



KEMENTERIAN KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA

Forensik Digital

Bukti Elektronik, Ketentuan Hukum dan Prosedur Penanganan

Disampaikan dalam acara

Manajemen Dokumen Pengadaan Elektronik

Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi

Bandung, 15 Juni 2021

Syofian Kurniawan, ST.,MTI,CEH,CHFI,CCPA

Subkoordinator Penyidikan,

Dit. Pengendalian Aplikasi Informatika

Data Diri

Pendidikan :

- S1 : Teknik Elektro UNDIP
- S2 : Magister Teknologi Informasi UI

Pekerjaan :

- 2008 – PNS/ASN Kementerian Kominfo

Aktifitas/Jabatan :

- PPNS UU ITE
- Subkoordinator Penyidikan
- Analis Kebijakan Ahli Muda
- Analis Digital Forensik – Tim Ahli
- Dewan Penasehat Industri – Telkom University

Kontak :

- E-mail : syofian.kurniawan@kominfo.go.id
- WA : 081575238762

Sertifikasi

- CEH - CCO
- CHFI - CCPA

Pengalaman Training :

- IVLP – USA
- JICA – JEPANG
- Cyber Security – Australia

Nomor : 38815/A7/LK.00.02/2021
Lampiran : Satu Berkas
Hal : Permohonan sebagai Narasumber dan Peserta

11 Juni 2021

Yth. (Daftar Terlampir)

Dalam rangka meningkatkan tata kelola pengadaan secara elektronik di lingkungan Kemendikbudristek, dengan hormat kami mengharapkan kehadiran Saudara pada kegiatan yang akan dilaksanakan pada:

hari, tanggal : Selasa, 15 Juni 2021
waktu : 08.00 s.d. 18.00 WIB (jadwal kegiatan terlampir)
tempat : Hotel Grand Mercure Setiabudi Bandung
Jl. Dr. Setiabudi No. 269-275, Isola, Kec. Sukasari Bandung Jawa Barat 40154
media : *Meeting ID* : 863 8593 1612
Passcode : ukpbj123
Join URL : <http://ringkas.kemdikbud.go.id/15062021>
acara : Manajemen Dokumen Pengadaan Elektronik

Sehubungan dengan hal tersebut, dengan hormat kami mohon Saudara berkenan hadir sebagai narasumber dan menugaskan 1 (satu) orang staf yang kompeten sebagai peserta pada kegiatan tersebut.

Untuk informasi dan konfirmasi kehadiran dapat menghubungi Sdr. Aris Ariyanto (081317531476) atau Sdri. Fathia Ainusyifa (082129557942).

Nomor : 38815/A7/LK.00.02/2021
Lampiran : Satu Berkas
Hal : Permohonan sebagai Narasumber dan Peserta

11 Juni 2021

Yth. (Daftar Terlampir)

Dalam rangka meningkatkan tata kelola pengadaan secara elektronik di lingkungan Kemendikbudristek, dengan hormat kami mengharapkan kehadiran Saudara pada kegiatan yang akan dilaksanakan pada:

hari, tanggal : Selasa, 15 Juni 2021
waktu : 08.00 s.d. 18.00 WIB (jadwal kegiatan terlampir)
tempat : Hotel Grand Mercure Setiabudi Bandung
Jl. Dr. Setiabudi No. 269-275, Isola, Kec. Sukasari Bandung Jawa Barat 40154
media : *Meeting ID* : 863 8593 1612
Passcode : ukpbj123
Join URL : <http://ringkas.kemdikbud.go.id/15062021>
acara : Manajemen Dokumen Pengadaan Elektronik

Sehubungan dengan hal tersebut, dengan hormat kami mohon Saudara berkenan hadir sebagai narasumber dan menugaskan 1 (satu) orang staf yang kompeten sebagai peserta pada kegiatan tersebut.

Untuk informasi dan konfirmasi kehadiran dapat menghubungi Sdr. Aris Ariyanto (081317531476) atau Sdri. Fathia Ainusyifa (082129557942).

Apa perbedaan 2 dokumen tersebut?

MD5 hash :

8a804c4b1ba90e29bc407a42768aa1e7

MD5 hash :

38f9e512e8180abfff273656b859392b



HxD - [D:\Presentasi\2021\Kemendikbudriset dan teknologi\bella.jpg]

File Edit Search View Analysis Tools Window Help

bella.jpg

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0001A750	E3	F3	A8	ED	20	9F	5F	02	E5	FA	38	E9	5D	B8	C6	0D	ãó'i Ÿ.âúøé].E.
0001A760	AF	80	54	28	85	71	FB	3A	BC	0D	50	CA	64	64	E5	9A	ET(...qû:4.PEdððš
0001A770	65	2A	EB	66	82	B5	86	B4	F6	AB	03	51	5A	8F	8C	5F	e*ëf,ut'ö«.QZ.E
0001A780	09	98	2B	66	C7	4E	CF	BA	A0	A8	46	56	4A	BE	85	C3	."+fçNI° "FVJ4.Ä
0001A790	23	ED	0B	F1	0A	61	5C	5F	E1	AC	01	AF	4C	61	D4	57	#i.ñ.a\á~.LaOW
0001A7A0	23	90	50	62	CB	F3	8D	C4	60	2D	3C	E6	C7	B0	20	B6	#.PbEö.Ä'~<æÇ° ¶
0001A7B0	A9	5D	F2	98	22	4A	EF	91	3F	AD	B6	10	04	04	53	25	©]ò"Ji'?.¶...S§
0001A7C0	4C	BA	D5	88	F7	60	B4	41	08	F2	98	54	89	3E	00	DC	L°ö÷'A.ò'Tk>.Ü
0001A7D0	47	14	92	83	38	16	06	48	21	25	B9	FB	22	52	41	11	G.'f8..H!%~ù"RA.
0001A7E0	14	88	19	B1	37	33	BF	94	2E	2B	F5	7F	7F	E7	32	BB	..±73i".+ö..ç2»
0001A7F0	D4	5D	F3	51	45	E5	E5	0A	0E	47	19	21	9F	45	43	21	ÔjôQEää..G.!YEC!
0001A800	32	C0	C9	02	E2	1B	6B	99	FF	00	08	A9	13	BF	8C	91	2ÄE.â.k"y..@.¿E'
0001A810	BE	30	78	9D	D8	4C	70	13	36	27	E6	78	9A	45	29	05	%0x.ØLp.6'exšE).
0001A820	39	32	56	03	8A	59	9F	DF	F2	A4	CE	73	38	F1	3B	F9	92V.ŠYšòwššñ;ù
0001A830	40	44	92	11	05	42	2C	B6	FE	53	99	D1	3F	30	AE	01	@D'..B.¶ps"ñ?oø.
0001A840	55	C1	43	33	35	CE	26	E9	E6	71	85	77	48	A8	5C	D4	UÄC35fšéæq..wH"\Ö
0001A850	C1	6F	31	27	37	BA	8F	0C	C2	72	6B	49	71	03	40	68	Áol'7°...ÄrkIq.@h
0001A860	10	53	13	25	68	31	53	FA	98	70	40	47	94	D2	A4	59	.S.%hlšú"p@G"Ömy
0001A870	F0	05	42	12	04	C6	46	69	83	30	90	CD	2A	1A	7B	30	š.B..EFif0.í.{}0
0001A880	47	9F	19	99	89	3A	0D	06	64	64	43	2D	01	29	11	01	çV.¶w:..ddC..)
0001A890	49	6E	69	20	72	61	68	61	73	69	61	20	6A	61	6E	67	Ini rahasia jang
0001A8A0	61	6E	20	62	69	6C	61	6E	67	20	73	69	61	70	61	20	an bilang siapa
0001A8B0	73	69	61	70	61	20	79	61	20	A0	F4	4B	42	19	02	F2	siapa ya öKB..ò
0001A8C0	B0	87	C0	32	55	40	8A	44	16	B3	53	B3	55	75	04	A2	+Ä2UöšD.šsUu..
0001A8D0	60	D4	88	A3	A9	19	06	47	88	3A	31	81	06	1F	44	03	Öf@..G~:1...D.
0001A8E0	4C	A4	11	31	48	12	20	BA	05	EC	24	8B	C0	8A	A0	DD	Lš.lH. °.iš<ÄŠ Ÿ
0001A8F0	4F	15	54	D1	6A	AA	43	5C	7F	AD	9B	11	30	2B	22	40	O.TñjæC\...x.0+"@
0001A900	B8	44	4F	42	44	B9	10	78	17	D7	F1	10	88	81	79	14	,DOBD¹.x.~ñ..y.
0001A910	17	BB	D4	20	22	1C	8B	3C	09	13	87	0B	33	A0	50	0C	..»Ö ".<...+.3 P.
0001A920	E3	39	82	F3	22	03	89	15	1E	64	72	FF	00	1D	AC	6A	š9,6".%.~dry...j
0001A930	6B	D5	DD	C5	53	53	34	D5	55	E5	AA	CD	88	69	18	A3	kÖYÄSS4ÖUÄ*í.i.š
0001A940	60	49	93	40	9D	C4	BE	41	10	22	26	22	42	22	20	88	¹I"®.Ä%A."&"B" ^
0001A950	A8	44	50	61	00	65	88	8C	11	40	8C	D2	2C	88	D8	08	"DPa.e"®.®@Ö,^Ø.
0001A960	B8	13	91	3F	CB	2E	40	8F	62	C1	93	27	12	60	F3	2F	..?E.®.bÄ"'.^ó/

Offset(h): 0

Informasi apa yang diperoleh dari gambar tersebut?

Bukti Elektronik



Bukti elektronik merupakan Informasi Elektronik/Dokumen Elektronik yang dapat diandalkan sebagai bukti. Bukti Elektronik dapat tersimpan dan/atau ditransmisikan melalui sebuah perangkat elektronik, jaringan, atau sistem komunikasi. Data inilah yang dibutuhkan untuk membuktikan sebuah kejahatan yang terjadi di persidangan, bukan bentuk fisik dari perangkat elektroniknya

Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya

Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Apakah perangkat/media yg dijadikan bukti harus asli?

Ketentuan UU ITE



terkait

Bukti Elektronik

Pasal 5 ayat (1)

Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang SAH.

Pasal 6

"Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap **sah** sepanjang informasi yang tercantum di dalamnya:

- dapat diakses;
- ditampilkan;
- dijamin keutuhannya; dan
- dapat dipertanggungjawabkan.

Pasal 6 ayat (4)

Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

- a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan
- b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

SIFAT DASAR BUKTI ELEKTRONIK



Rapuh (rusak, hapus, berubah)



Laten (tersembunyi)



Sensitif terhadap Waktu



Melintas batas yuridiksi

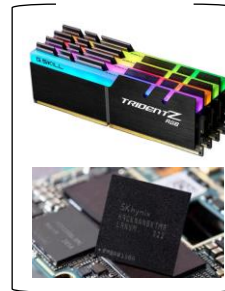
RAPUH - MUDAH DIUBAH/DIRUSAK/DIMUSNAHKAN

Sengaja / Tidak Sengaja

Remote / Jarak Jauh



Volatile



Network configuration
Network connection
Running process
Open file
Login session
Operating system time

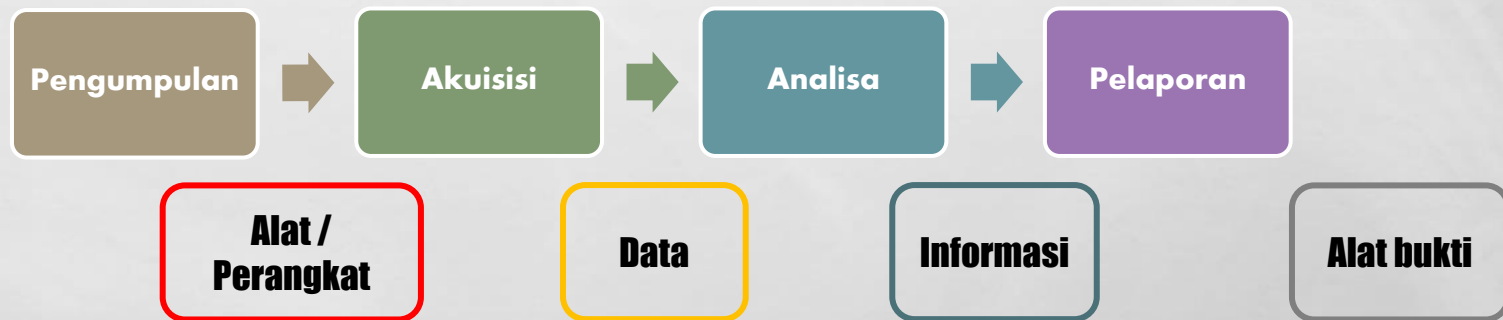
**Non
Volatile**



File konfigurasi
Logs file
Application file
Data file

FORENSIK DIGITAL

Forensik Digital adalah keseluruhan proses dalam mengumpulkan, mengakuisisi, memulihkan, menyimpan, dan memeriksa Informasi dan/atau Dokumen Elektronik yang terdapat dalam Sistem Elektronik, Perangkat Elektronik dan/atau media penyimpanan, berdasarkan cara dan dengan alat yang dapat dipertanggungjawabkan secara ilmiah, dilakukan oleh orang yang memiliki keahlian untuk kepentingan pembuktian di Pengadilan.





Apakah Forensik Digital
hanya untuk Pidana UU ITE ?

Kejahatan Siber

- Kejahatan yang timbul dengan memanfaatkan Teknologi Informasi (Internet)
- Kejahatan Siber merupakan perbuatan melawan hukum dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi



Ruang Lingkup

- Komputer sebagai target, Komputer sebagai alat, Komputer terkait dengan kejahatan

PRINSIP PENANGANAN BUKTI ELEKTRONIK

1

Terpeliharanya
integritas data

ACPO (Association of Chief Police Officers), Inggris, 2012

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.

Google translate :

Tidak ada tindakan yang dilakukan oleh lembaga penegak hukum, orang-orang yang dipekerjakan dalam lembaga-lembaga tersebut atau agen-agen nya yang dapat mengubah data barang bukti yang diandalkan di pengadilan.

Write protect

Imaging

Hashing

PRINSIP PENANGANAN BUKTI ELEKTRONIK

2

Adanya
personel yang
kompeten

ACPO (Association of Chief Police Officers), Inggris, 2012

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.

Google translate :

Dalam keadaan di mana seseorang merasa perlu untuk mengakses data asli, orang tersebut harus kompeten untuk melakukannya dan dapat memberikan bukti yang menjelaskan relevansi dan implikasi tindakan mereka.

PRINSIP PENANGANAN BUKTI ELEKTRONIK

3

Terpeliharanya
*chain of
custody*

ACPO (Association of Chief Police Officers), Inggris, 2012

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.

Google translate :

Jejak audit atau catatan lain dari semua proses yang diterapkan pada bukti digital seharusnya dibuat dan dipelihara. Pihak ketiga yang independen harus dapat memeriksa proses tersebut dan mencapai hasil yang sama.

EVIDENCE	
Agency: _____	
Item No.: _____	Case No.: _____
Date of Collection: _____ Time of Collection: _____	
Collected By: _____	
Description of Evidence: _____	

Location of Collection: _____	

Type of Offense: _____	
Victim: _____	
Suspect: _____	
CHAIN OF CUSTODY	
Received From: _____	By: _____
Date: _____	Time: _____
Received From: _____	By: _____
Date: _____	Time: _____
Received From: _____	By: _____
Date: _____	Time: _____

PRINSIP PENANGANAN BUKTI ELEKTRONIK

4

Kepatuhan
terhadap
regulasi

ACPO (Association of Chief Police Officers), Inggris, 2012

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

Google translate :

Penanggung jawab investigasi (Ketua Tim) bertanggung jawab untuk memastikan keseluruhan kegiatan Forensik Digital mematuhi prinsip dan hukum yang berlaku .



DIGITAL FORENSIK FRAMEWORK

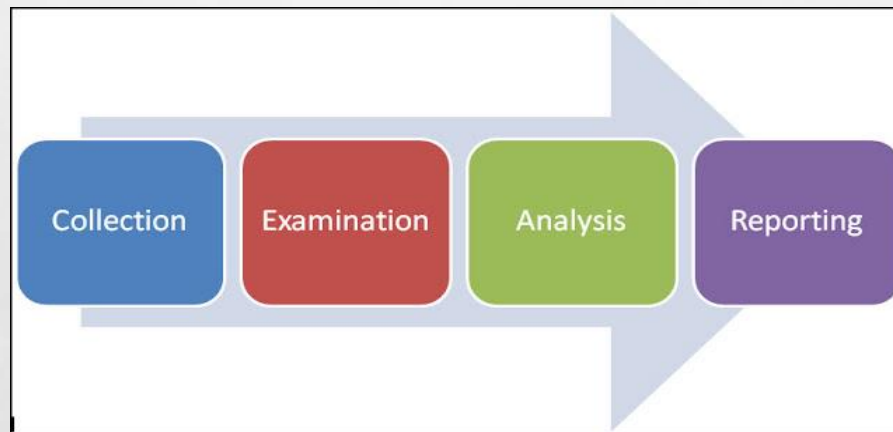
ACPO
Association
Chief
Police
Officers

NIJ
National
Institute
Of Justice

SWGDE
Scientific
Working Group
on Digital
Evidence

NIST
National
Institute of
Standards and
Technology

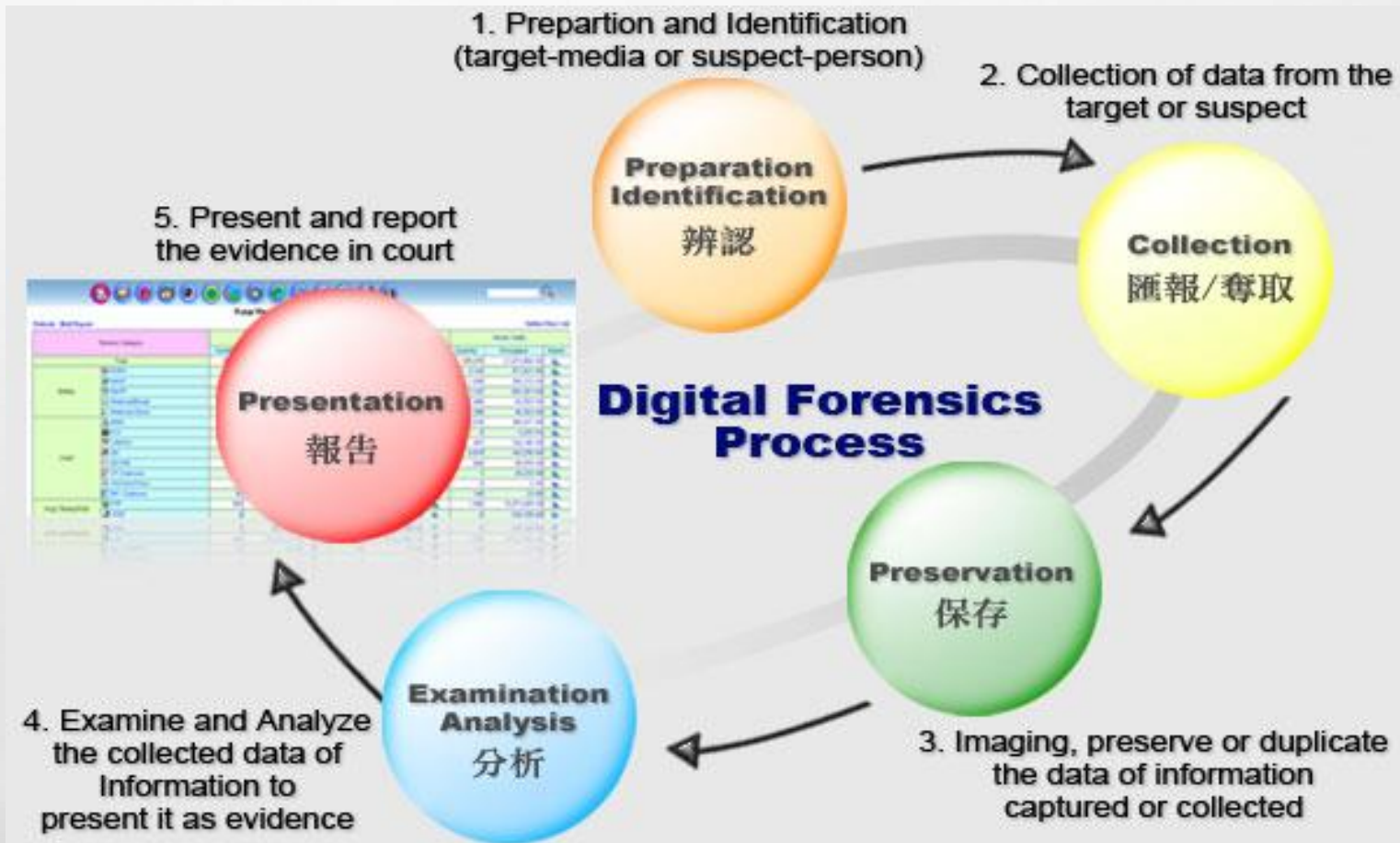
ISO
International
Organization for
Standardization



publication 800-86 Guide to
Integrating Forensic Techniques into
Incident Response

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce





Investigasi Principles and Processes



ISO/IEC 27035
Insident
Management

ISO/IEC 27037
Identification, Collection,
Acquisition &
Preservation of Digital
Evidence

ISO/IEC 27042
Analysis &
Interpretation
of digital
evidence



ISO/IEC 27041 Assuring suitability & adequacy of
investigative methodes

Prosedur Penanganan dan Pemeriksaan Barang Bukti Elektronik di Tempat Kejadian Perkara

Surat Edaran Menteri Kominfo No 4 tahun 2019 tentang Panduan Identifikasi, Koleksi, Akuisisi & Preservasi Bukti Elektronik

Maksud : sebagai acuan dalam penanganan bukti digital di tempat kejadian perkara khususnya mengenai identifikasi, koleksi, akuisisi dan preservasi bukti elektronik

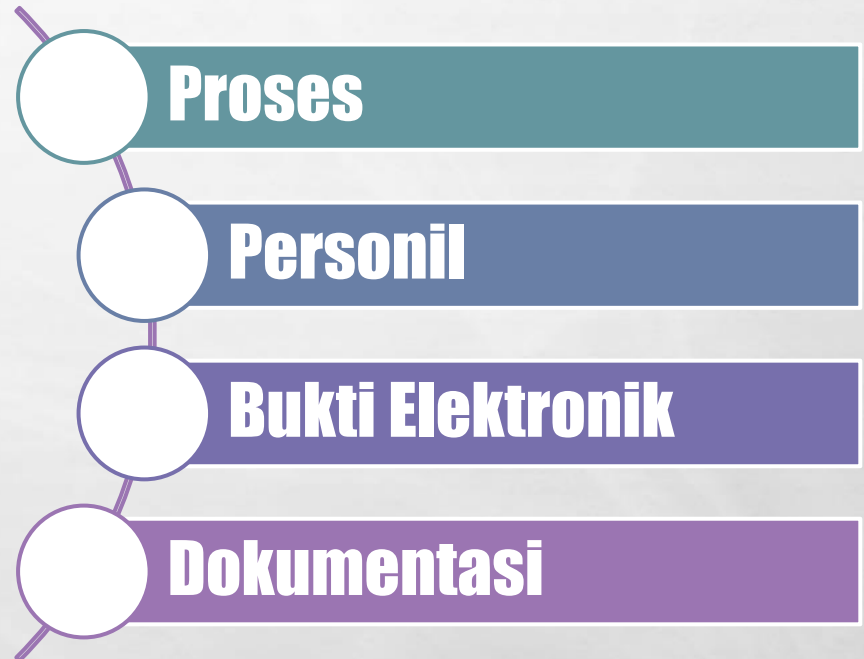
Tujuan :

- 1) Mewujudkan keseragaman dan keterpaduan dalam proses identifikasi, koleksi, akuisisi, dan preservasi bukti digital; dan
- 2) menjamin kesesuaian penerapan dengan ketentuan peraturan perundangan-undangan bidang informasi dan transaksi elektronik

Contents	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative reference	1
3 Terms and definitions	2
4 Abbreviated terms	4

1. Ruang Lingkup
2. Acuan Normative
3. Istilah dan Definisi
4. Istilah singkat
5. Ikhtisar (Overview)
6. Komponen Kunci Identifikasi, Pengumpulan, Akuisisi, Pemeliharaan bukti Digital (Preservation)
7. Contoh Identifikasi, Pengumpulan, Akuisisi dan Pemeliharaan (Preservation)
8. Lampiran A (Informatif) Keterampilan Inti DEFR dan Deskripsi Kompetensi
9. Lampiran B (Informatif) Persyaratan Dokumentasi minimum untuk Transfer Bukti

6.7.5 Other briefing information	15
6.8 Prioritizing collection and acquisition	16
6.9 Preservation of potential digital evidence	17
6.9.1 Overview	17
6.9.2 Preserving potential digital evidence	17
6.9.3 Packaging digital devices and potential digital evidence	17
6.9.4 Transporting potential digital evidence	18
7 Instances of identification, collection, acquisition and preservation	19
7.1 Computers, peripheral devices and digital storage media	19
7.1.1 Identification	19
7.1.2 Collection	21



ISO / SNI 27037

- Mencari
- Mengenal
- Mendokumentasikan

Perangkat penyimpan
dan/atau pengolah data

- Membuat prioritas berdasar volatilitas,
- Identifikasi bukti tersembunyi

Menyalin Bukti Digital

Dokumentasi Metode dan Aktivitas
Jelas dan Rinci
(dapat dipraktikkan, direproduksi, diverifikasi)

Proses tidak sebabkan perubahan data Asli
Hasil harus diverifikasi (sama)

Identifikasi

Koleksi

Akuisisi

Preservasi

Perangkat di TKP

Laboratorium

Prosedur pengumpulan bukti : menyala dan mati,
Dokumentasi Perangkat,
Proses Pengemasan

Bukti Digital + Perangkat

Dilakukan sejak awal (Identifikasi)

Dibuktikan tidak ada Perubahan
Jika ada perubahan => dijelaskan

Digital Evidence First Responder (DEFR)

- ☐ Individu yang berwenang, terlatih dan memiliki kemampuan untuk melakukan tindakan pertama di lokasi
- ☐ Pengumpulan Bukti Digital dan Akuisisi

Digital Evidence Specialist (DES)

- ☐ Individu yang dapat melaksanakan tugas - tugas DEFR
- ☐ Memiliki spesialisasi pengetahuan, keterampilan dan kemampuan untuk menangani berbagai masalah teknis.

Bukti Elektronik

- ❖ Berhubungan langsung terhadap suatu unsur dalam kasus
- ❖ Dapat digunakan untuk membuktikan suatu unsur dalam suatu kasus

Relevansi (relevance)

Kecukupan (Sufficiency)

- ☐ mempertimbangkan bahwa materi yang telah dikumpulkan cukup untuk memungkinkan pelaksanaan penyelidikan yang tepat
- ☐ DEFR harus dapat melalui audit dan justifikasi

Kehandalan (Reliability)

- Kesamaan hasil ketika dilakukan analisis menggunakan lingkungan testing yang sama secara berulang
- Kesamaan hasil ketika dilakukan analisis menggunakan lingkungan testing yang berbeda

DOKUMENTASI

CHAIN OF CUSTODY

- Foto, Video, Gambar sketsa, tulisan;
- Identifikasi bukti yang unik;
- Siapa yang mengakses bukti, kapan dan dimana dilakukan pengaksesan;
- Siapa yang memeriksa bukti baik diluar maupun didalam fasilitas pemeliharaan bukti, kapan dilakukan;
- Mengapa bukti tersebut perlu diperiksa (tujuan pemeriksaan) dan relevansi pemeriksaan;
- Setiap perubahan yang tidak dapat dihindari pada bukti digital, nama individu yang bertanggung jawab serta justifikasi terhadap perubahan yang terjadi.

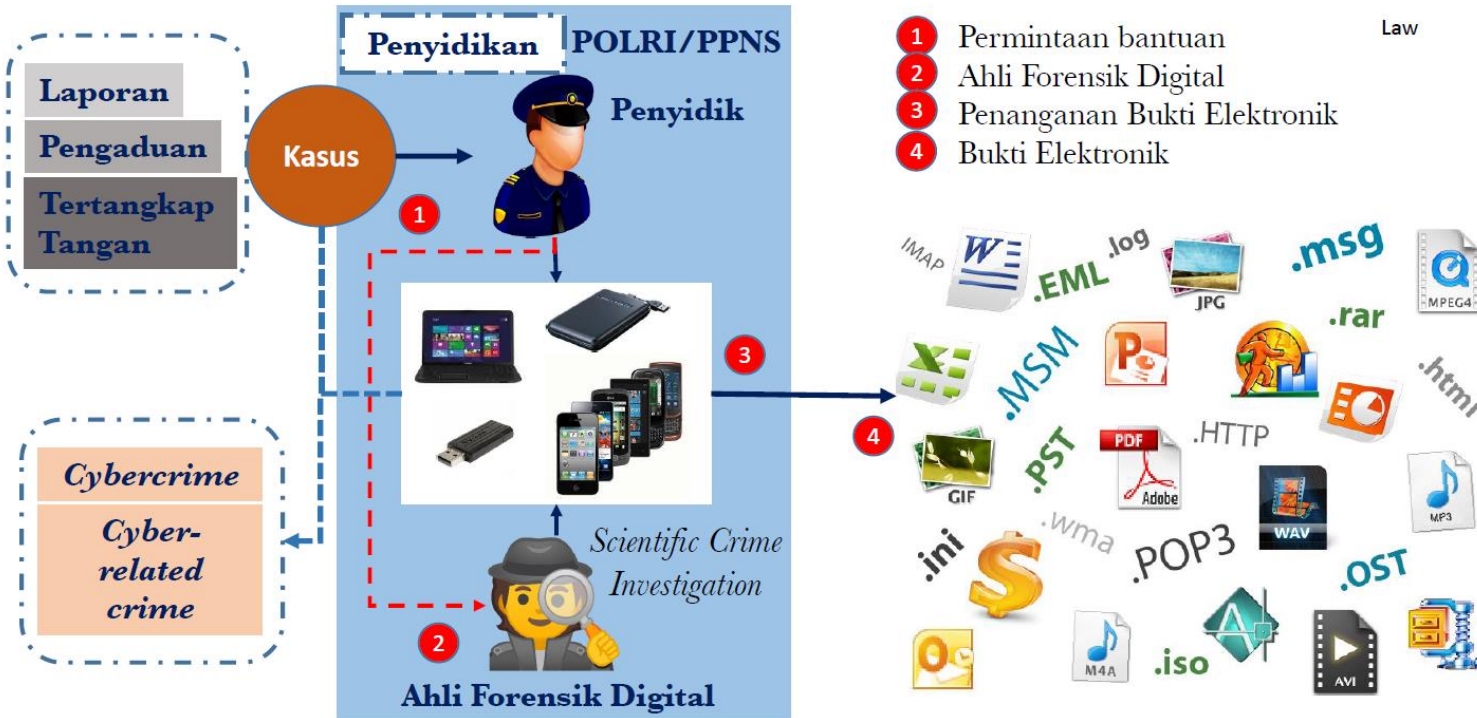
CoC harus dapat dipertahankan selama life time
bukti dan disimpan untuk jangka waktu tertentu

Hard Drive/Computer Details			
Description:			
Manufacturer:		Model #:	
		Serial #:	
Chain of Custody			
Date/Time:	From:	To:	Reason:
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	

Scientific Crime Investigation

Scientific

Law





Terima Kasih

