Pengaturan Teknis Penanganan Bukti Elektronik Berdasarkan ISO/SNI 27037

Posisi ahli Digital Forensics dalam Proses Penanganan Bukti Elektronik dalam Proses Pembuktian dan Pengungkapan Perkara

Roni Sadrah | roni.sadrah@gmail.com

RONI SADRAH

Pendidikan Formal

- S1 – Teknik Sipil ITB,1999
- S2 – Teknik Informatika ITB, 2005
- MBA ITB, 2018 - skr

Keorganisasian

- High Technology Crime Investigation Association (HTCIA)
- Asosiasi Forensik Digital Indonesia (AFDI)

Sertifikasi

- Mobile Forensic - Belgium, 2011
- Computer Forensic - UK, 2012
- Mobile Forensic - HK, 2013
- Video Forensic - UK, 2014
- Mobile Forensic - Indonesia, 2017
- Mobile Forensic - S Korea, 2018
- Social Media Analysis: USA, 2019

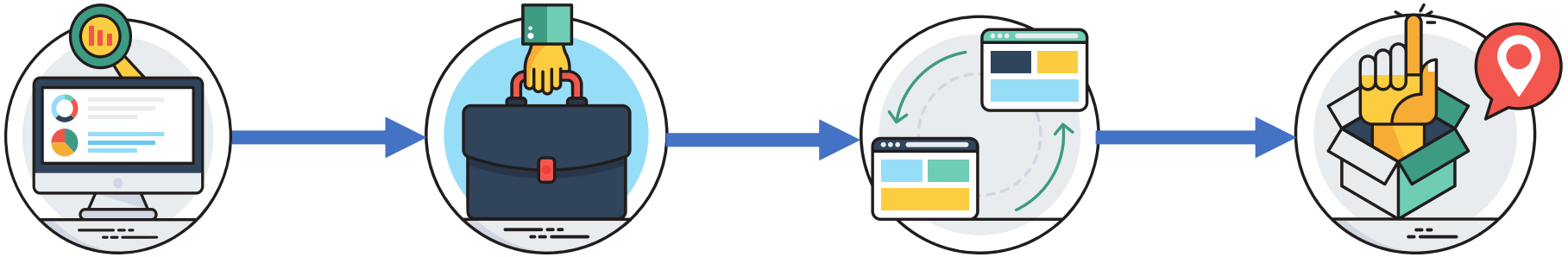
Instruktur

Mobile Forensic, Computer Forensic, Social Media Analysis

KPK, BPK, BPKP, Polri, Kemenkeu, Kominfo, Kemenkumham, BI, LPS, BSSN, BIN, BNN, SPRM (Malaysia), dll

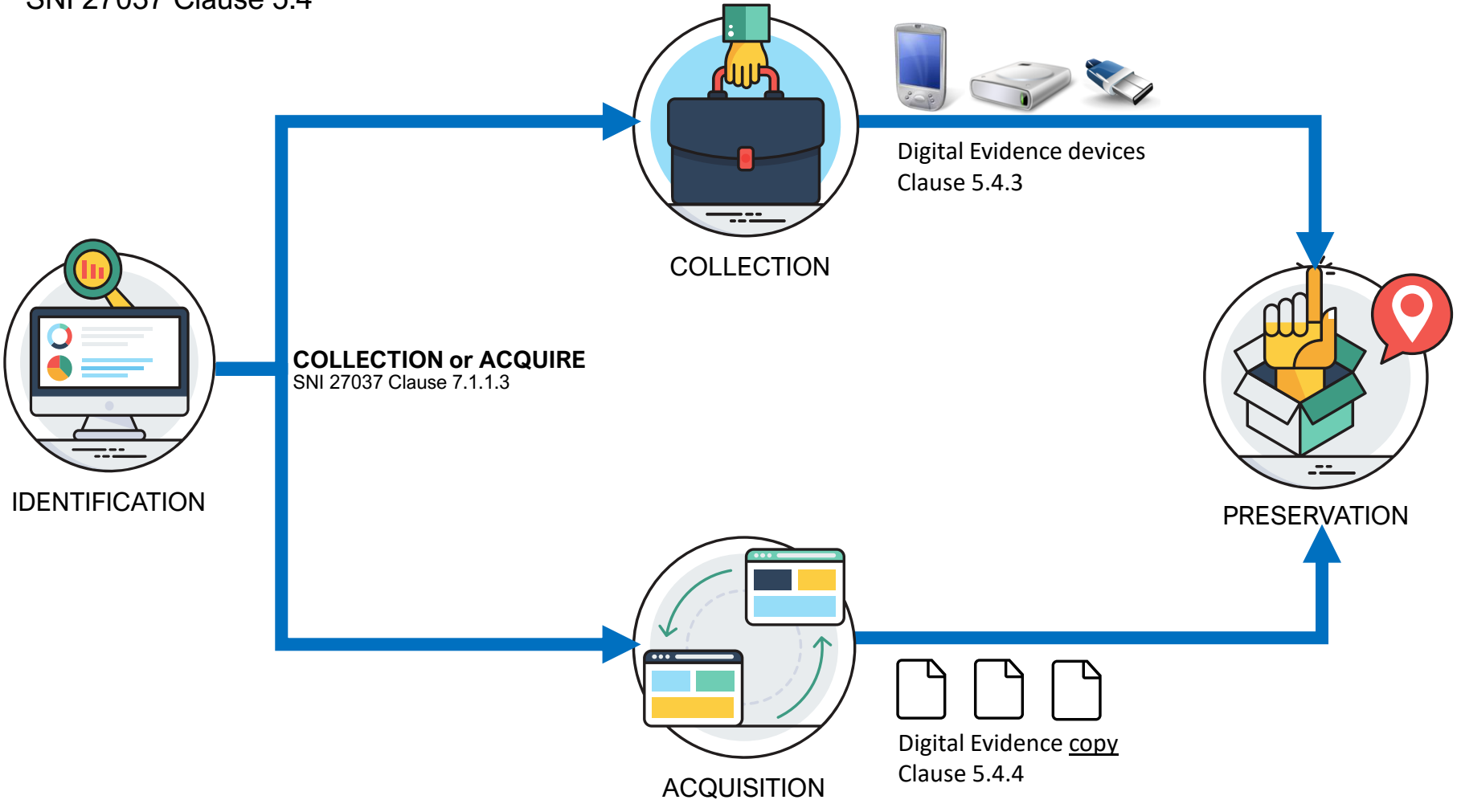
DIGITAL EVIDENCE HANDLING PROCESSES

SNI 27037 Clause 5.4 – SIMPLE MODEL



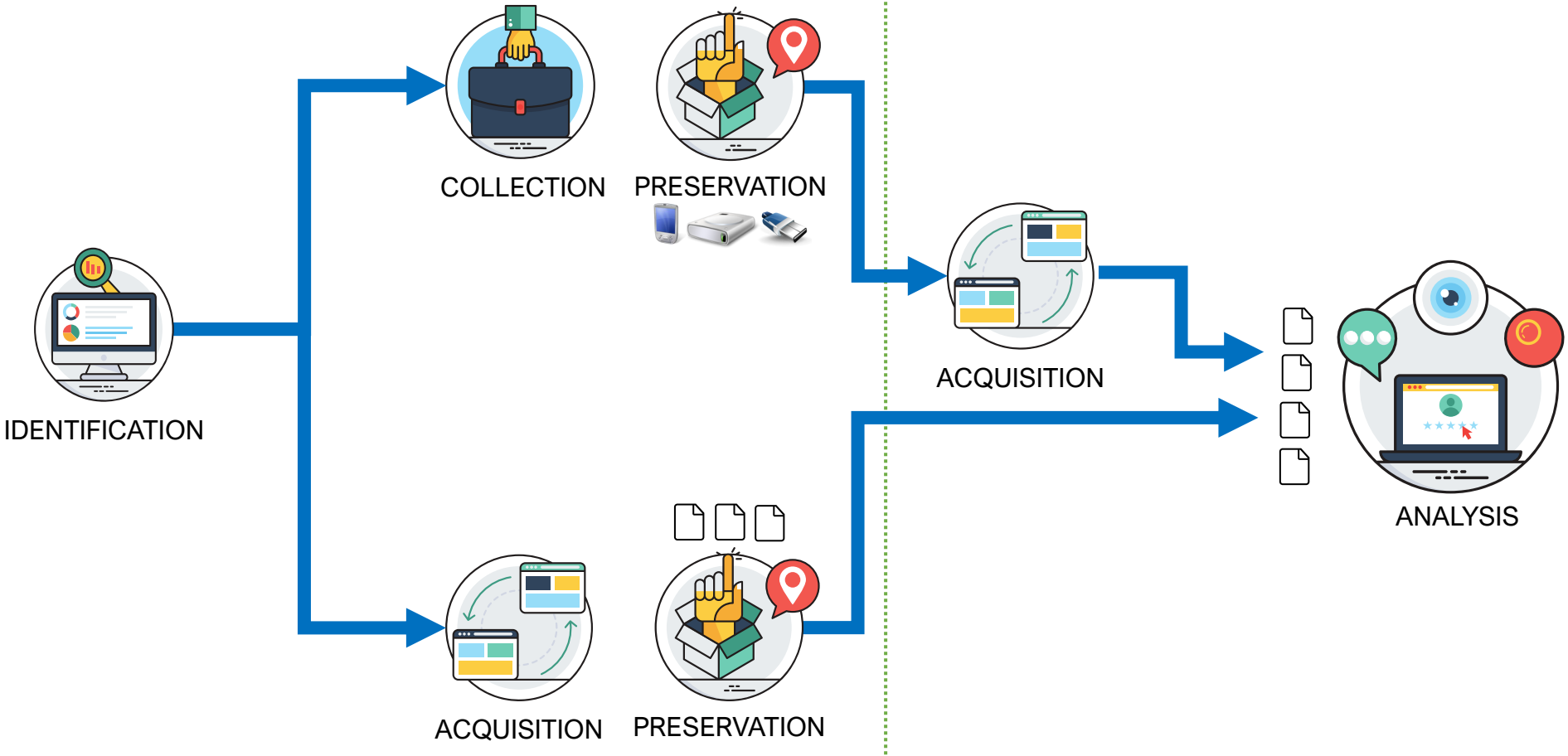
DIGITAL EVIDENCE HANDLING PROCESSES

SNI 27037 Clause 5.4



DIGITAL EVIDENCE HANDLING PROCESSES

SNI 27037 Clause 5.4



IDENTIFICATION

SNI 27037 Clause 5.4.2

IDENTIFICATION

STORAGE

- HDD/SSD
- CD/DVD ROM
- EXTERNAL DRIVES

NETWORK

- TOPOLOGY
- SHARED FOLDER
- CENTRALIZED/LOCAL STORAGE

WIRELESS NETWORK

- CONNECTED DEVICES
- NOT VISIBLE STORAGES

CLOUD

- ACCOUNT CREDENTIALS
- SYNC METHOD

VOLATILE DATA

- RAM, RUNNING PROCESSES
- ACTIVE CONNECTION
- ENCRYPTION INFORMATION

CCTV

- NETWORK DVR
- STORAGE SYSTEM
- VIDEO FORMAT

NON-DIGITAL

- RELATED PASSWORDS
- ENCRYPTION KEY
- SYSTEM CONFIGURATION

COLLECT or ACQUIRE

SNI 27037 Clause 7.1.1.3

IDENTIFICATION

COLLECT
or
ACQUIRE

DIAKUISISI DI LAB

SNI 27037 Clause 7.1.1.3

- Volatilitas Data (RAM / Memory Komputer)
- Informasi Enkripsi yang diinput manual (passphrase, keys)
- Sistem Kritikal
- Aturan/hukum
- Keterbatasan sumberdaya (kapasitas penyimpanan, personil, waktu)
- Informasi penyimpanan data di jaringan computer
- Keamanan di lokasi

UU ITE Pasal 43 ayat 4

(4) Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya **kepentingan pelayanan umum.**

AKUISISI DI LOKASI

File Salinan
Manual
(*.doc, *.log, dll)

File hasil
Imaging RAM
(*.DD, *.E01, dll)

File hasil
Imaging HDD, FD, SSD, Smartphone
(*.DD, *.E01, *.BIN, dll)

COLLECTION

SNI 27037 Clause 5.4.3

Digital Evidence devices

COLLECTION

IDENTIFICATION

- Labeling
- Bag & Tag
- Seal
- Transporting Procedures
- Etc

PRESERVATION

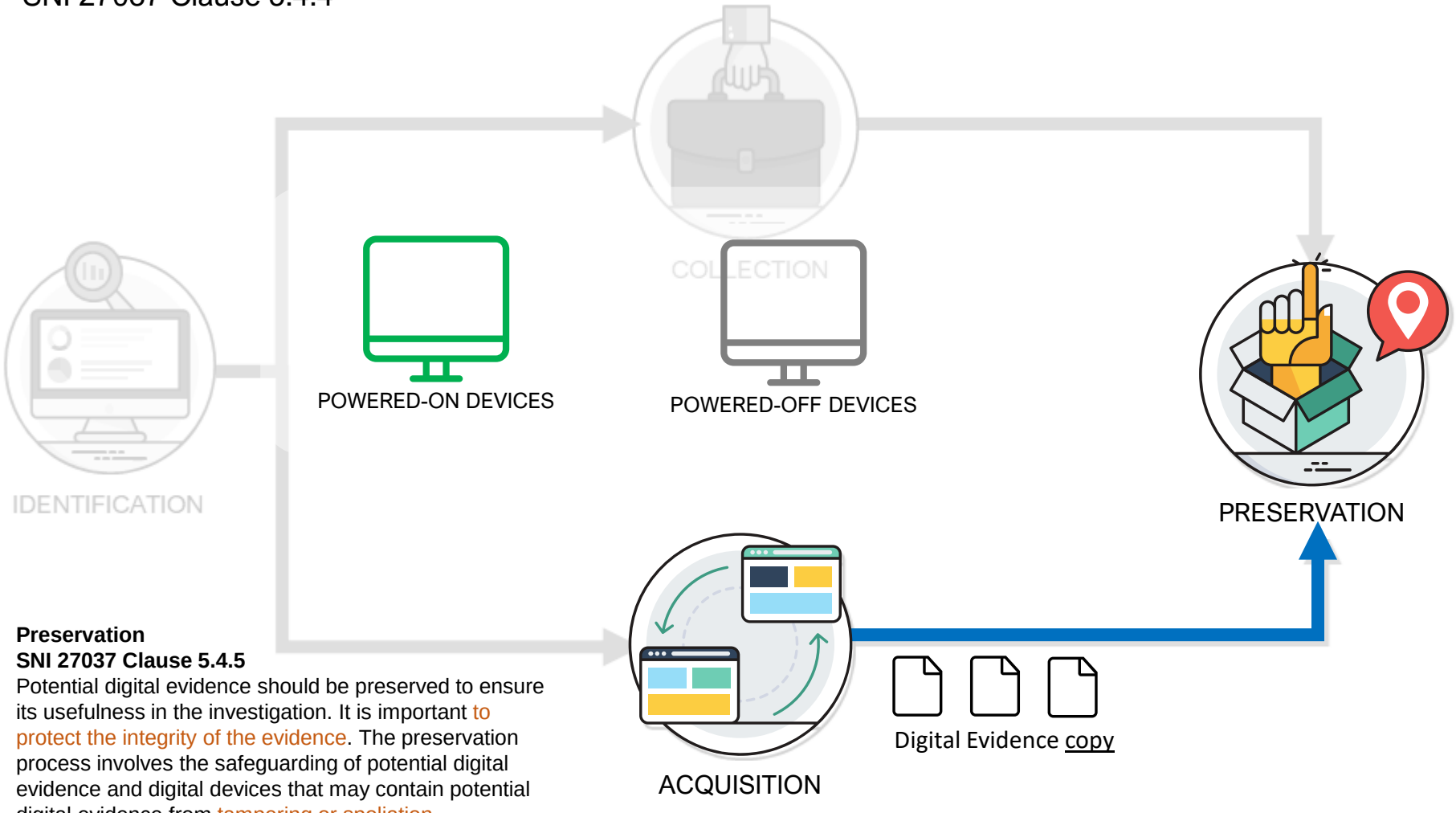
Preservation

SNI 27037 Clause 5.4.5

Potential digital evidence should be preserved to ensure its usefulness in the investigation. It is important to protect the integrity of the evidence. The preservation process involves the safeguarding of potential digital evidence and digital devices that may contain potential digital evidence from tampering or spoliation.

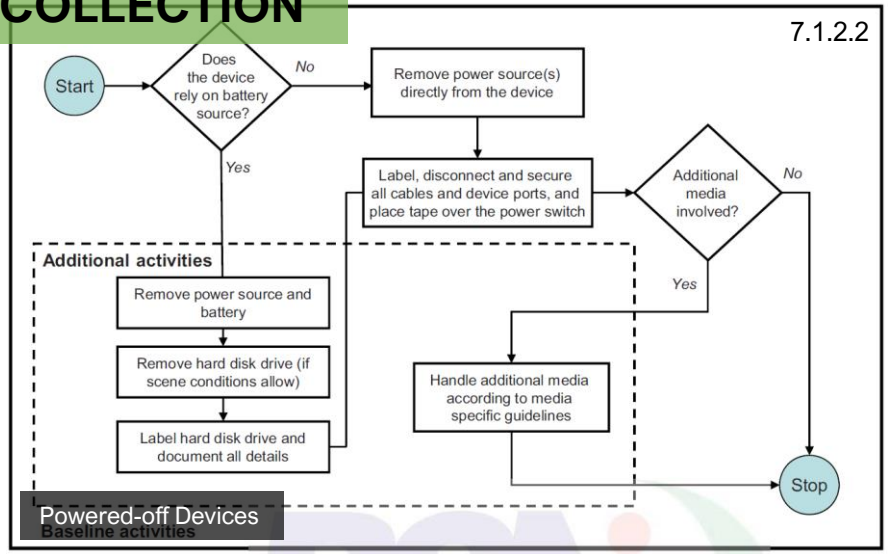
ACQUISITION

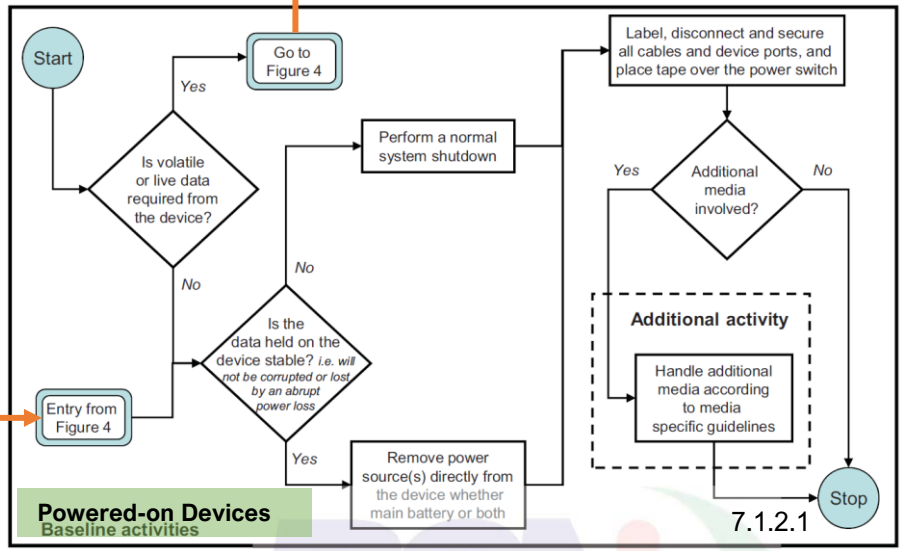
SNI 27037 Clause 5.4.4

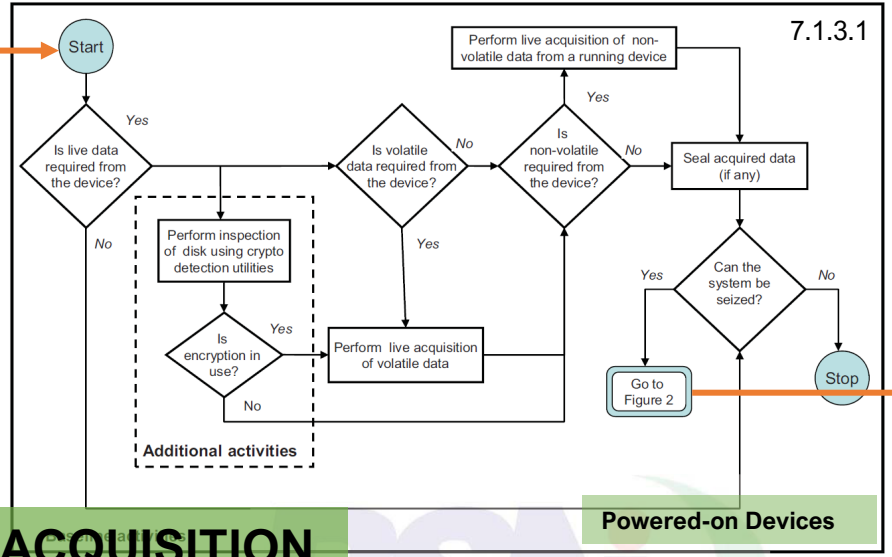


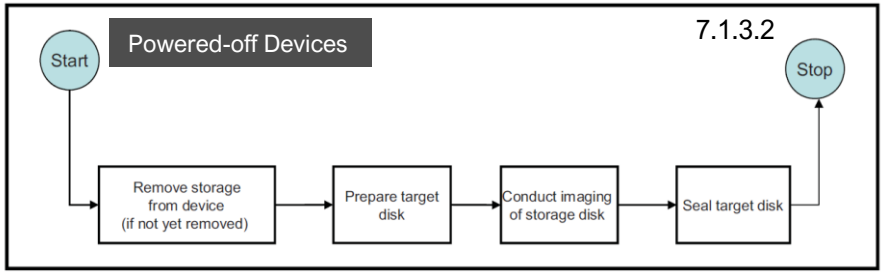
Preservation
SNI 27037 Clause 5.4.5
Potential digital evidence should be preserved to ensure its usefulness in the investigation. It is important to protect the integrity of the evidence. The preservation process involves the safeguarding of potential digital evidence and digital devices that may contain potential digital evidence from tampering or spoliation.

COLLECTION





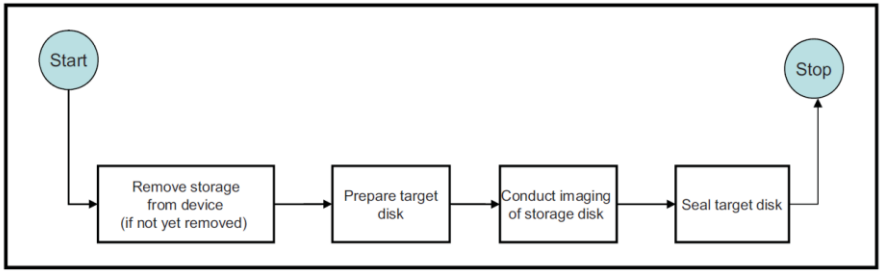




ACQUISITION

ACQUISITION
SNI 27037 Clause 5.4.4

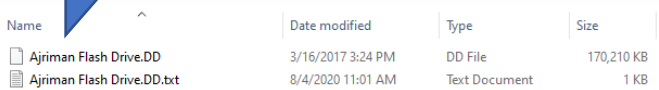
POWERED-OFF DEVICES
Clause 7.1.3.2

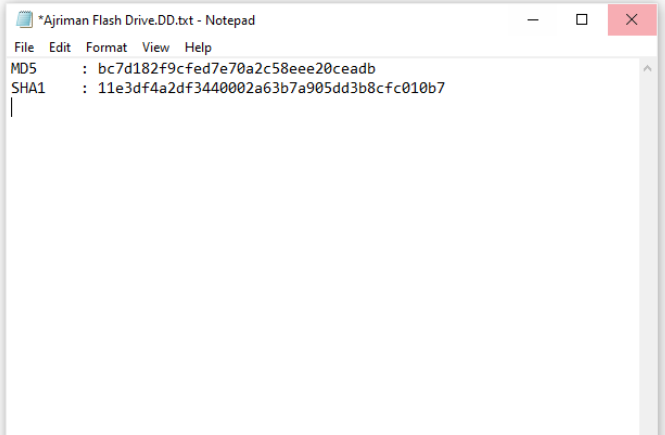


Forensic Imager (Duplicator)

Laptop + Forensic Bridge (Write Blocker)

Digital Evidence copy + Hash Value





ACQUISITION
SNI 27037 Clause 5.4.4

POWERED-ON DEVICES
Clause 7.1.3.1

ENCRYPTION INFORMATION

Truecrypt, etc

NON-VOLATILE DATA

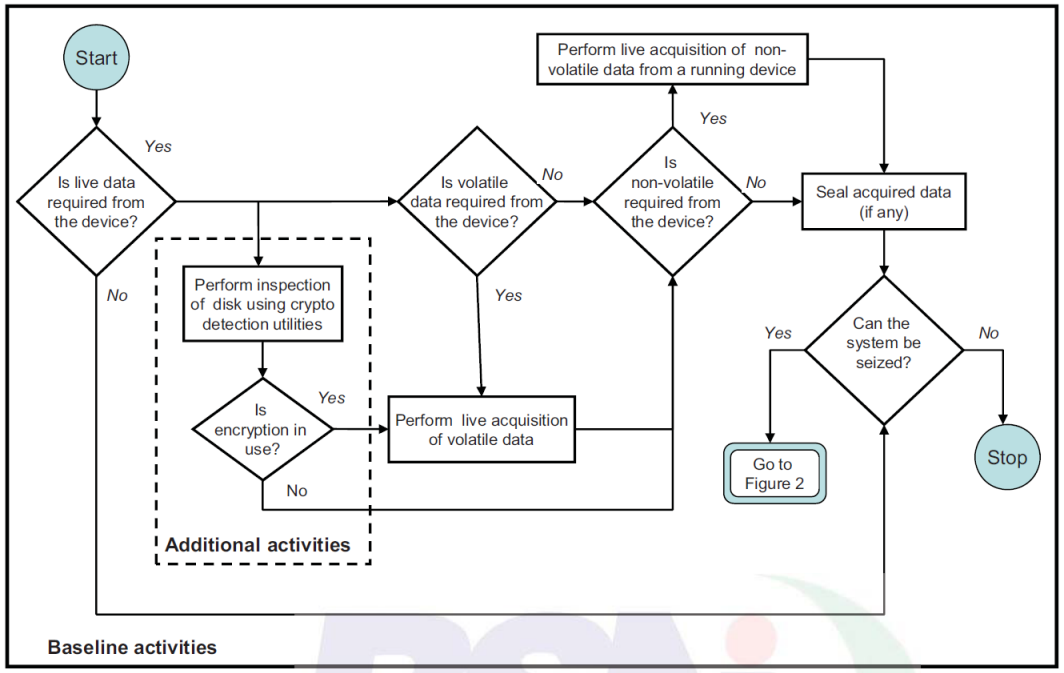
FILE KERJA *.pdf, *.xls, dll
FILE LOG *.log, dll

VOLATILE DATA

RAM
Credentials, Running Process, Network Connections, dll

SYSTEM SNAPSHOT
System Information, Running Process, Network Connections, dll

TEMPORARY STORAGE
Remote Storage, VeraCrypt, etc



ACQUISITION
SNI 27037 Clause 5.4.4

POWERED-ON DEVICES
Clause 7.1.3.1

ENCRYPTION INFORMATION

```
* Checking physical drives on system... *

Checking PhysicalDrive0 - WDC WD10JPVX-60JC3T1 (1.000 GB) - Status: OK
Checking PhysicalDrive1 - Toshiba THNSNJ256G8NU M.2 2280 256GB (256 GB) - Status: OK

* Completed checking physical drives on system. *

* Now checking logical volumes on system... *

Drive C: [Label: Windows] (PhysicalDrive1), Drive Type: Fixed, Filesystem: NTFS, Size: 125 GB, Free Space: 14 GB
Drive D: [Label: DATA] (PhysicalDrive0), Drive Type: Fixed, Filesystem: NTFS, Size: 1.000 GB, Free Space: 98 GB
Drive E: [Label: CACHE] (PhysicalDrive1), Drive Type: Fixed, Filesystem: NTFS, Size: 129 GB, Free Space: 36 GB
Drive G: [Label: <Error getting label: The device is not ready.>] (CD/DVDRom0), Drive Type: CDRom, Filesystem: Unknown, Size: Unknown, Free Space: Unknown

* Completed checking logical volumes on system. *

* Running Secondary Bitlocker Check... *

Volume D: [DATA] is encrypted using Bitlocker.

* Completed Secondary Bitlocker Check... *

* Checking for running processes... *

* Completed checking running processes. *

*** Encrypted volumes and/or processes were detected by EDD. ***

Press any key to continue...
(use 'EDD /batch' to bypass this prompt next time)
```

ACQUISITION
SNI 27037 Clause 5.4.4

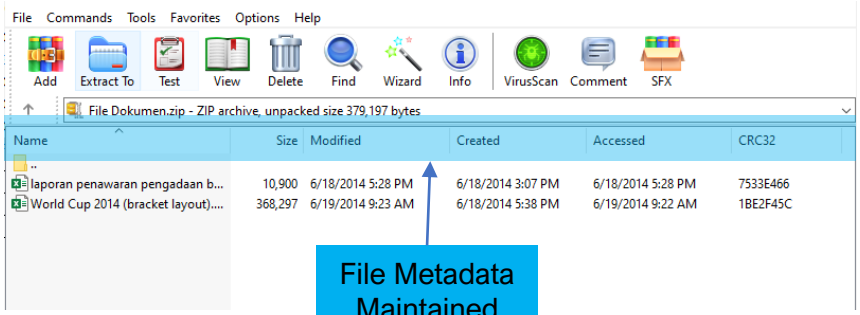
POWERED-ON DEVICES
Clause 7.1.3.1

Preservation
SNI 27037 Clause 5.4.5 (cont..)
In the best-case scenario, there should be no spoliation to the data itself or any metadata associated with it (e.g. date and time-stamps). The DEFR should be able to demonstrate that the evidence has not been modified since it was collected or acquired, or provide the rationale and documented actions if unavoidable changes were made.

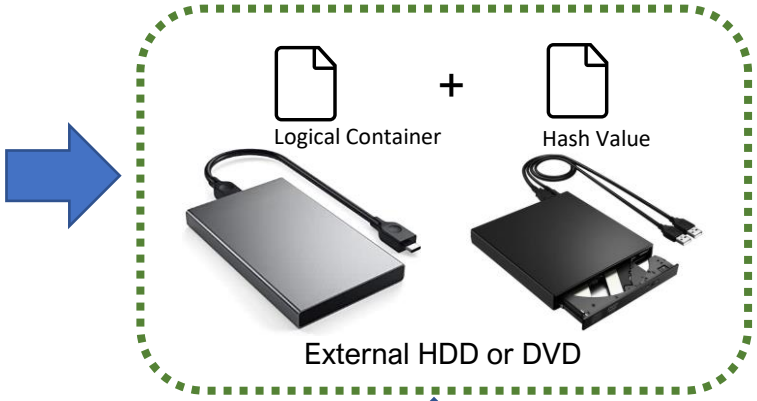
NON-VOLATILE DATA
FILE KERJA *.pdf, *.xls, dll
FILE LOG

1 Hasil akuisisi dengan logical container ZIP

SNI 27037 Clause 7.1.3.1.2
Zip container

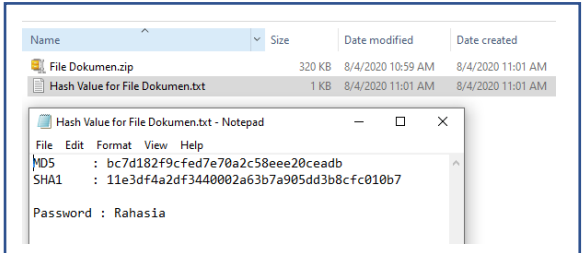


File Metadata Maintained



2 Hasil akuisisi dengan logical container L01

	Name	Logical Size	Last Written	File Created	Last Accessed	MD5
1	Genset Honda 2 KVA-12,5 KVA.pdf	2,981,380	18-Jun-2014 17:01:07	18-Jun-2014 17:01:04	18-Jun-2014 17:01:04	1ea422eca9f3c5f161ebb4a724e01e33
2	HP workstation brochure.pdf	6,804,590	18-Jun-2014 15:35:58	18-Jun-2014 15:28:33	18-Jun-2014 15:28:33	ecd6322ee3e7121d86c6f930da51d01d
3	laporan penawaran pengadaan barang.xlsx	10,900	18-Jun-2014 17:28:49	18-Jun-2014 15:07:42	18-Jun-2014 17:28:49	910b6f39f9dee761ec300a48a651d762
4	sbm600factsheet.pdf	769,497	18-Jun-2014 17:09:52	18-Jun-2014 17:09:49	18-Jun-2014 17:09:49	fbf97200b03d427d05ef90632819eea3
5	specssbm680i6v30jan14.pdf	271,284	18-Jun-2014 17:12:15	18-Jun-2014 17:12:12	18-Jun-2014 17:12:12	57537281f03ff7aa5e99d0ea99f8d8eb
6	surat penawaran informatika revisi.pdf	55,147	18-Jun-2014 18:01:00	18-Jun-2014 18:01:00	18-Jun-2014 18:02:07	78cd2fe3af8088f5e7db0da3bb2ab891
7	World Cup 2014 (bracket layout).xlsx	368,297	19-Jun-2014 09:23:00	18-Jun-2014 17:38:49	19-Jun-2014 09:22:59	180f8ed9021adc9fd304bcefae18f506



Logical Container with Hash

ACQUISITION
SNI 27037 Clause 5.4.4

POWERED-ON DEVICES
Clause 7.1.3.1

Preservation
SNI 27037 Clause 5.4.5 (cont..)
In the best-case scenario, there should be no spoliation to the data itself or any metadata associated with it (e.g. date and time-stamps). The DEFR should be able to demonstrate that the evidence has not been modified since it was collected or acquired, or provide the rationale and documented actions if unavoidable changes were made.

3 Hasil akuisisi dengan penyalinan tanpa logical container

File Asli

Name	Size	Date modified	Date created	Date accessed
laporan penawaran pengadaan barang.xlsx	11 KB	6/18/2014 5:28 PM	6/18/2014 3:07 PM	8/6/2020 5:38 AM
World Cup 2014 (bracket layout).xlsx	360 KB	6/19/2014 9:23 AM	6/18/2014 5:38 PM	8/6/2020 5:38 AM

File Salinan

Name	Size	Date modified	Date created	Date accessed
laporan penawaran pengadaan barang.xlsx	11 KB	6/18/2014 5:28 PM	8/6/2020 5:39 AM	8/6/2020 5:39 AM
World Cup 2014 (bracket layout).xlsx	360 KB	6/19/2014 9:23 AM	8/6/2020 5:39 AM	8/6/2020 5:39 AM

Created Date berubah

PRESERVATION

SNI 27037 Clause 5.4.5

Potential digital evidence should be preserved to ensure its usefulness in the investigation. It is important **to protect the integrity of the evidence**. The preservation process involves the safeguarding of potential digital evidence and digital devices that may contain potential digital evidence from **tampering or spoliation.**

UU ITE Pasal 43 ayat 2

(2) Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, dan **integritas atau keutuhan data** sesuai dengan ketentuan peraturan perundang-undangan.

HOW VALIDATION WORKS?

VALIDATION OF

PHYSICAL IMAGE

SNI 27037 Clause 3.25
verification function
function which is used to verify that two sets of data are identical

NOTE 1 No two non-identical data sets should produce an identical match from a verification function.
NOTE 2 Verification functions are commonly implemented using hash functions such as MD5, SHA1, etc., but other methods may be used.

NORMAL DIGITAL EVIDENCE

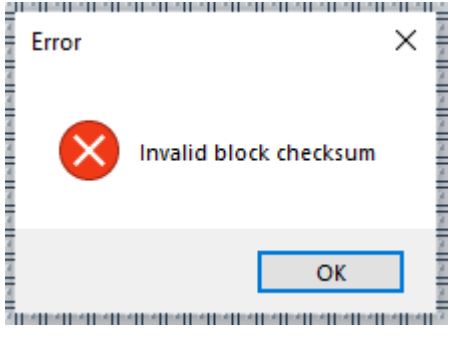
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	4992fddfbf0a0778441fcb1af3da8641
Verification MD5	4992fddfbf0a0778441fcb1af3da8641
Acquisition SHA1	da18dedf2619de5e935104830f667ff9501e1cbe
Verification SHA1	da18dedf2619de5e935104830f667ff9501e1cbe

Acquisition & Verification hash **MATCH**

TAMPERED DIGITAL EVIDENCE

File Integrity	Completely Verified, 2 Errors
Acquisition MD5	4992fddfbf0a0778441fcb1af3da8641
Verification MD5	6c7664a5d39504338179cebf64b0b61c
Acquisition SHA1	da18dedf2619de5e935104830f667ff9501e1cbe
Verification SHA1	0b560f5ff385d8370af98a85b39c5406f96b5ce3

Acquisition & Verification hash **NOT MATCH**



E01 FORMAT INFORMS TAMPERED BLOCKS

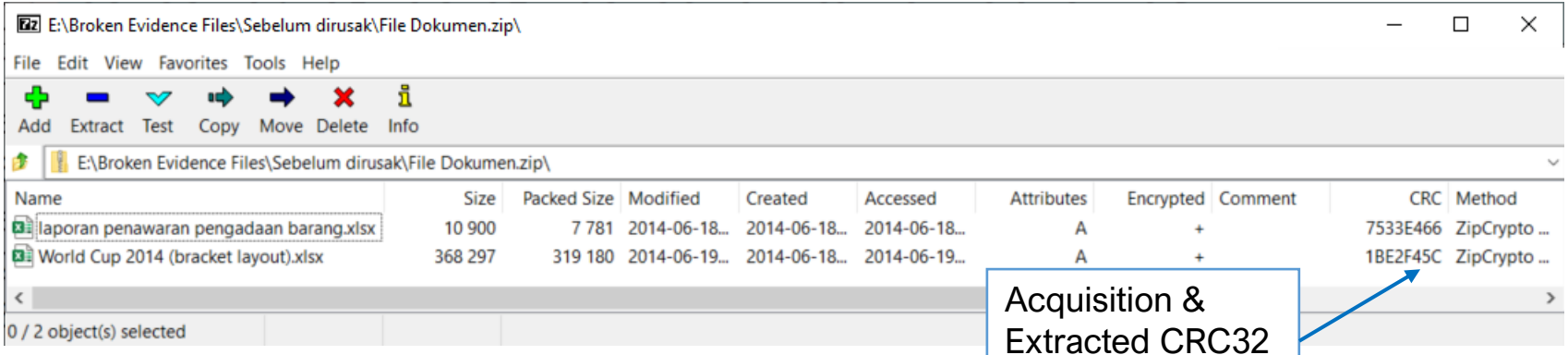
The integrity of the following sector groups could not be verified
Ajriman Flash Drive.E01: 141184-141247,329344-329407

VALIDATION OF

LOGICAL IMAGE (ZIP)

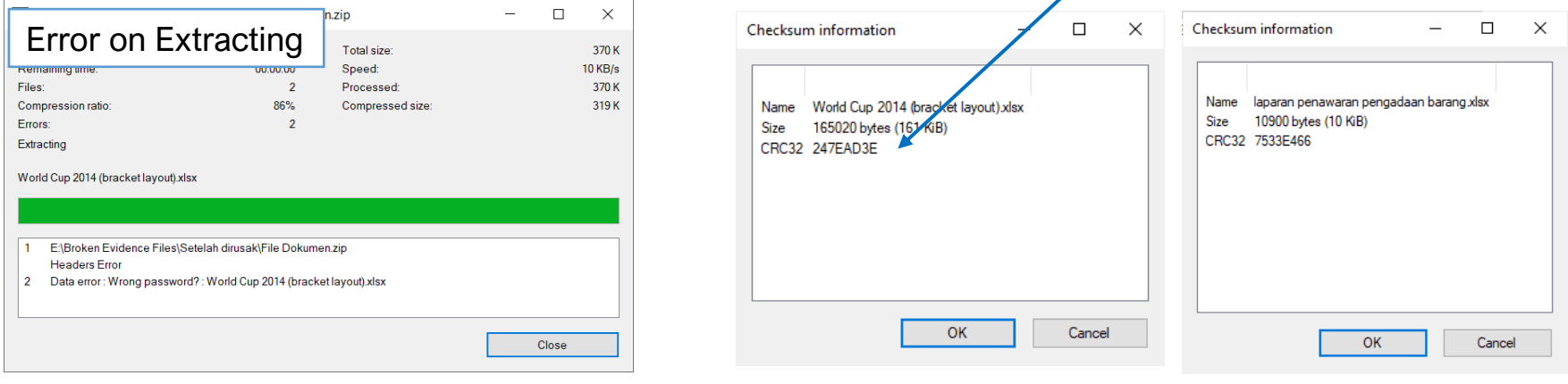
NORMAL DIGITAL EVIDENCE

ZIP HASH VALUE MATCH & ZIP FILE EXTRACTED NORMALLY



TAMPERED DIGITAL EVIDENCE

ZIP HASH VALUE NOT MATCH, ZIP FILE ERROR ON EXTRACTION, AT LEAST ONE CRC32 NOT MATCH



VALIDATION OF

LOGICAL IMAGE (L01)

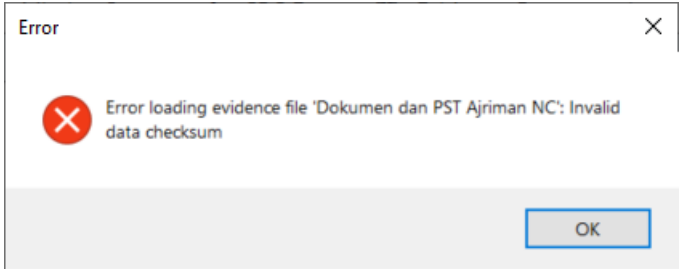
NORMAL DIGITAL EVIDENCE

L01 HASH VALUE MATCH & L01 FILE OPENED NORMALLY

	Name	Logical Size	Last Written	File Created	Last Accessed	MD5
1	Genset Honda 2 KVA-12,5 KVA.pdf	2,981,380	18-Jun-2014 17:01:07	18-Jun-2014 17:01:04	18-Jun-2014 17:01:04	1ea422eca9f3c5f161ebb4a724e01e33
2	HP workstation brochure.pdf	6,804,590	18-Jun-2014 15:35:58	18-Jun-2014 15:28:33	18-Jun-2014 15:28:33	ecd6322ee3e7121d86c6f930da51d01d
3	laporan penawaran pengadaan barang.xlsx	10,900	18-Jun-2014 17:28:49	18-Jun-2014 15:07:42	18-Jun-2014 17:28:49	910b6f39f9dee761ec300a48a651d762
4	sbm600factsheet.pdf	769,497	18-Jun-2014 17:09:52	18-Jun-2014 17:09:49	18-Jun-2014 17:09:49	fbf97200b03d427d05ef90632819eea3
5	specssbm680i6v30jan14.pdf	271,284	18-Jun-2014 17:12:15	18-Jun-2014 17:12:12	18-Jun-2014 17:12:12	57537281f03ff7aa5e99d0ea99f8d8eb
6	surat penawaran informatika revisi.pdf	55,147	18-Jun-2014 18:01:00	18-Jun-2014 18:01:00	18-Jun-2014 18:02:07	78cd2fe3af8088f5e7db0da3bb2ab891
7	World Cup 2014 (bracket layout).xlsx	368,297	19-Jun-2014 09:23:00	18-Jun-2014 17:38:49	19-Jun-2014 09:22:59	180f8ed9021adc9fd304bcefae18f506

TAMPERED DIGITAL EVIDENCE

L01 HASH VALUE NOT MATCH & L01 FILE FAILED TO BE OPENED



VALIDATION OF

MOBILE DEVICES

SNI 27037 Clause 7.2.2.1
Generally, mobile devices such as PDAs and mobile phones need to be switched on in order to acquire potential digital evidence. This devices can continuously alter its operating environment whilst powered on, for example, the clock timer can be updated. The associated problem is that two digital evidence copies of the same device may not pass standard verification functions such as hashing. In this situation, alternate verification functions that identify areas of commonality and/or difference may be appropriate

- Akuisisi mobile phone menghasilkan hasil hash yang sama dengan menggunakan metode:
  - Chip-off (hash sama untuk seluruh physical storage)
  - Custom boot loader (hash sama untuk partisi **system** dan **data**)
- Selain dengan kedua metode itu, hash dari file hasil akuisisi smartphone dapat berbeda. Hal ini biasanya disebabkan oleh perubahan file log, *cache*, atau smartphone membuat *temporary files* ketika smartphone dihidupkan untuk proses akuisisi
- Perubahan file atau data biasanya bersifat *incremential*, seperti:
  - Penambahan baris log untuk event yang terjadi
  - Penambahan record database jika data disimpan dalam database lokal mobile device

  Data sebelumnya biasanya tidak berubah
- Karena data berubah, konsep hash function tidak dapat digunakan, sehingga validasi menggunakan prinsip *commonality,* yaitu mengidentifikasi data yang selalu muncul/tampil pada setiap ekstraksi yang dilakukan

VALIDATION OF

MOBILE DEVICES

SNI 27037 Clause 7.2.2.1

Generally, mobile devices such as PDAs and mobile phones need to be switched on in order to acquire potential digital evidence. This devices can continuously alter its operating environment whilst powered on, for example, the clock timer can be updated. The associated problem is that two digital evidence copies of the same device may not pass standard verification functions such as hashing. In this situation, alternate verification functions that identify areas of commonality and/or difference may be appropriate

EVENTS BEFORE SEIZURE (**AREA OF COMMONALITY**)

SMS	02/11/2013 11:59:27 AM	Hi don't forget to print all the brochures
MMS	02/11/2013 12:00:19 PM	This is the phone you need to sell
SMS	02/11/2013 12:01:20 PM	Understood
SMS	02/11/2013 12:01:51 PM	I'll do the best
SMS	02/11/2013 12:02:49 PM	I don't forget about tax evasion
FlexiSPY location report	02/11/2013 12:30:12 PM	N 55.7364635, E 37.6952248 network
FlexiSPY location report	02/11/2013 01:30:13 PM	N 55.7365784, E 37.6945863 network
FlexiSPY location report	02/11/2013 02:30:14 PM	N 55.7364708, E 37.6949040 network
Appointment	02/23/2013 05:00:00 PM	Visit private club with Mary Ades
Appointment	03/30/2013 07:00:00 PM	Ann's birthday
Appointment	07/14/2013 01:30:00 PM	Exhibition in Atlanta
All day event	07/23/2013 12:00:00 AM	Book tickets to Finland

SYSTEM-GENERATED EVENTS

KESIMPULAN

1. Ahli forensik digital memastikan seluruh proses penanganan bukti elektronik dari mulai identifikasi, pengumpulan, akuisisi, dan preservasi dilakukan dengan tujuan tidak merusak integritas bukti digital

2. Ahli forensik digital harus memiliki kompetensi untuk melakukan pengumpulan dan akuisisi data yang dilakukan secara live atau langsung

3. Ahli forensik digital harus memastikan dokumentasi seluruh proses penanganan bukti digital dilakukan dengan memadai

4. Metode verifikasi yang akan digunakan untuk validasi bukti digital sudah harus dapat ditentukan sejak proses identifikasi

THANK YOU

roni.sadrah@gmail.com

Roni Sadrah

@ronisadrah

roni.sadrah