i>Transportation</i>	40
		<i>Storing evidence</i>	41
		<i>Triage processing</i>	42
		<i>Acquisition</i>	15
		<i>Examination</i>	10
		<i>Analysis</i>	11
		<i>Reporting</i>	43
7	HDFIP	<i>Initialization processes</i>	44
		<i>Incident Detection</i>	28
		<i>First Response</i>	29
		<i>Planning</i>	30
		<i>Preparation</i>	1
		<i>Acquisition processes</i>	45
		<i>Potential digital evidence identification</i>	32
		<i>Potential digital evidence collection</i>	46
		<i>Potrntial digital evidence acquisition</i>	47
		<i>Potential digital evidence transportation</i>	48
		<i>Potential digital evidence storage</i>	49
		<i>Potential digital evidence preservation</i>	50
		<i>Investigation processes</i>	51
		<i>Potential digital evidence acquisition</i>	47
		<i>Digital evidence examination</i>	52
		<i>Digital evidence analysis</i>	36
		<i>Digital evidence interpretation</i>	53
<i>Reporting</i>	43		
<i>Presentation</i>	12		
<i>Investigation closure</i>	54		



Lanjutan lampiran 2: Pemberian ID pada setiap tahapan IDFIF dan DFIF untuk *smartphone investigation*

<b>No.</b>	<b>Nama Framework</b>	<b>Nama Tahapan</b>	<b>ID</b>
8	IDFIF	<i>Pre-Process</i>	55
		<i>Notification</i>	56
		<i>Authorization</i>	57
		<i>Preparation</i>	1
		<i>Proactive Process</i>	58
		<i>Proactive collection</i>	59
		<i>Incident response volatile collection</i>	60
		<i>Collection of network traces</i>	61
		<i>Crime scene investigation</i>	62
		<i>Event triggering function</i>	63
		<i>Communication shielding</i>	6
		<i>Documenting the scene</i>	5
		<i>Proactive preservation</i>	64
		<i>Proactive analysis</i>	65
		<i>Preliminary report</i>	66
		<i>Securing the scene</i>	2
		<i>Detection of incident/ crime</i>	67
		<i>Reactive Process</i>	68
		<i>Identification</i>	14
		<i>Survey</i>	3
		<i>Recognition</i>	4
		<i>Collection</i>	69
		<i>Acquisition</i>	15
		<i>Preservation</i>	9
		<i>Transportation</i>	40
		<i>Storage</i>	70
<i>Examination</i>	10		
<i>Analysis</i>	11		
<i>Presentation</i>	12		
<i>Post-Process</i>	71		
<i>Conclusion</i>	72		
<i>Reconstruction</i>	73		
<i>Dissemination</i>	74		

### Lampiran 3: Terminologi DFIF untuk *Smartphone Investigation*

#### 1. ***Windows Mobile Device Forensic Model (WMDFM)***

Terminologi tahapan-tahapan *Windows Mobile Device Forensic Model* dijelaskan sebagai berikut:

- a. *Preparation* adalah proses persiapan yang meliputi ketersediaan alat, personil dan berbagai hal kebutuhan penyelidikan.
- b. *Securing the scene* adalah melakukan sebuah mekanisme untuk mengamankan TKP dan melindungi integritas barang bukti.
- c. *Survey and recognition* adalah proses identifikasi TKP berdasarkan *chain custody* sampai mencatat siapa saja yang terlibat dalam TKP.
- d. *Documenting the scene* adalah mengolah tempat kejadian perkara, mencari sumber pemicu kejadian, mencari sambungan komunikasi atau jaringan dan mendokumentasikan tempat kejadian dengan mengambil gambar setiap detail TKP.
- e. *Communication shielding* adalah tahapan menonaktifkan komunikasi data pada barang bukti digital sehingga dapat mencegah perubahan data dari luar.
- f. *Volatile evidence collection* adalah proses pengamanan bukti digital yang sifatnya mudah hilang.
- g. *Non-volatile evidence collection* adalah proses pengamanan barang bukti digital.
- h. *Preservation* adalah proses menjaga integritas temuan dengan menggunakan *chain custody* dan fungsi *hashing*.
- i. *Examination* adalah proses pengolahan barang bukti untuk menemukan keterkaitannya dengan kejadian.
- j. *Analysis* adalah merupakan kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada.
- k. *Presentation* adalah proses pembuatan laporan dari seluruh temuan dan keterkaitannya yang disusun dalam bentuk yang mudah di pahami.

1. *Review* adalah proses analisa dan evaluasi keseluruhan terhadap hasil investigasi.

2. ***Symbian Smartphone Forensics Process Model (SSFPM)***

Terminologi tahapan-tahapan *Symbian Smartphone Forensics Process Model* dijelaskan sebagai berikut:

- a. *Preparation and version identification* adalah tahapan persiapan yang meliputi ketersediaan alat, personil dan berbagai hal yang dibutuhkan untuk proses penyelidikan serta melakukan identifikasi TKP yang mencakup memotret, sketsa, pemetaan TKP, pengolahan *chain custody* sampai mencatat siapa saja yang terlibat dalam TKP.
- b. *Remote evidence acquisition* adalah proses pengumpulan barang bukti digital baik *volatile* maupun *non-volatile*.
- c. *Internal evidence acquisition* adalah proses pengumpulan barang bukti fisik.
- d. *Analysis* adalah kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada.
- e. *Presentation and review* adalah proses pembuatan laporan dari seluruh temuan dan keterkaitannya yang disusun dalam bentuk yang mudah di pahami serta proses analisa dan evaluasi keseluruhan terhadap hasil investigasi.

3. ***Association of Chief Police Officer (ACPO)***

Terminologi tahapan-tahapan *Association of Chief Police Officer* dijelaskan sebagai berikut:

- a. *Preparation* adalah tahapan persiapan yang meliputi ketersediaan alat, personil dan berbagai hal yang dibutuhkan untuk proses penyelidikan.
- b. *Securing the scene* adalah pengamanan TKP untuk melindungi integritas barang bukti yang ada.

- c. *Documenting the scene* adalah tahapan untuk melakukan dokumentasi di TKP dengan mengambil gambar setiap detail TKP
- d. *PDA mode* adalah tahapan yang digunakan untuk melakukan pemilihan proses investigasi smartphone ketika kondisinya dalam keadaan “On” atau “Off”.
- e. *Communication shielding* adalah tahapan yang dilakukan untuk melindungi data yang terdapat pada barang bukti digital dari pertukaran data melalui jaringan komunikasi.
- f. *Packaging* adalah proses penyimpanan barang bukti digital yang ditemukan di TKP.
- g. *Plug in portable power supply* adalah proses pengamanan daya baterai pada barang bukti digital.
- h. *Seize* adalah proses penyitaan barang bukti digital yang telah ditemukan di TKP.
- i. *Examination* adalah tahapan pengolahan barang bukti digital untuk menemukan keterkaitannya dengan kejadian serta proses kajian teknis untuk merangkai keterkaitannya dengan temuan-temuan yang ada di TKP.

#### 4. ***Smartphone Forensics Investigation Process Model (SFIPM)***

Terminologi tahapan-tahapan *Smartphone Forensics Investigation Process Model* dijelaskan sebagai berikut:

- a. *Preparation and securing the scene* adalah tahapan persiapan yang meliputi ketersediaan alat, personil dan berbagai hal yang dibutuhkan untuk proses penyelidikan serta pengamanan TKP untuk melindungi integritas barang bukti yang ada.
- b. *Documentation* adalah tahapan untuk melakukan dokumentasi di TKP dengan mengambil gambar setiap detail TKP
- c. *PDA mode* adalah tahapan yang digunakan untuk melakukan pemilihan proses investigasi smartphone ketika kondisinya dalam keadaan “On” atau “Off”.

- d. *Communication shielding* adalah tahapan yang dilakukan untuk melindungi data yang terdapat pada barang bukti digital dari pertukaran data melalui jaringan komunikasi.
- e. *Evidence collection* adalah proses pengumpulan barang bukti digital yang ditemukan di TKP.
- f. *Volatile memory* adalah proses pengamanan bukti digital yang mudah hilang.
- g. *Non-volatile memory* adalah proses pengamanan bukti digital yang tidak mudah hilang.
- h. *Off-set/ cloud memory* adalah proses pengamanan bukti digital dari *cloud data*.
- i. *Preservation* adalah proses untuk menjaga integritas temuan dengan menggunakan *chain custody* dan fungsi *hashing*.
- j. *Examination* adalah proses untuk pengolahan barang bukti untuk menemukan keterkaitannya dengan kejadian.
- k. *Analysis* adalah kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada.
- l. *Presentation* adalah proses pembuatan laporan dari seluruh temuan dan keterkaitannya yang disusun dalam bentuk yang mudah di pahami.
- m. *Review* adalah proses analisa dan evaluasi keseluruhan terhadap hasil investigasi.

##### 5. ***International Standart Organisation (ISO/IEC 27041)***

Terminologi tahapan-tahapan ISO/IEC 27041 dijelaskan sebagai berikut:

- a. *Incident detection* adalah proses pemberitahuan pelaksanaan investigasi ataupun melaporkan adanya kejahatan kepada penegak hukum.
- b. *First response* adalah proses untuk mendapatkan hak akses terhadap barang bukti digital.

- c. *Planing* adalah tahapan persiapan yang meliputi ketersediaan alat, personil dan berbagai hal yang dibutuhkan untuk proses penyelidikan
- d. *Preparation process* adalah proses pelaksanaan investigasi di TKP.
- e. *Incident scene documentation* adalah tahapan untuk melakukan dokumentasi di TKP dengan mengambil gambar setiap detail TKP
- f. *Potential digital evidence identification* adalah proses pengumpulan barang bukti digital yang ditemukan di TKP.
- g. *Communication shielding* adalah tahapan yang dilakukan untuk melindungi data yang terdapat pada barang bukti digital dari pertukaran data melalui jaringan komunikasi.
- h. *Digital evidence acquisition* adalah proses pengumpulan barang bukti fisik ataupun digital baik *volatile* maupun *non-volatile*.
- i. *Digital evidence transportation* adalah proses pemindahan barang bukti digital ke tempat yang lebih aman.
- j. *Digital evidence storage* adalah proses penyimpanan barang bukti digital ke tempat yang aman.
- k. *Digital evidence analysis* adalah kajian teknis dan merangkai keterkaitan antara temuan-temuan yang ada
- l. *Report writing* adalah proses analisa dan evaluasi keseluruhan terhadap hasil investigasi.

#### 6. *National Institute of Standards and Technology (NIST)*

Terminologi tahapan-tahapan *National Institute of Standards and Technology* dijelaskan sebagai berikut:

- a. *Preservation (securing and evaluating the scene, documenting the scene, isolation, packaging, transporting and storing evidence, triage processing and decision making)* adalah tahapan yang dilakukan untuk pengamanan barang bukti digital yang telah ditemukan di TKP

- b. *Acquicition* adalah proses pengumpulan bukti digital yang terdapat pada barang bukti digital yang telah ditemukan di TKP
- c. *Examination and analysis* adalah tahapan pengolahan barang bukti digital untuk menemukan keterkaitannya dengan kejadian serta proses kajian teknis untuk merangkai keterkaitannya dengan temuan-temuan yang ada di TKP
- d. *Reporting* adalah proses pembuatan laporan terhadap seluruh temuan yang disusun dalam bentuk yang mudah dipahami.

#### 7. ***Harmonised Digital Forensics Investigation Process (HDFIP)***

Terminologi tahapan-tahapan *Harmonised Digital Forensics Investigation Process* dijelaskan sebagai berikut:

- a. *Initialization processes (incident detection, first response, planning, preparation)* adalah pemberitahuan pelaksanaan investigasi ataupun melaporkan adanya kejahatan kepada penegak hukum serta proses persiapan yang meliputi ketersediaan alat, personil dan berbagai hal kebutuhan penyelidikan.
- b. *Acquicition processes (potential digital evidence identification, potential digital evidence collection, potential digital evidence acquicition, potential digital evidence transportation, potential digital evidence storage and preservation)* adalah proses pengumpulan barang bukti fisik ataupun digital baik *volatile* maupun *non-volatile*.
- c. *Investigation processes (potential digital evidence acquicition, digital evidence examination and analysis, digital evidence interpretation, reporting, presentation, investigation closure)* adalah proses pengolahan barang bukti untuk menemukan keterkaitannya dengan kejadian serta proses pembuatan laporan dari seluruh temuan dan keterkaitannya yang disusun dalam bentuk yang mudah di pahami

Lampiran 4: Tahapan IDFIF dan DFIF untuk *smartphone investigation*

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
1	<i>Preparation</i>	1	1	1	1	4		1.4	1.3
2	<i>Securing the scene</i>	2		2	1		1.1		2.6
3	<i>Survey</i>	3							3.1.1
4	<i>Recognition</i>	3							3.1.2
5	<i>Documenting the scene</i>	4					1.2		2.2.2
6	<i>Communication shielding</i>	5		6	4				2.2.1
7	<i>Volatile evidence collection</i>	6							
8	<i>Non-volatile evidence collcetion</i>	7							
9	<i>Preservation</i>	8			6		1		3.3
10	<i>Examination</i>	9		10	7		3		3.4
11	<i>Analysis</i>	10	3		8		3		3.5
12	<i>Presentation</i>	11	4		9			3.5	3.6
13	<i>Review</i>	12	4		10				
14	<i>Identification</i>		1						3.1
15	<i>Acquicition</i>		2				2		3.2
16	<i>Remote evidence acquicition</i>		2.1						
17	<i>Internal evidence acquicition</i>		2.2						
18	<i>PDA mode</i>			3	3				
19	<i>Documentation</i>			4	2				
20	<i>Report writing</i>			5					



Lanjutan Lampiran 4: Tahapan IDFIF dan DFIF untuk *smartphone investigation*

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
21	<i>Package</i>			7					
22	<i>Seize</i>			8					
23	<i>Plug in portable power supply</i>			9					
24	<i>Evidence Collection</i>				5				
25	<i>Volatile memory</i>				5.1				
26	<i>Non-volatile memory</i>				5.2				
27	<i>Off-set/cloud memory</i>				5.3				
28	<i>Incident detection</i>					1		1.1	
29	<i>First response</i>					2		1.2	
30	<i>Planning</i>					3		1.3	
31	<i>Incident scene documentation</i>					5			
32	<i>Potential digital evidence identification</i>							2.1	
33	<i>Digital evidence acquisition</i>								
34	<i>Digital evidence transportation</i>								
35	<i>Digital evidence storage</i>								
36	<i>Digital evidence analysis</i>							3.2	
37	<i>Evaluation the scene</i>					1.1			
38	<i>Isolation</i>						1.3		
39	<i>Packaging</i>						1.4		
40	<i>Transportation</i>						1.4		3.3.1





Lampiran 5: Proses eliminasi tahapan yang sesuai dengan tahapan *Pre-Process* dan *Post-Process* pada IDFIF

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
1	<i>Preparation</i>	1	1	1	1	4		1.4	1.3
2	<i>Securing the scene</i>	2		2	1		1.1		2.6
3	<i>Survey</i>	3							3.1.1
4	<i>Recognition</i>	3							3.1.2
5	<i>Documenting the scene</i>	4					1.2		2.2.2
6	<i>Communication shielding</i>	5		6	4				2.2.1
7	<i>Volatile evidence collection</i>	6							
8	<i>Non-volatile evidence collection</i>	7							
9	<i>Preservation</i>	8			6		1		3.3
10	<i>Examination</i>	9		10	7		3		3.4
11	<i>Analysis</i>	10	3		8		3		3.5
12	<i>Presentation</i>	11	4		9			3.5	3.6
13	<i>Review</i>	12	4		10				
14	<i>Identification</i>		1						3.1
15	<i>Acquicition</i>		2				2		3.2
16	<i>Remote evidence acquicition</i>		2.1						
17	<i>Internal evidence acquicition</i>		2.2						
18	<i>PDA mode</i>			3	3				
19	<i>Documentation</i>			4	2				
20	<i>Report writing</i>			5					

Lanjutan Lampiran 5: Proses eliminasi tahapan yang sesuai dengan tahapan *Pre-Process* dan *Post-Process* pada IDFIF

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
21	<i>Package</i>			7					
22	<i>Seize</i>			8					
23	<i>Plug in portable power supply</i>			9					
24	<i>Evidence Collection</i>				5				
25	<i>Volatile memory</i>				5.1				
26	<i>Non-volatile memory</i>				5.2				
27	<i>Off-set/cloud memory</i>				5.3				
28	<i>Incident detection</i>					1		1.1	
29	<i>First response</i>					2		1.2	
30	<i>Planning</i>					3		1.3	
31	<i>Incident scene documentation</i>					5			
32	<i>Potential digital evidence identification</i>							2.1	
33	<i>Digital evidence acquisition</i>								
34	<i>Digital evidence transportation</i>								
35	<i>Digital evidence storage</i>								
36	<i>Digital evidence analysis</i>							3.2	
37	<i>Evaluation the scene</i>					1.1			
38	<i>Isolation</i>						1.3		
39	<i>Packaging</i>						1.4		
40	<i>Transportation</i>						1.4		3.3.1





Lampiran 6: Tahapan yang sesuai dengan *Proactive dan Reactive Process* pada IDFIF

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
2	<i>Securing the scene</i>	2		2	1		1.1		2.6
3	<i>Survey</i>	3							3.1.1
4	<i>Recognition</i>	3							3.1.2
5	<i>Documenting the scene</i>	4					1.2		2.2.2
6	<i>Communication shielding</i>	5		6	4				2.2.1
7	<i>Volatile evidence collection</i>	6							
8	<i>Non-volatile evidence collection</i>	7							
9	<i>Preservation</i>	8			6		1		3.3
10	<i>Examination</i>	9		10	7		3		3.4
11	<i>Analysis</i>	10	3		8		3		3.5
14	<i>Identification</i>		1						3.1
15	<i>Acquicition</i>		2				2		3.2
16	<i>Remote evidence acquicition</i>		2.1						
17	<i>Internal evidence acquicition</i>		2.2						
18	<i>PDA mode</i>			3	3				
19	<i>Documentation</i>			4	2				
20	<i>Report writing</i>			5					
21	<i>Package</i>			7					
22	<i>Seize</i>			8					
23	<i>Plug in portable power supply</i>			9					







Lampiran 7: Tahapan yang sesuai dengan *Proactive Process* pada IDFIF

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
2	<i>Securing the scene</i>	2		2	1		1.1		2.6
3	<i>Survey</i>	3							3.1.1
4	<i>Recognition</i>	3							3.1.2
5	<i>Documenting the scene</i>	4					1.2		2.2.2
6	<i>Communication shielding</i>	5		6	4				2.2.1
7	<i>Volatile evidence collection</i>	6							
8	<i>Non-volatile evidence collection</i>	7							
9	<i>Preservation</i>	8			6		1		3.3
10	<i>Examination</i>	9		10	7		3		3.4
11	<i>Analysis</i>	10	3		8		3		3.5
14	<i>Identification</i>		1						3.1
15	<i>Acquicition</i>		2				2		3.2
16	<i>Remote evidence acquicition</i>		2.1						
17	<i>Internal evidence acquicition</i>		2.2						
18	<i>PDA mode</i>			3	3				
19	<i>Documentation</i>			4	2				
20	<i>Report writing</i>			5					
21	<i>Package</i>			7					
22	<i>Seize</i>			8					
23	<i>Plug in portable power supply</i>			9					





Lampiran 8: Baris dengan terminologi yang sama dengan *documenting the scene* pada IDFIF

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
2	<i>Securing the scene</i>	2		2	1		1.1		2.6
5	<i>Documenting the scene</i>	4					1.2		2.2.2
6	<i>Communication shielding</i>	5		6	4				2.2.1
7	<i>Volatile evidence collection</i>	6							
8	<i>Non-volatile evidence collcetion</i>	7							
14	<i>Identification</i>		1						3.1
15	<i>Acquicition</i>		2				2		3.2
16	<i>Remote evidence acqicition</i>		2.1						
17	<i>Internal evidence acqicition</i>		2.2						
19	<i>Documentation</i>			4	2				
20	<i>Report writing</i>			5					
24	<i>Evidence Collection</i>				5				
25	<i>Volatile memory</i>				5.1				
26	<i>Non-volatile memory</i>				5.2				
28	<i>Incident detection</i>					1		1.1	
31	<i>Incident scene documentation</i>					5			
32	<i>Potential digital evidence identification</i>							2.1	
37	<i>Evaluation the scene</i>					1.1			
38	<i>Isolation</i>						1.3		
42	<i>Triage processing</i>						1.5		



Lampiran 9: Baris dengan terminologi yang sama dengan *event triggering* pada IDFIF

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
2	<i>Securing the scene</i>	2		2	1		1.1		2.6
5	<i>Documenting the scene</i>	4					1.2		2.2.2
6	<i>Communication shielding</i>	5		6	4				2.2.1
7	<i>Volatile evidence collection</i>	6							
8	<i>Non-volatile evidence collection</i>	7							
14	<i>Identification</i>		1						3.1
15	<i>Acquicition</i>		2				2		3.2
16	<i>Remote evidence acquicition</i>		2.1						
17	<i>Internal evidence acquicition</i>		2.2						
19	<i>Documentation</i>			4	2				
20	<i>Report writing</i>			5					
24	<i>Evidence Collection</i>				5				
25	<i>Volatile memory</i>				5.1				
26	<i>Non-volatile memory</i>				5.2				
28	<i>Incident detection</i>					1		1.1	
31	<i>Incident scene documentation</i>					5			
32	<i>Potential digital evidence identification</i>							2.1	
37	<i>Evaluation the scene</i>					1.1			
38	<i>Isolation</i>						1.3		
42	<i>Triage processing</i>						1.5		





Lampiran 10: Baris dengan terminologi yang sama dengan *Proactive Preservation* pada IDFIF

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
2	<i>Securing the scene</i>	2		2	1		1.1		2.6
5	<i>Documenting the scene</i>	4					1.2		2.2.2
6	<i>Communication shielding</i>	5		6	4				2.2.1
7	<i>Volatile evidence collection</i>	6							
8	<i>Non-volatile evidence collection</i>	7							
14	<i>Identification</i>		1						3.1
15	<i>Acquisition</i>		2				2		3.2
16	<i>Remote evidence acquisition</i>		2.1						
17	<i>Internal evidence acquisition</i>		2.2						
19	<i>Documentation</i>			4	2				
20	<i>Report writing</i>			5					
24	<i>Evidence Collection</i>				5				
25	<i>Volatile memory</i>				5.1				
26	<i>Non-volatile memory</i>				5.2				
28	<i>Incident detection</i>					1		1.1	
31	<i>Incident scene documentation</i>					5			
32	<i>Potential digital evidence identification</i>							2.1	
37	<i>Evaluation the scene</i>					1.1			
38	<i>Isolation</i>						1.3		
42	<i>Triage processing</i>						1.5		



Lampiran 11: Baris dengan terminologi yang sama dengan *proactive analysis* pada IDFIF

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
2	<i>Securing the scene</i>	2		2	1		1.1		2.6
5	<i>Documenting the scene</i>	4					1.2		2.2.2
6	<i>Communication shielding</i>	5		6	4				2.2.1
7	<i>Volatile evidence collection</i>	6							
8	<i>Non-volatile evidence collection</i>	7							
14	<i>Identification</i>		1						3.1
15	<i>Acquisition</i>		2				2		3.2
16	<i>Remote evidence acquisition</i>		2.1						
17	<i>Internal evidence acquisition</i>		2.2						
19	<i>Documentation</i>			4	2				
20	<i>Report writing</i>			5					
24	<i>Evidence Collection</i>				5				
25	<i>Volatile memory</i>				5.1				
26	<i>Non-volatile memory</i>				5.2				
28	<i>Incident detection</i>					1		1.1	
31	<i>Incident scene documentation</i>					5			
32	<i>Potential digital evidence identification</i>							2.1	
37	<i>Evaluation the scene</i>					1.1			
38	<i>Isolation</i>						1.3		
42	<i>Triage processing</i>						1.5		



Lampiran 12: Tahapan yang sesuai dengan *Reactive Process* pada IDFIF

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
2	<i>Securing the scene</i>	2		2	1		1.1		2.6
3	<i>Survey</i>	3							3.1.1
4	<i>Recognition</i>	3							3.1.2
5	<i>Documenting the scene</i>	4					1.2		2.2.2
6	<i>Communication shielding</i>	5		6	4				2.2.1
7	<i>Volatile evidence collection</i>	6							
8	<i>Non-volatile evidence collection</i>	7							
9	<i>Preservation</i>	8			6		1		3.3
10	<i>Examination</i>	9		10	7		3		3.4
11	<i>Analysis</i>	10	3		8		3		3.5
14	<i>Identification</i>		1						3.1
15	<i>Acquicition</i>		2				2		3.2
16	<i>Remote evidence acquicition</i>		2.1						
17	<i>Internal evidence acquicition</i>		2.2						
18	<i>PDA mode</i>			3	3				
19	<i>Documentation</i>			4	2				
20	<i>Report writing</i>			5					
21	<i>Package</i>			7					
22	<i>Seize</i>			8					
23	<i>Plug in portable power supply</i>			9					

















Lampiran 18: Tahapan yang tidak teridentifikasi pada IDFIF

No/ID	Tahapan	Urutan Tahapan Pada DFIF Untuk <i>Smartphone</i> :							
		WMFPM	SSFPM	ACPO	SFIPM	ISO 27041	NIST	HDFIP	IDFIF
2	<i>Securing the scene</i>	2		2	1		1.1		2.6
3	<i>Survey</i>	3							3.1.1
4	<i>Recognition</i>	3							3.1.2
5	<i>Documenting the scene</i>	4					1.2		2.2.2
6	<i>Communication shielding</i>	5		6	4				2.2.1
7	<i>Volatile evidence collection</i>	6							
8	<i>Non-volatile evidence collection</i>	7							
9	<i>Preservation</i>	8			6		1		3.3
10	<i>Examination</i>	9		10	7		3		3.4
11	<i>Analysis</i>	10	3		8		3		3.5
14	<i>Identification</i>		1						3.1
15	<i>Acquicition</i>		2				2		3.2
16	<i>Remote evidence acquicition</i>		2.1						
17	<i>Internal evidence acquicition</i>		2.2						
18	<i>PDA mode</i>			3	3				
19	<i>Documentation</i>			4	2				
20	<i>Report writing</i>			5					
21	<i>Package</i>			7					
22	<i>Seize</i>			8					
23	<i>Plug in portable power supply</i>			9					







Lampiran 19: Pemberian Tahapan Baru Pada *Proactive* dan *Reactive Process*

No.	ID	Tahapan	Tahapan IDFIF v2
1		<i>Incident Response</i>	2
2	2	<i>Securing the scene</i>	2.1
3	5	<i>Documenting the scene</i>	2.2
4	63	<i>Event trigering</i>	2.3
5	18	<i>PDA Mode</i>	<i>Decicion Process</i>
6	64	<i>Proactive preservation</i>	2.4
7	61	<i>Network trace</i>	2.4.1
8	23	<i>Plug In Portable Power Supply</i>	2.4.2
9	6	<i>Communication Shielding</i>	2.4.3
10	7	<i>Volatile evidence</i>	2.4.4
11	8	<i>Non-Volatile evidence</i>	2.4.5
12	65	<i>Proactive analysis</i>	2.5
13	67	<i>Detection of inciden/crime</i>	2.5.1
14	15	<i>Acquicition</i>	2.5.2
15	66	<i>Premilinary report</i>	2.5.3
16	22	<i>Seize</i>	2.6
17	40	<i>Transportation</i>	2.7
18		<i>Labolatorium Process</i>	3
19	9	<i>Preservation</i>	3.1
20	15	<i>Acquicition</i>	3.1.1
21	60	<i>Storage</i>	3.1.2
22	10	<i>Examination</i>	3.2
23	11	<i>Analysis</i>	3.3
24	19	<i>Documentaion</i>	3.4

## Lampiran 20: Hasil Kuesioner IDFIF v2

1. *Preparation*

No.	Pertanyaan	Jawaban	
		Ya	Tidak
1	Dalam menangani kasus, apakah bpk./ibu/sdr. selalu melalui pemberitahuan akan adanya proses investigasi?	√	
2	Apakah bpk./ibu/sdr. mendapatkan akses terhadap barang bukti dan proses hukum dalam kasus tersebut?	√	
3	Apakah dalam penanganan kasus selalu melaksanakan tahap persiapan meliputi alat, dokumen penyelidikan dan lain-lain?	√	

2. *Incident Response*

No.	Pertanyaan	Jawaban	
		Ya	Tidak
1	Apakah bpk./ibu/sdr. melaksanakan proses pengamanan tempat kejadian perkara ketika melakukan investigasi?	√	
2	Apakah bpk./ibu/sdr. melaksanakan proses dokumentasi tempat kejadian perkara ketika melakukan investigasi?	√	
3	Apakah bpk./ibu/sdr. melaksanakan rekonstruksi kejadian dan merangkai 5W1H?	√	
4	Apakah bpk./ibu/sdr. melaksanakan pengamanan sumber daya?	√	
5	Apakah bpk./ibu/sdr. melaksanakan pengamanan komunikasi data?	√	
6	Apakah bpk./ibu/sdr. melaksanakan penyitaan terhadap barang bukti tersebut?	√	
7	Apakah bpk./ibu/sdr. melaksanakan pemindahan barang bukti dari tempat kejadian ke laboratorium untuk proses pemeriksaan lebih lanjut?	√	

Lanjutan Lampiran 20: Hasil Kuesioner IDFIF v2

3. **Laboratorium Process**

No.	Pertanyaan	Jawaban	
		Ya	Tidak
1	Apakah bpk./ibu/sdr. melaksanakan kegiatan mengumpulkan bukti dari barang bukti yang didapat?	√	
2	Apakah bpk./ibu/sdr. melaksanakan kegiatan penyimpanan dan pengamanan barang bukti dan bukti yang telah didapat?	√	
3	Apakah bpk./ibu/sdr. melaksanakan pemeriksaan secara menyeluruh terhadap barang bukti yang sudah dikumpulkan?	√	
4	Apakah bpk./ibu/sdr. melaksanakan kajian terhadap temuan-temuan yang didapat pada proses <i>analysis</i> ?	√	
5	Apakah temuan dan keterkaitan dengan kasus yang ada disusun kedalam format yang mudah dipahami?	√	

4. **Presentation**

No.	Pertanyaan	Jawaban	
		Ya	Tidak
1	Apakah bpk./ibu/sdr. dalam melaksanakan penyelidikan kasus ada tahapan akhir?	√	
2	Apakah bpk./ibu/sdr. dalam melaksanakan penyelidikan kasus melalui tahapan analisis keseluruhan proses investigasi?	√	
3	Apakah bpk./ibu/sdr. melaksanakan tahapan pencatatan proses penyelidikan dan penyebarluasan catatan penyelidikan?	√	