

BUKTI ELEKTRONIK DAN DIGITAL FORENSIC

(TANTANGAN STANDARDISASI DAN ASPEK LEGAL)



Teguh Arifiyadi, S.H. M.H. CEH., CHFI
Kepala Subdit Penyidikan dan Penindakan
Kementerian Kominfo



TEGUH ARIFIYADI

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

INFORMAL TRAINING AND EXPERIENCES

- CERTIFIED HACKING FORENSIC INVESTIGATOR (CHFI), EC COUNCIL, JAKARTA;
- CERTIFIED ETHICAL HACKER (CEH), EC COUNCIL, JAKARTA;
- CERTIFIED INFORMATION SYSTEM AUDITOR (CISA) REVIU AND TRAINING, 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;
- CYBER LAW INTERNATIONAL-CYBER OPERATIONS, VIRTUAL EXECUTIVE COURSE, DEPARTEMENT OF FOREIGN AFFAIRS AND TRADES AUSTRALIA.
- ETC.

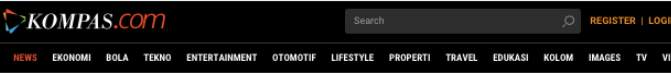
ACTIVITIES

- CHAIRMAN OF INDONESIA CYBER LAW COMMUNITY (ICLC)
[www.cyberlawindonesia.net]
- 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
- TRAINER





2. Kasus Kaesang di-SP3



News / Megapolitan
Kuasa Hukum Buni Yani Merasa Diuntungkan Kesaksian Ahli ITE



Liputan6.com

FOTO: Sidang Kasus Hoaks, Ratna Sarumpaet Hadirkan Saksi Ahli dan ...





Karakter dan Tantangan Bukti Elektronik

Karakter

- Dapat berubah/Diubah/Dimanipulasi
- Salah penanganan akan rusak/hilang
- Bersifat mekanis – elektromekanis
- Umumnya dapat di recovery

Tantangan

- Enkripsi/Proteksi
- Data pada Cloud yang borderless
- Volume
- dll

Sistem Elektronik?

Dokumen Elektronik?

Informasi Elektronik?

Data Elektronik?

Bentuk Bukti Elektronik

Tanda Foto
Simbol Angka Email Rancangan Peta Tulisan Gambar
Teleks Telegram Telecopy Suara
Kode Akses Electronic Data Interchange Huruf
Perforasi

Data Elektronik

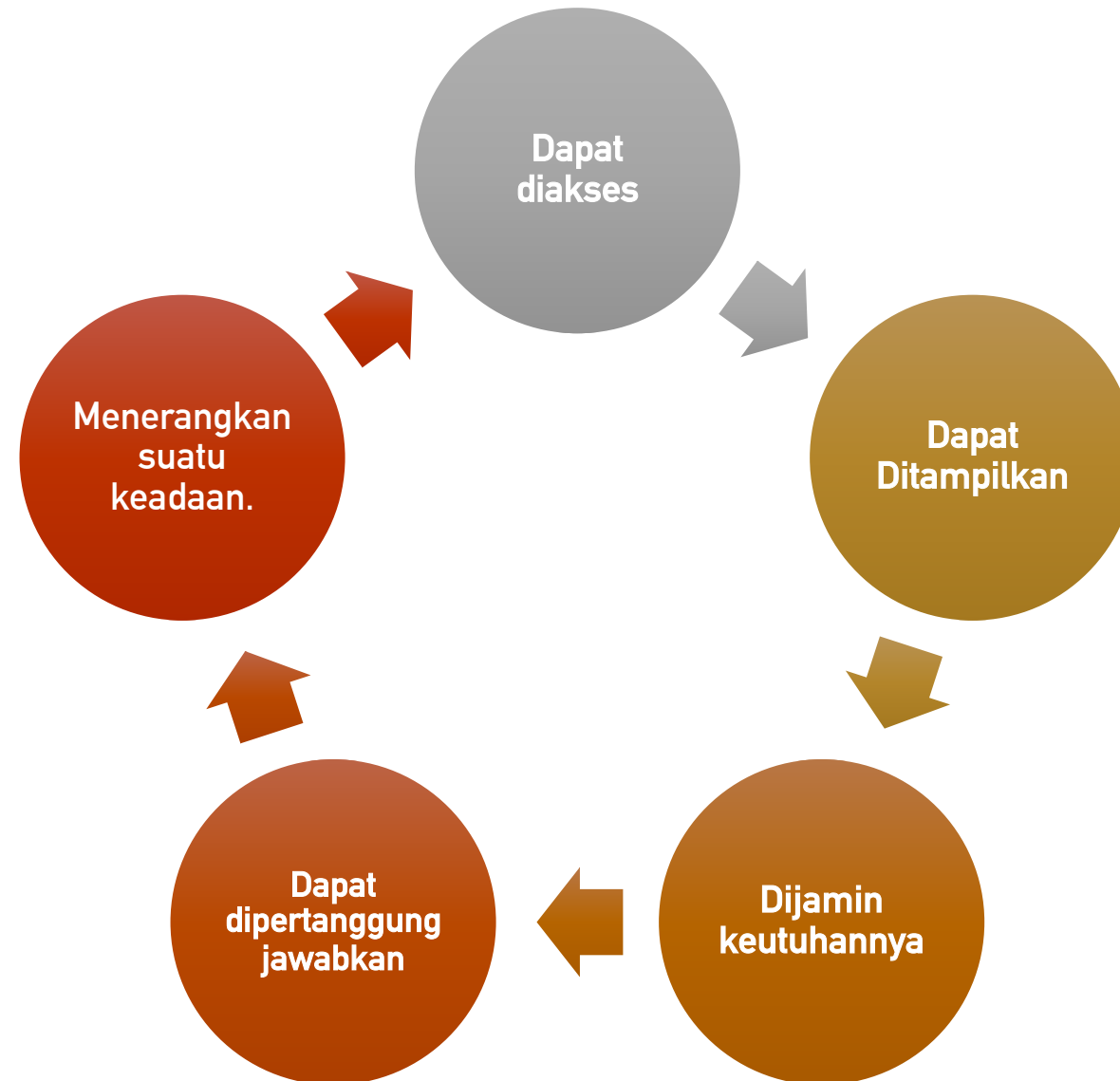
Data Elektronik Data Elektronik
Data Elektronik Data Elektronik
Data Elektronik

Informasi Elektronik

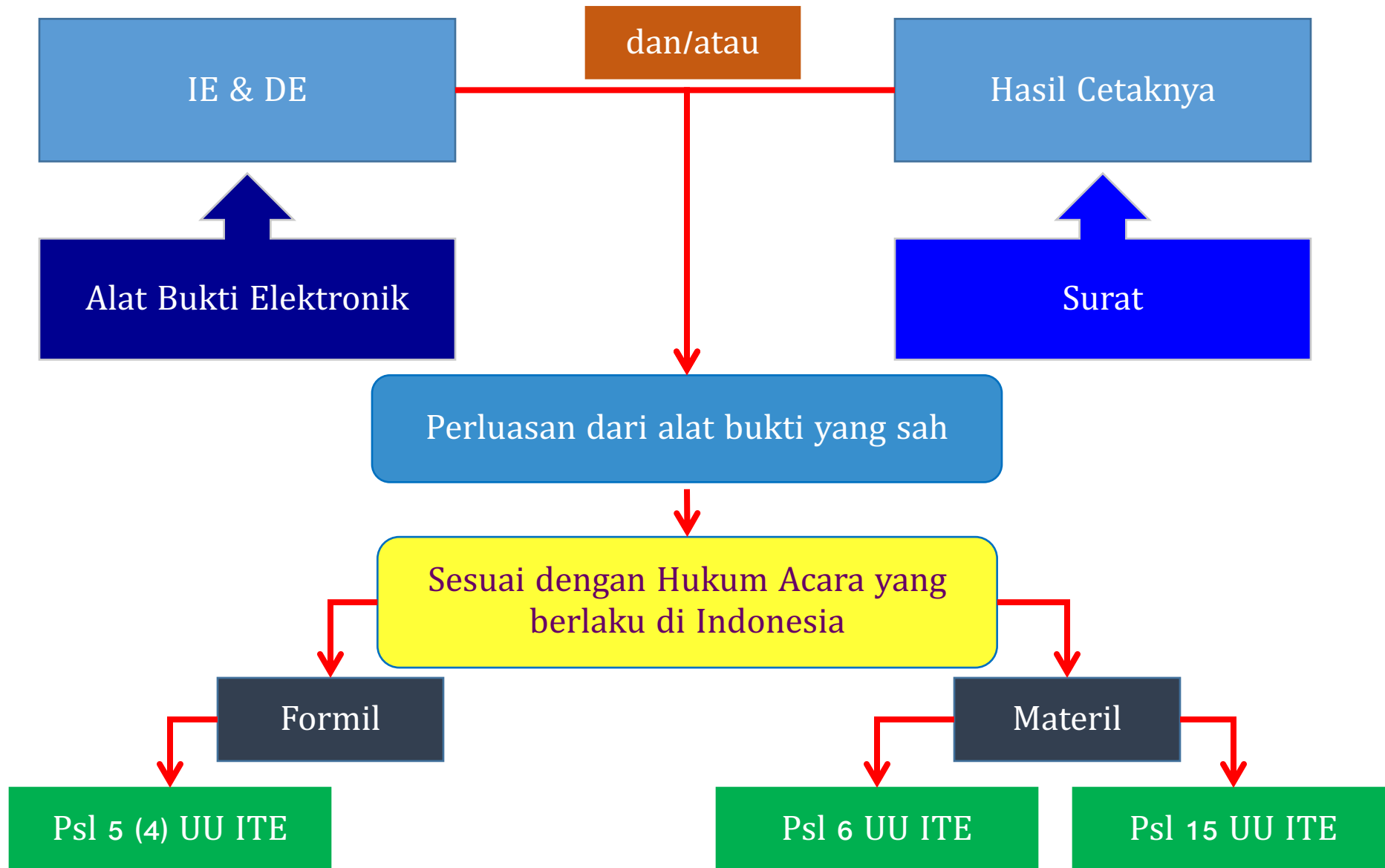
Informasi Elektronik Informasi Elektronik
Informasi Elektronik Informasi Elektronik

Dokumen Elektronik

Syarat Sah Bukti Elektronik



Konsep Bukti Elektronik dalam UU ITE



UU ITE



Isu Bukti Elektronik

- Bukti Elektronik Wajib di cetak?
- Penyitaan akun dan kata sandi?
- Dispute atas bukti cetak?
- Tata cara menyajikan bukti elektronik di bawa ke Pengadilan?
- Apakah sah menyajikan bukti elektronik yang tidak melalui proses uji Digital Forensik?

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, CFReDS)
- **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
- **ACPO:** Association of Chief Police Officers
- **DSCI Manual India** (Not specific standards but Manual)

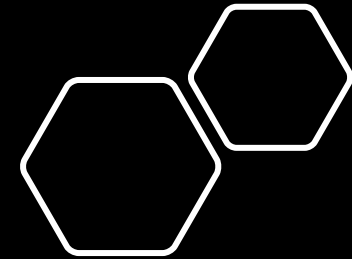




**MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA**

- Kepada Yth.
1. Ketua Mahkamah Agung Republik Indonesia;
 2. Jaksa Agung Republik Indonesia;
 3. Kepala Kepolisian Republik Indonesia;
 4. Ketua Komisi Pemberantasan Korupsi;
 5. Para Pimpinan Kementerian/Lembaga;
 6. Para Akademisi; dan
 7. Para Penggiat Teknologi Informasi.

**SURAT EDARAN
MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA
NOMOR 04 TAHUN 2019
TENTANG
PANDUAN IDENTIFIKASI, KOLEKSI, AKUISISI, DAN PRESERVASI
BUKTI DIGITAL**



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, 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 inspection 2. ISO/IEC 27000:2012, Information technology – Security techniques – Information security management systems – Overview and vocabulary 3. ISO/TR 15801, Document management - Information stored electronically - Recommendations for trustworthiness and reliability 4. ISO/IEC 17025:2005, General requirement for the competence of testing and calibration laboratories

INTERNATIONAL
STANDARD

ISO/IEC
27037

First edition
2012-10-15

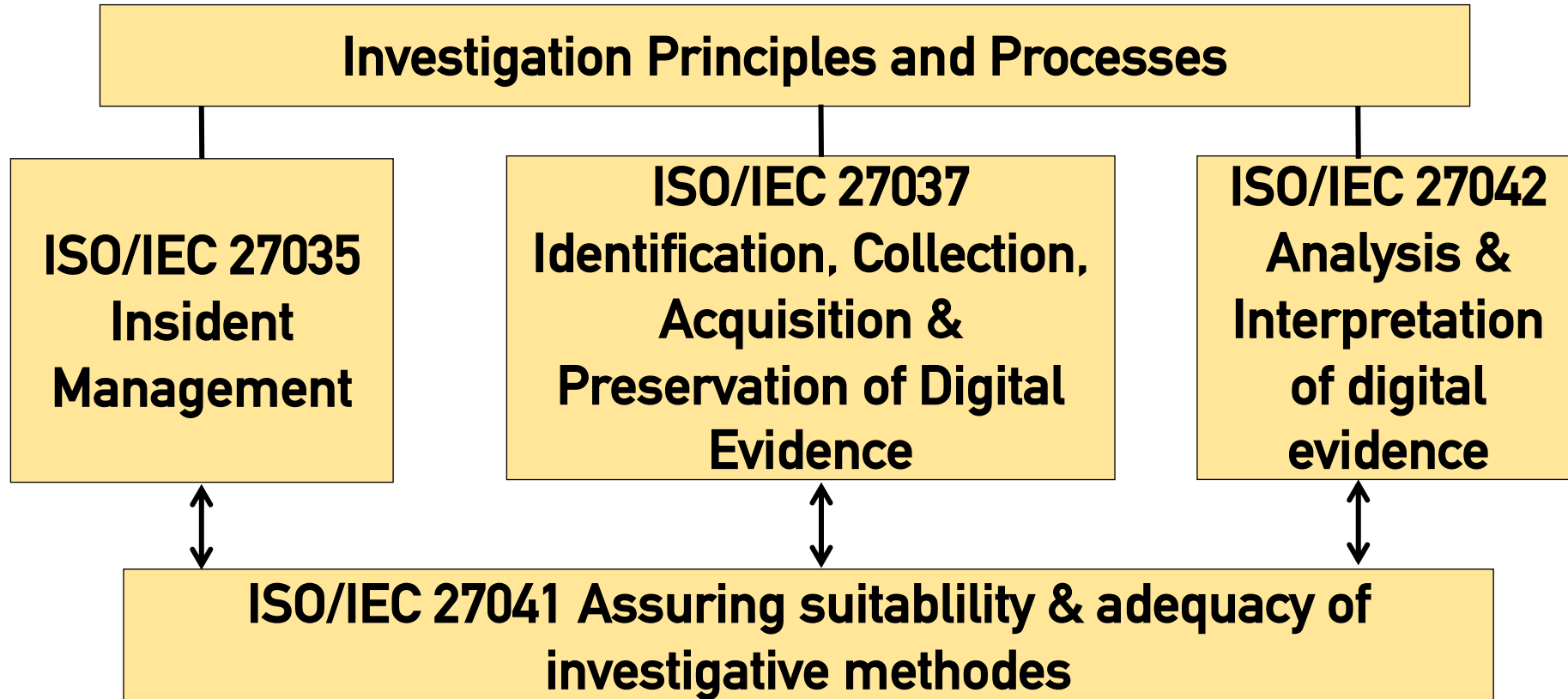
Reviewed and confirmed in 2018

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

*Technologies de l'information — Techniques de sécurité — Lignes
directrices pour l'identification, la collecte, l'acquisition et la préservation
de preuves numériques*

SNI/ ISO IEC 27037

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



- Mencari
- Mengenali
- Mendokumentasikan

Perangkat penyimpan
dan/atau pengolah data

- Membuat prioritas berdasar volatilitas,
- Identifikasi bukti tersembunyi

Menyalin Bukti Digital

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

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



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

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)

Kehandalan
(Reliability)

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

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

PENTINGNYA DEFR?

Home News Pemkot Manado Bisnis Video Lifestyle Seleb Kesehatan
Sulut Manado Bitung Tomohon Minahasa Minut Minsel Mitra Kotamobagu Bolmang
Travel Akomodasi Kuliner Destinasi Shopping Ticketing

Home » News » Nasional

Pengacara Jessica Pertanyakan Video CCTV yang Diputar Ahli Asli Atau Tidak

Rabu, 10 Agustus 2016 16:32



Ahli Digital Forensik Polri, AKBP Muhammad Nuh, menunjukkan rekaman CCTV yang diperbesar saat Jessica Kumala Wongso duduk di kursi paling ujung di meja 54 dalam persidangan di Pengadilan Negeri Jakarta Pusat, Rabu (10/8/2016).

TRIBUNMANADO.CO.ID, JAKARTA - [Otto Hasibuan](#), kuasa hukum Jessica Kumala Wongso, mempertanyakan keaslian video yang diputar dalam sidang kasus kematian [Wayan Mirna](#) Sallihin di Pengadilan Negeri Jakarta Pusat, Rabu (10/8/2016).

"Majelis sudah menetapkan yang diputar (video) di sini asli, tidak boleh yang asli. Sehingga apa yang diputar sungguh-sungguh rekaman yang asli," kata Hasibuan.

Ia juga mempertanyakan kepada jaksa penuntut umum apakah video yang diputar oleh penuntut umum sama yang denean

f
t
g+
p
+

KOMPAS TV

RELEVANSI BUKTI

Home / News / Nasional

Mendagri Putar Video Muktamar HTI di Sidang MK, Yusril Protes

FACHRI FACHRUDIN

Kompas.com - 30/08/2017, 17:09 WIB

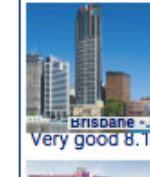


Menteri Dalam Negeri (Mendagri) Tjahjo Kumolo sebagai perwakilan pemerintah menyampaikan keterangan dalam sidang uji materi terhadap Perppu No 2 Tahun 2017 Tentang Perubahan Atas UU No 17 Tahun 2013 tentang Organisasi Kemasyarakatan (Perppu Ormas). Sidang digelar di Mahkamah Konstitusi, Jakarta, Rabu (30/8/2017). (Fachri Fachrudin)

Booking.com



Very good 8.3



very good 8.1

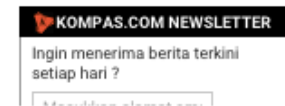
JAKARTA, KOMPAS.com - Kuasa hukum Hizbut Tahrir Indonesia (HTI), Yusnil Ihza Mahendra, mempersoalkan penayangan video muktamar HTI di persidangan uji materi Perppu Ormas di Gedung Mahkamah Konstitusi, Jakarta, Rabu (30/8/2017).

Video tersebut merupakan rekaman Muktamar HTI yang digelar di Gelora Bung Karno, Senayan, Jakarta, pada 2013 silam.

Di dalam video, salah seorang petinggi HTI menyerukan empat pilar Khilafah kepada massa HTI.

Yusnil mempertanyakan tujuan Pemerintah yang diwakili oleh Menteri Dalam Negeri Tjahjo Kumolo, atas penayangan video tersebut.

"Kenapa Saudara sebelum memberikan keterangan, Saudara menayangkan sesuatu? Saudara bermaksud berpropaganda tentang sesuatu yang tidak disenangi Pemerintah atau apa?" kata Yusril.



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