

CYBER CRIME, BUKTI ELEKTRONIK, DAN DIGITAL FORENSIC

(PENGANTAR DAN ASPEK LEGAL)

TEGUH ARIFIYADI, S.H. M.H., CEH., CHFI
Deputy Director For Cyber Crime Investigation



TEGUH ARIFIYADI

- LAW FACULTY, UNIVERSITY OF DIPONEGORO, CYBER CRIME
- MASTER OF LAW, UNIVERSITY OF INDONESIA, ECONOMIC LAW-INFORMATION SYSTEM

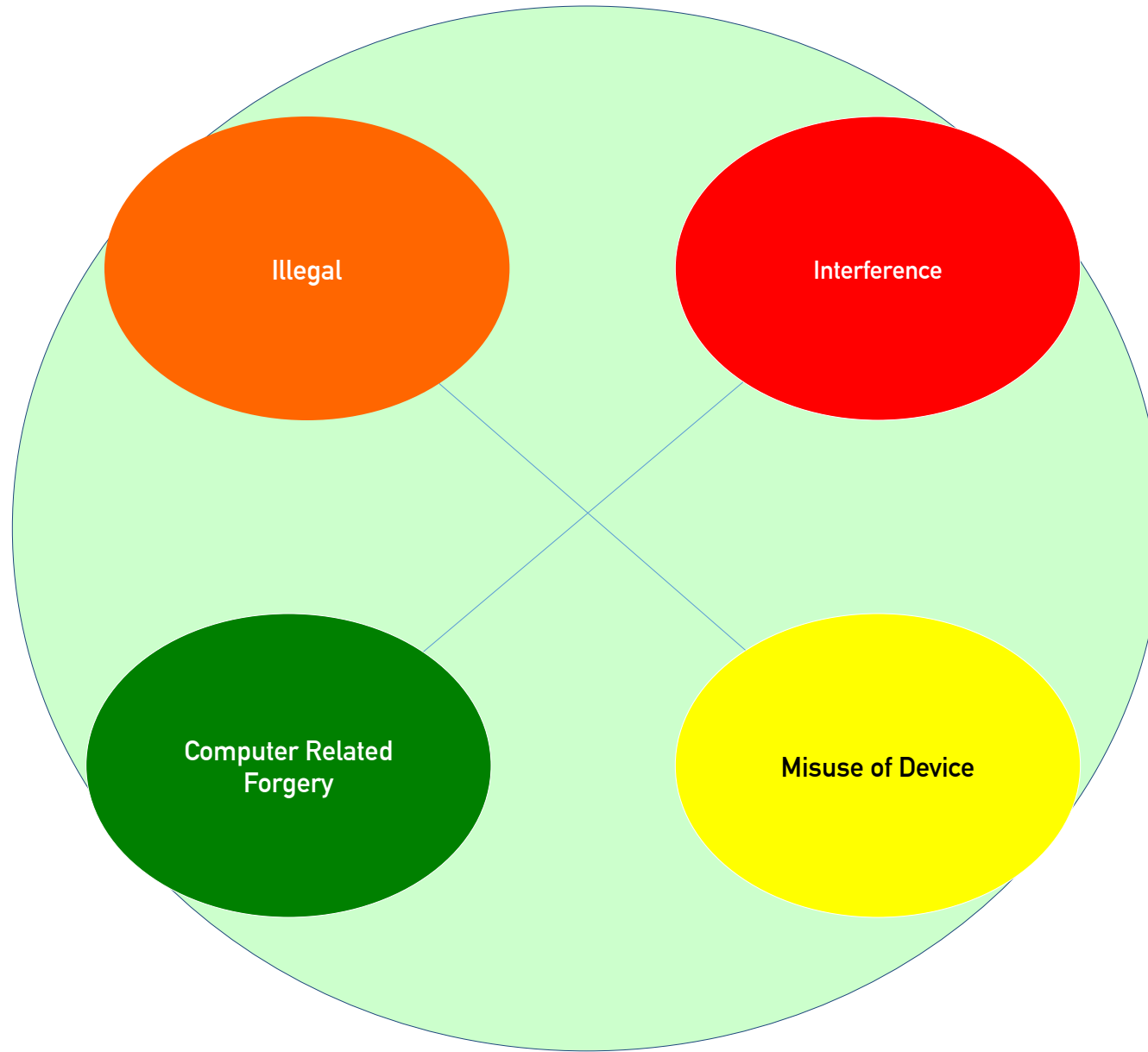
INFORMAL

- CERTIFIED HACKING FORENSIC INVESTIGATOR (CHFI), EC COUNCIL, JAKARTA;
- CERTIFIED ETHICAL HACKER (CEH), EC COUNCIL, JAKARTA;
- CERTIFIED INFORMATION SYSTEM AUDITOR (CISA) REVIU, BANDUNG;
- CERTIFIED OF CIVIL INVESTIGATOR, BARESKRIM, BOGOR;
- SMART CARD TECHNOLOGY, SEOUL, KOREA
- COUNTERFITING AND PIRACY, PARIS, FRANCE
- FUTURE NETWORK, INTERNATIONAL TELECOMMUNICATION UNION, GENEVA, SWITZERLAND
- LAWFULL INTERCEPTION, SS8, BANDUNG
- LAWFULL INTERCEPTION, ISS WORLD TRAINING, PRAGUE, CZECH REPUBLIC
- PROTOCOL TESTING, INTERNATIONAL TELECOMMUNICATION UNION, GENEVA, SWITZERLAND
- ELECTROTECHNICAL STANDAR DEVELOPMENT TRAINING, SINGAPORE
- COPY RIGHT ON IEC STANDARD DOCUMENTS, TOKYO, JAPAN
- LAWFULL INTERCEPTION, ISS WORLD TRAINING, JOHANNESBURG, SOUTH AFRICA
- TECHNOLOGY TRANSFER, D-8 MEMBER COUNTRIES, TEHRAN, I.R. IRAN
- INTERNATIONAL VISITOR LEADERSHIP PROGRAM ON CYBER SECURITY, WASHINGTON DC, UNITED STATE OF AMERICA.

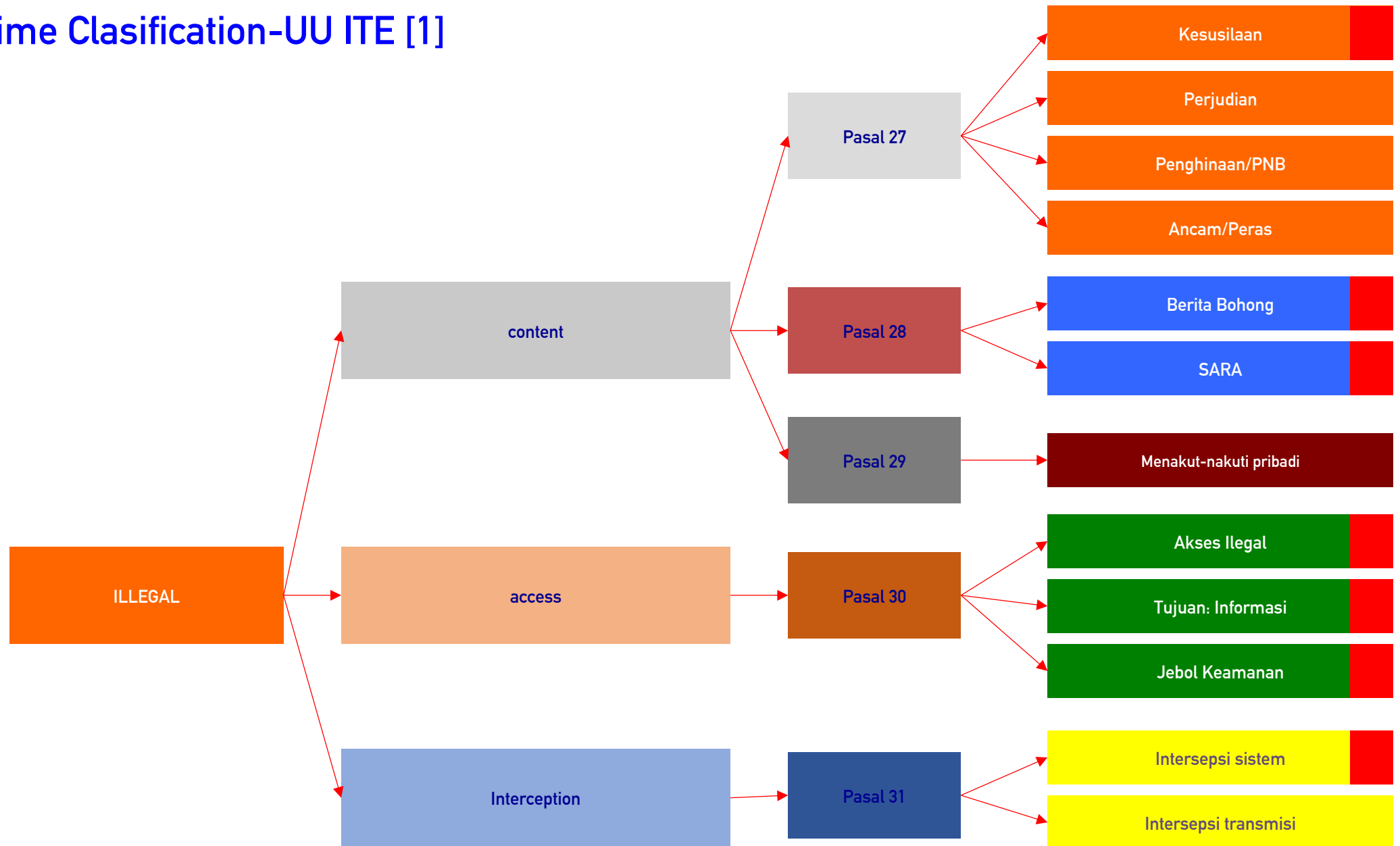
ACTIVITIES

- CHAIRMAN OF INDONESIA CYBER LAW COMMUNITY (ICLC) [www.cyberlawindonesia.net]
- ADVISOR AT ARSA LAW FIRM
- HEAD OF LEGAL AND ETHICS INDONESIA DIGITAL FORENSIC ASSOCIATION (AFDI)
- DEPUTY DIRECTOR FOR CYBER CRIME INVESTIGATION AND LAW ENFORCEMENT MINISTRY OF ICT
- WRITER ON LAW CLINIC [www.hukumonline.com]
- CYBER LAW EXPERT ON THE COURT
- TRAINER

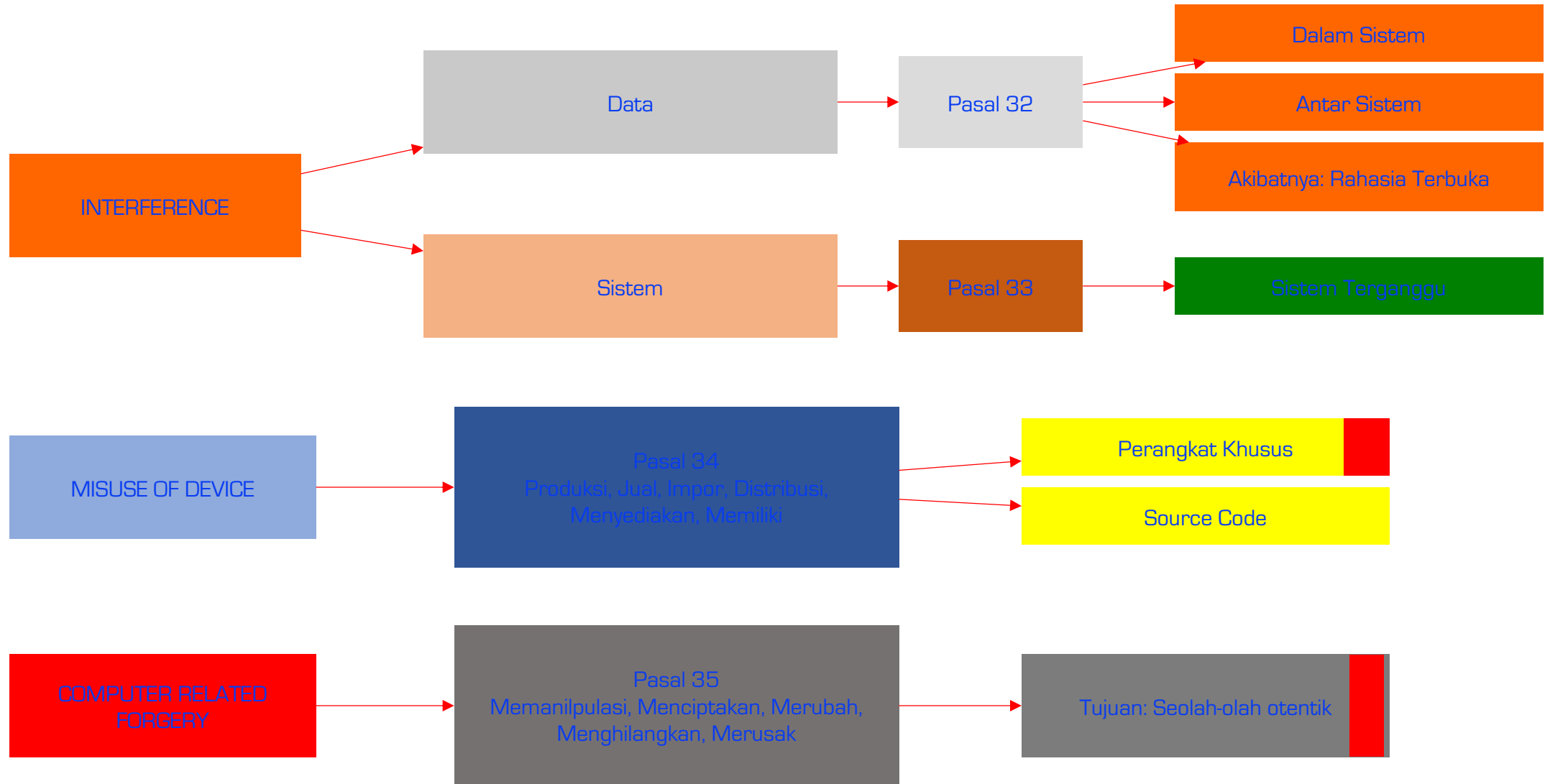
Kluster Tindak Pidana ITE



IT & ET Crime Clasification-UU ITE [1]



IT & ET Crime Clasification-UU ITE [2]



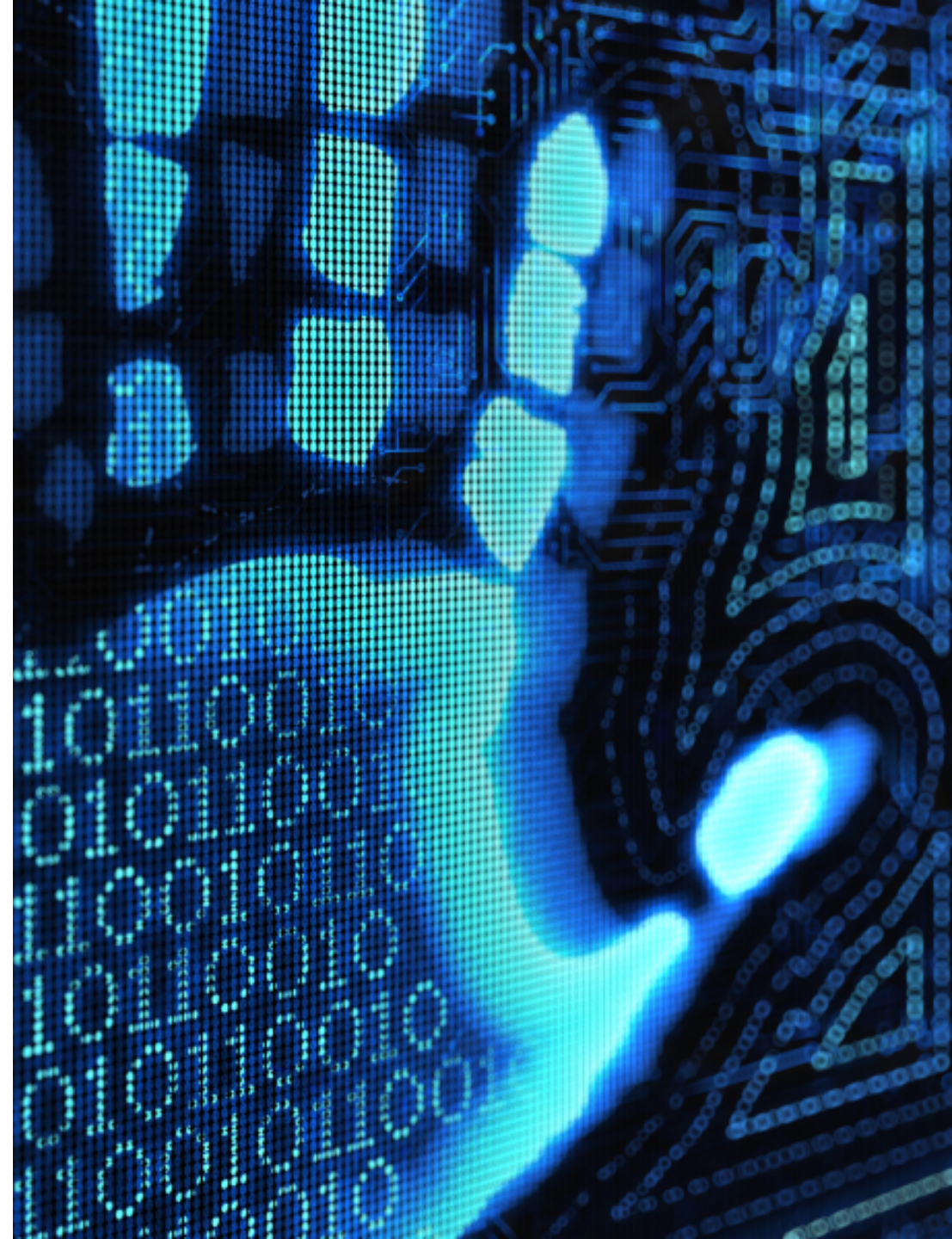
Karakter dan Tantangan Bukti Elektronik

Karakter

1. Dapat berubah/Diubah/Dimanipulasi
2. Salah Penanganan akan rusak
3. Bersifat mekanis – elektromekanis
4. Umumnya dapat di recovery

Tantangan

1. Enkripsi/Proteksi
2. Data pada Cloud
3. Volume
4. dll





PENYIMPANAN BUKTI DIGITAL



Memilih media Penyimpan Seberapa lama bukti digital harus disimpan

Media penyimpanan	Kapasitas	Ketahanan (thn)
Floppy Disk-Disket	1.44 MB	1-2
Harddisk	250 GB – 6 TB	12 - 15
CD	700 MB	1-3
DVD	4 GB – 16 GB	10 – 50
Flashdisk	1-256 GB	5-10
Memmmory Card	256 MB – 64 GB	5-10
RAID SISTEM	> 6 TB	> 50

- Tidak menyimpan hanya dalam satu media penyimpanan
- Menggunakan peralatan yg berbeda dalam membuat 2 image

Sistem dan/atau Bukti Elektronik yang Ideal dalam Pembuktian?

Audit Ready

Digital Forensic Ready

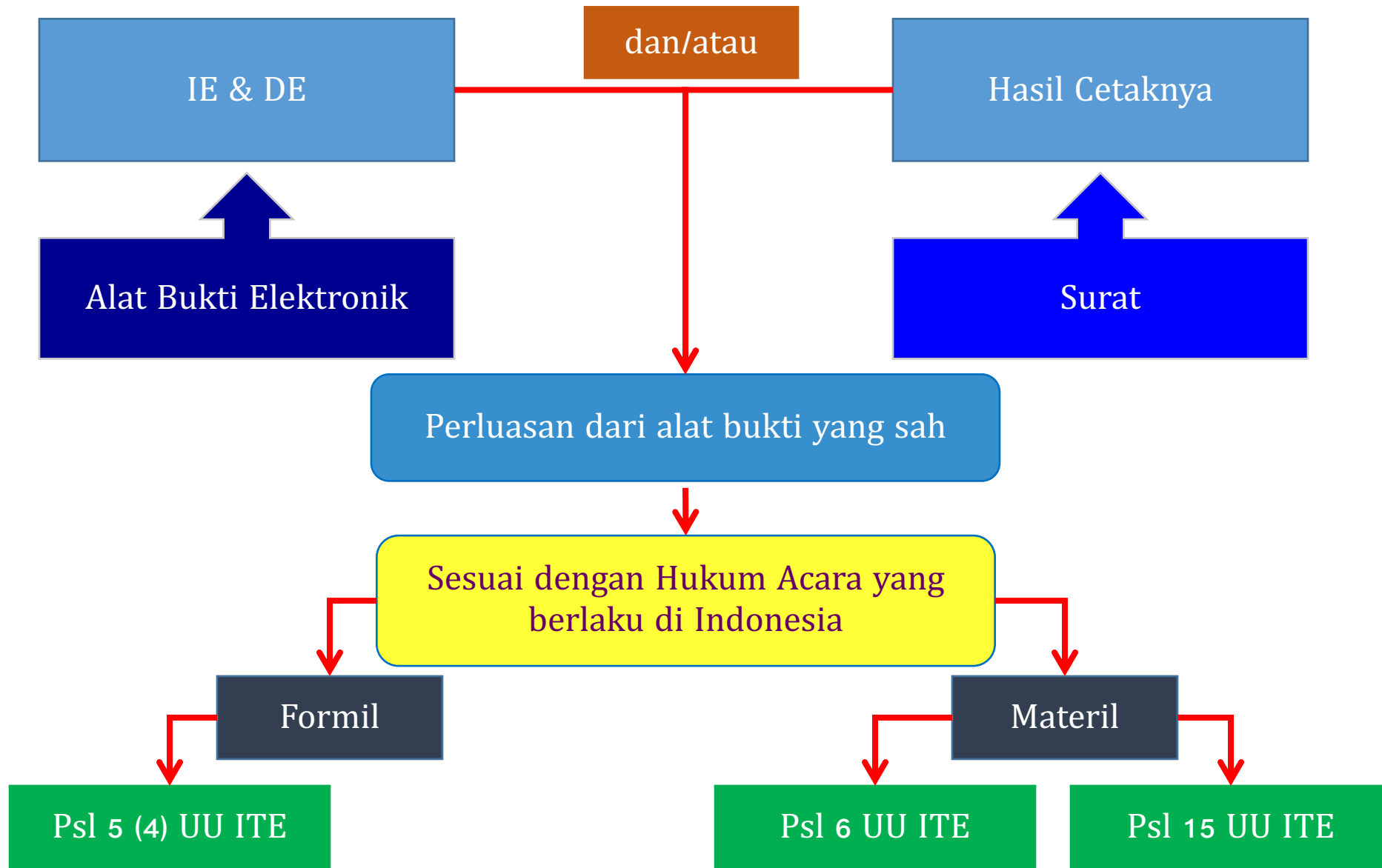
Dasar Hukum

Pasal 15 ayat (1) UU ITE
Pasal 14 dan 18 PP PSTE



1. memelihara log transaksi sesuai kebijakan retensi data penyelenggara, sesuai ketentuan peraturan perundang-undangan;
2. memberikan notifikasi kepada konsumen apabila suatu transaksi telah berhasil dilakukan;

Konsep Bukti Elektronik dalam UU ITE



Syarat Sah Bukti Elektronik



UU ITE

Pasal 5 UU ITE



Konsep Dasar Bukti Elektronik



Bukti Elektronik



Informasi Elektronik

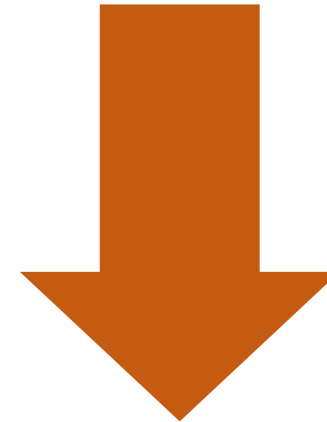
Dokumen Elektronik



Bukti Digital



Perangkat Elektronik



Barang Bukti

Isu Bukti Elektronik

- Bukti Elektronik Wajib di cetak?
- Bukti Elektronik yang Tidak di cetak?
- Dispute atas bukti cetak?
- Tata Cara bukti elektronik di bawa ke Pengadilan?
- Apakah sah menyajikan bukti elektronik yang tidak melalui proses uji Digital Forensik?



Standardisasi Ahli

Siapa yang dapat disebut Ahli Digital Forensik?

Persyaratan Utama Ahli:

- Akademis [Pendidikan, Sertifikasi]
- Praktis [Praktik Bidang terkait]

Persyaratan Pendukung:

- ditetapkan dalam SK/Surat Perintah otoritas [syarat formil]
- Keanggotaan Profesional

Pengambilan Bukti Digital oleh Ahli Digital Forensik

[Aspek Hukum dan Standard Apa yang harus diperhatikan]



Aspek Hukum

- Syarat Formil
- Privasi
- Dokumentasi
- Pelayanan Publik

Pemenuhan Standard dan SOP

- Standard Nasional / Internasional
- SOP Internal
- Sertifikasi Lab

DIGITAL FORENSICS STANDARDS & GUIDELINES

- **NIST:** National Institute of Standard Technology (CFTT, NSRL, CReDS)
- **NIJ:** National Institute of Justice (Several Standards, National Criminal Justice Reference Service)
- **IOCE:** International Organization on Computer Evidence
- **ASCLD/LAB:** American Society of Crime Laboratory Directors/Laboratory Accreditation Board
- **ASTM:** E2678 standard; Guide for Education & Training
- **ISO SC 27 CSI: 17025** General requirements for the competence of testing and calibration laboratories
- **AES:** Audio Engineering Society (Authentication of Analog tape)
- **SWGDE & SWGIT:** Scientific Working Group on Digital Evidence & Scientific Working Group on Imaging Technology
- **ACPD:** Association of Chief Police Officers
- **DSCI** Manual India (Not specific standards but Manual)



Contoh Standard Eksisting

SOP Forensik Digital Puslabfor Mabes Polri

- Akuisisi HD, FD, MemCard
- Analisa HD, FD, MemCard
- Akuisisi HP dan SimCard
- Analisa HP dan SimCard
- Analisa Audio Forensik
- Akuisisi langsung Komp
- Komitmen jam kerja
- Prosedur Analisa Forensic

PSO Direktorat Pengendalian Aplikasi Informatika Kementerian Kominfo

- Prosedur Berbasis TKP
 - Perlindungan Barang Bukti
 - Pembuatan Image Live Memory
 - Imaging dan Preview
- Prosedur Berbasis Laboratorium
 - Persiapan Pengujian: workstation
 - Inspeksi Fisik
 - Media Write Protecting
 - Wiping Media, dll



Badan Standardisasi Nasional
National Standardization Agency of Indonesia

[Beranda](#) [Komtek](#) [PNPS](#) [RSNI](#) **[SNI](#)** [Jajak Pendapat](#) [Regulasi](#) [LPK](#) [Dok & Panduan](#)

[SNI](#) > [Detail SNI](#)


Informasi Penting

Mulai Tahun 2013, website BSN akan menyediakan full text akses SNI yang baru ditetapkan selama 1 tahun. Terimakasih

SNI hasil adopsi badan standar asing tidak dapat kami tampilkan semua secara fulltext, terkait peraturan hak cipta di masing-masing Organisasi Pengembang Standar.

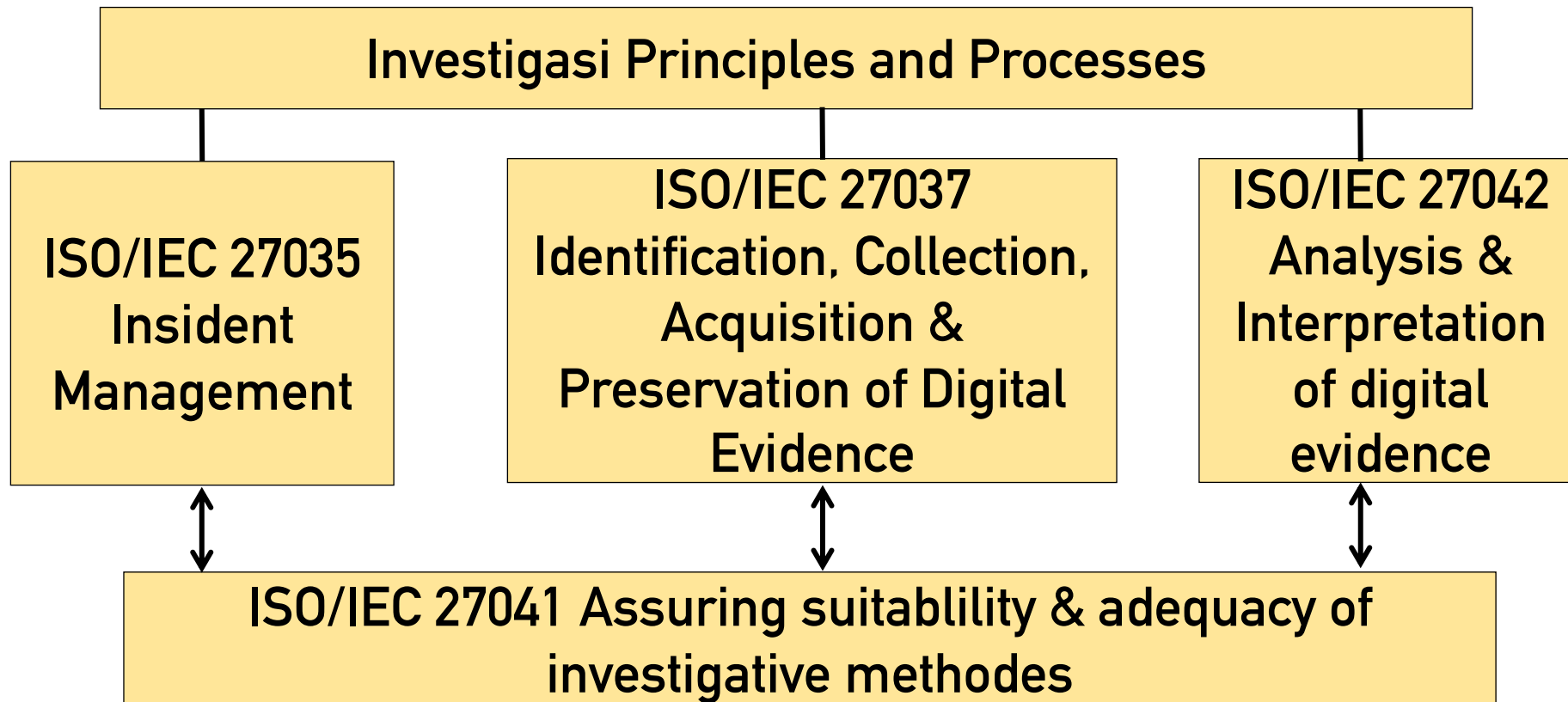
Dokumen SNI yang tidak tersedia secara online dapat diperoleh (sesuai ketentuan yang berlaku) di:
Perpustakaan BSN,
[email:dokinfo@bsn.go.id](mailto:dokinfo@bsn.go.id),
phone: +62 21 3927422 ext 222

Detail SNI

Nomor SNI	SNI ISO/IEC 27037:2014
Judul	Teknologi Informasi - Teknik keamanan - Pedoman identifikasi, pengumpulan, akuisisi dan preservasi bukti digital (ISO/IEC 27037:2012, IDT)
Abstraksi	
Komite Teknis	35-01 Teknologi Informasi
ICS	1. 35.040 Set huruf dan pengkodean informasi
SK Penetapan	37/KEP/BSN/3/2014 
Tanggal Penetapan	24-March -2014
Acuan Non SNI	<ol style="list-style-type: none">1. ISO/IEC 17020, Conformity assessment - Requirements for the operation of various types of bodies performing inspection2. ISO/IEC 27000:2012, Information technology – Security techniques – Information security management systems – Overview and vocabulary3. ISO/TR 15801, Document management - Information stored electronically - Recommendations for trustworthiness and reliability4. ISO/IEC 17025:2005, General requirement for the competence of testing and calibration laboratories

SNI/ ISO IEC 27037

Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence



Bagaimana?

- Mencari
- Mengenali
- Mendokumentasikan

Perangkat penyimpan
dan/atau pengolah data

- Membuat prioritas berdasar volatilitas,
- Identifikasi bukti tersembunyi

Bagaimana
Menyalin Bukti Digital?

Dokumentasi Metode dan Aktifitasnya
Harus Jelas dan Rinci
(dapat dipraktekan, direproduksi, diverifikasi)

- Proses tidak menyebabkan perubahan data Asli
- Hasil harus bisa diverifikasi (sama)

TAHAPAN

Identifikasi

Koleksi

Akuisisi

Preservasi

Teknik mengambil Perangkat di TKP → Pengujian di Laboratorium

Bagaimana Prosedur pengumpulan bukti?
Misal jika perangkat menyala atau mati?
Bagaimana Dokumentasi Perangkat?
Bagaimana Proses Pengemasan Bukti?

Apa saja yang disajikan dalam laporan?

Bukti Digital + Perangkat

Proses yang dilakukan
sejak awal (Identifikasi)

Dibuktikan tidak ada Perubahan
Jika ada perubahan => dijelaskan

SE Menkominfo No. 04/2019
Standard Penanganan Pertama Bukti
Digital untuk kebutuhan Penegakan
Hukum sesuai SNI/ISO 27037

Kompetensi Personil

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 Digital

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

Relevansi (relevance)

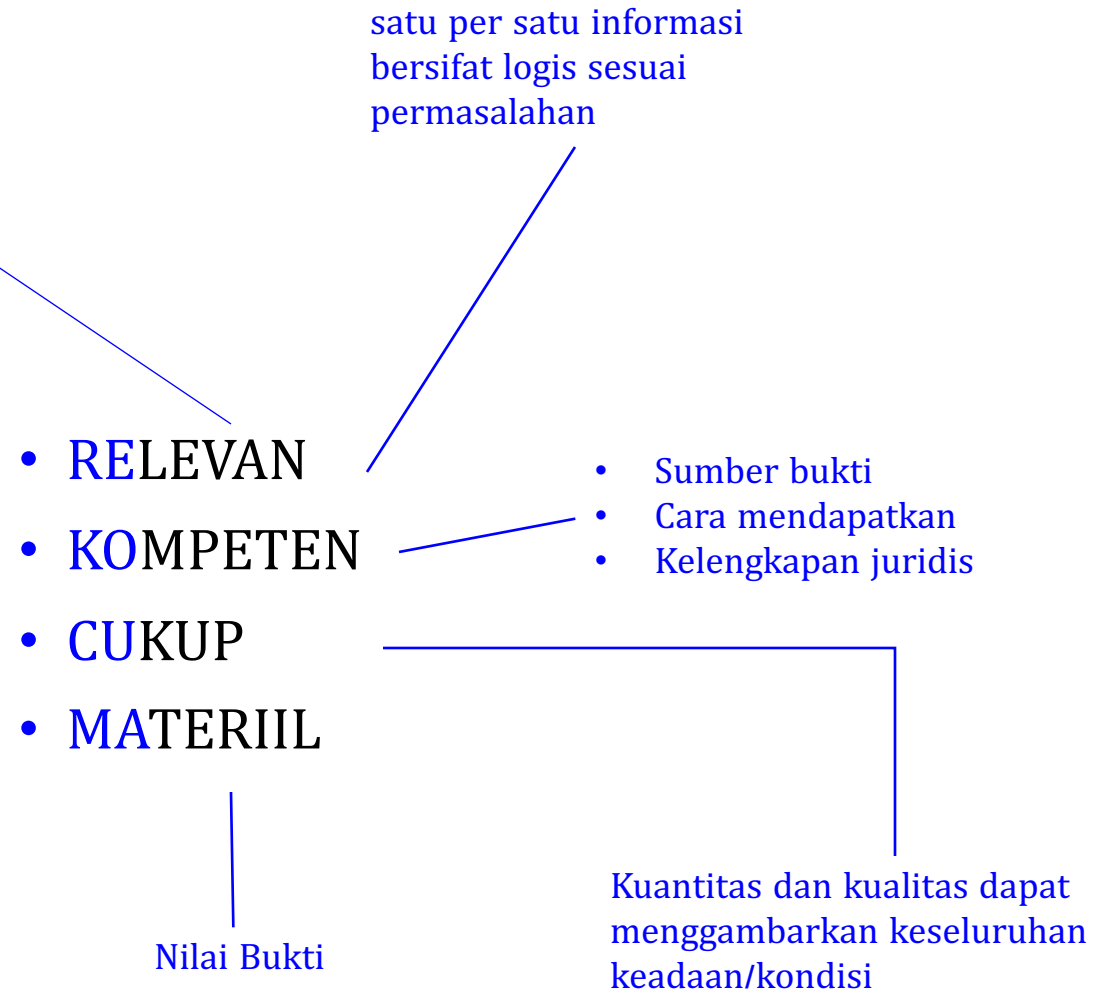
Kecukupan (Sufficiency)

- ❑ 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

Menilai Bukti Digital



Konteks Pengumpulan Bukti Digital



4 (Empat) Aspek utama Penanganan Bukti Digital

Auditability

- Independent assessment => scientific method, technique or procedure was followed

Repeatability

- Same test results are produced : same measurement procedure and method; same instruments and under the same conditions; Can be repeated at any time.

Reproducibility

- Same test results are produced : same measurement method; different instruments and under different conditions; Can be reproduced at any time.

Justifiability

- The DEFR should be able to justify all actions and methods used

terima kasih

teguh.arifiyadi@kominfo.go.id

0818 140 188