URGENSI STANDARD KOMPETENSI FORENSIK DIGITAL DALAM SKEMA ISO 27037

Izazi Mubarok SST, MSc, CHFI, CEH, ACE, OFCE, CISA, CDSS

outline

- Kebutuhan Standar Kompetensi Forensik Digital di Era Digital
- SKKNI Forensik Digital
- Gambaran Standar Kompetensi Forensik Digital dalam skema ISO 27037
- Tujuan Standar Kompetensi Forensik Digital dalam skema ISO 27037
- Pemetaan RSKKNI Forensik Digital dalam skema ISO 27037 [Usulan]
- Simpulan

1

Kebutuhan Standar Kompetensi Forensik Digital di Era Digital

- Teknologi
- Individu, Bisnis, Pemerintah, Organisasi

- Insiden Keamanan Informasi (Siber)
- Tindak Pidana terkait Teknologi (UU ITE & UU lainnya)
- Internal Fraud

- **Prinsip-prinsip** (ISO 27037 dan ACPO)
- **Sumber Daya**: Personel, Peralatan, Fasilitas, Metodologi (proses)
- Standar (ISO 27037)

- **Syarat Formal dan Materil** (UU ITE)
- Prinsip Bukti Digital (ISO 27037)

Forensik Digital: Prinsip-prinsip

ISO 27037 Principle No 1: Data Integrity.

- "Minimize handling of the original digital device or potential digital evidence."

ISO 27037 Principle No 2: Competency!

- "The DEFR and DES should not take actions beyond their competence."

ISO 27037 Principle No 3: Chain of custody!

- "Account for any chance and document actions taken (to the extent that an expert is able to form an opinion on reliability)."

ISO 27037 Principle No 4: Regulation.

- "Comply with the local rules of evidence."

ACPO Guideline No 1: Don't modify anything! Minimize Evidence Contamination.

- "No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court."

ACPO Guideline 2: Prove your competence! If you have to risk modifying something, make sure you know what you are doing.

- "In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions."

ACPO Guideline 3: Document everything! Record everything you do, in the right order.

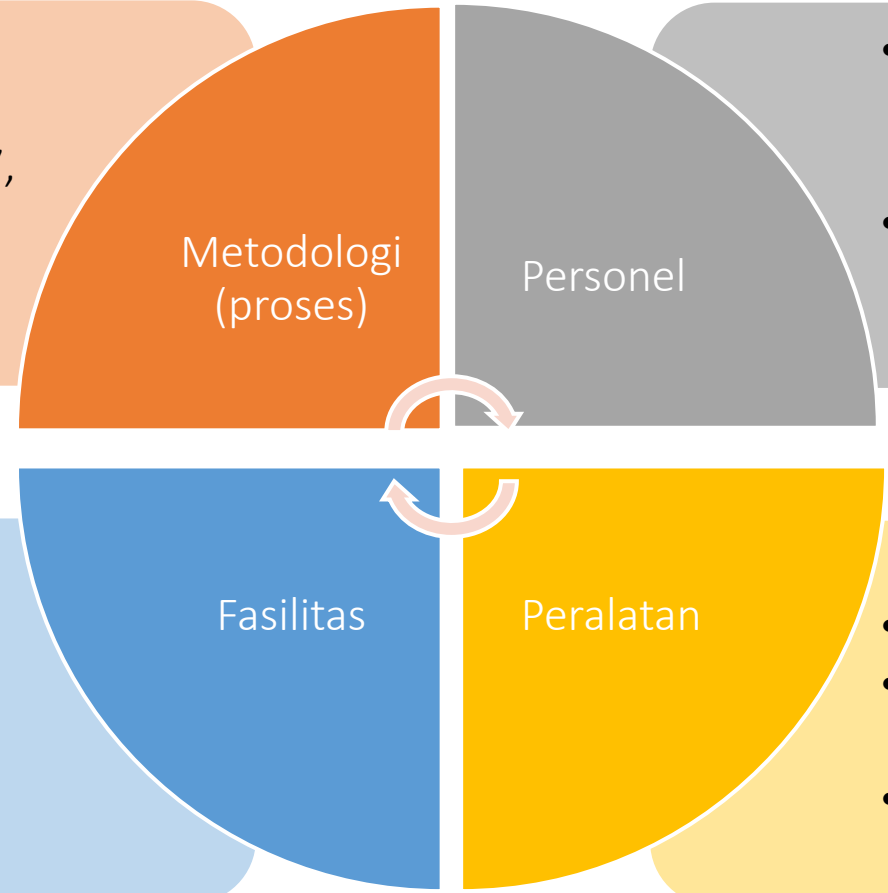
- "An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result."

ACPO Guideline 4: Someone must take responsibility for making sure everything is done both legal and in accordance with these principles.

- "The person in charge of the case (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to."

Forensik Digital: Sumber Daya

- Prosedur dan Teknik
- Best practice/standar: ISO 27037, ACPO, NIJ, NIST, SWGDE



- Pasal 43 ayat 1 (h) UU ITE, punya Keahlian khusus (akademis dan praktis)
- ISO 27037: *core skills* dan kompetensi (awareness, knowledge, dan skill)

- Ruangan Akuisisi
- Ruangan Analisis
- Pengelolaan bukti digital
- Standar Kompetensi Lab: ISO 17025:2017

- Jenis (*software & hardware*)
- Peruntukan (*computer, mobile, cloud, network, etc*)
- Validasi dan pemeliharaan

Bukti Digital: Syarat sah sebagai Alat Bukti menurut UU ITE

"Informasi Elektronik dan/atau Dokumen Elektronik tersebut bukanlah dokumen atau surat yang menurut Undang-undang harus dibuat dalam bentuk tertulis/asli seperti akta notaris/akta PPA."

Dapat diakses

- Bukti digital yang diperoleh dapat diakses oleh sistem elektronik;

Data ditampilkan

- Bukti digital yang diperoleh dapat ditampilkan oleh sistem elektronik;

Dijamin keutuhannya

- Keutuhan bukti digital tersebut harus terjamin.
- Mempertahankan *hash-value* (MD5, SHA1, SHA256) dari bukti digital yang diperoleh.

Dapat dipertanggungjawabkan

- Seluruh prosedur dan kegiatan forensik digital harus dapat dipertanggungjawabkan secara teknis maupun secara legal.
- Menggunakan *best practises* atau standar yang telah ada dan diterapkan dalam organisasi lainnya baik dalam skala lokal maupun global.
- Penerapan prinsip-prinsip dasar seperti *forensics soundness*, dokumentasi, *chain of custody* dan standar kompetensi pemeriksa forensik digital dalam penyusunan kebijakan dan prosedur.

SKKNI Forensik Digital

https://skkni.kemnaker.go.id/tentang-skkni/dokumen

SKKNI

- Rumusan kemampuan kerja yang mencakup aspek **pengetahuan**, **keterampilan**, dan/atau **keahlian** serta **sikap kerja** yang relevan dengan pelaksanaan tugas dan syarat jabatan yang ditetapkan.
- Dikembangkan melalui konsultasi dengan **industri terkait**, untuk memastikan kesesuaian kebutuhan di tempat kerja.
- Digunakan terutama untuk merancang dan mengimplementasikan **pelatihan kerja**, melakukan **asesmen (penilaian)** keluaran pelatihan, serta asesmen tingkat **keterampilan** dan **keahlian** terkini yang dimiliki oleh seseorang.
- Ditetapkan oleh Menteri Ketenagakerjaan.

SKKNI Forensik Digital

- Rumusan kemampuan kerja yang mencakup aspek **pengetahuan**, **keterampilan**, dan/atau **keahlian** serta **sikap kerja** terkait dengan bidang Forensik Digital.

Gambaran Standar Kompetensi Forensik Digital dalam skema ISO 27037

INTERNATIONAL STANDARD

ISO/IEC 27037

First edition
2012-10-15

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

Contents Page

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

1 Scope

This International Standard provides guidelines for specific activities in handling digital evidence, which are identification, collection, acquisition and preservation of digital evidence that may be of evidential value. This International Standard provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

This International Standard gives guidance for the following devices and/or functions that are used in various circumstances:

— Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions,

— Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards,

— Mobile navigation systems,

— Digital still and video cameras (including CCTV),

— Standard computer with network connections,

— Networks based on TCP/IP and other digital protocols, and

— Devices with similar functions as above.

Gambaran Standar Kompetensi Forensik Digital dalam skema ISO 27037 (2)

Konteks untuk koleksi bukti digital	Prinsip bukti digital	Persyaratan untuk penanganan bukti digital	Proses penanganan bukti digital	Komponen Kunci
• Kualitas pembuktian • Ketepatan waktu analisis • Pemulihan layanan • Biaya koleksi bukti digital	• Relevan • Keandalan • Kecukupan	• *Auditability* (dapat diaudit) • Dapat diulang • Dapat diproduksi ulang • Dapat dijustifikasi	• Identifikasi • Koleksi • Akuisisi • Preservasi	• *Chain of custody* • Tindakan pencegahan di lokasi kejadian • Peran dan tanggung jawab • Kompetensi • Pemeliharaan • Dokumentasi • *Briefing* • Memprioritaskan koleksi dan akuisisi • Pemeliharaan bukti digital yang potensial

PERSONEL YANG KOMPETEN

Personel yang kompeten

- Digital Evidence First Responder (DEFR)
  - Individu yang berwenang, terlatih dan berkualifikasi untuk bertindak terlebih dahulu di tempat kejadian perkara melakukan koleksi dan akuisisi bukti digital dengan tanggung jawab menangani bukti tersebut.
  - CATATAN Kewenangan, pelatihan dan kualifikasi adalah persyaratan yang diperlukan untuk menghasilkan bukti digital yang dapat diandalkan, tetapi kondisi masing-masing individu dapat menyebabkan individu tersebut tidak mematuhi ketiga persyaratan. Dalam hal ini, hukum lokal, kebijakan organisasi dan kondisi individu harus dipertimbangkan.
- Digital Evidence Specialist (DES)
  - Individu yang dapat melaksanakan tugas-tugas seorang DEFR dan memiliki pengetahuan, keterampilan dan kemampuan khusus untuk menangani berbagai permasalahan teknis.
  - CATATAN Seorang DES dapat memiliki keterampilan tambahan yang sesuai, seperti, akuisisi jaringan, akuisisi RAM, pengetahuan perangkat lunak, sistem operasi atau Mainframe.

Kemampuan inti (*core skills*) DEFR

Identifikasi bukti digital

- Merinci perangkat digital, komponen, dan informasi yang dapat membantu investigasi dan hukum terkait penanganan bukti digital potensial dan kejahatan yang berhubungan dengan komputer.
- Mengidentifikasi persyaratan alat untuk koleksi, akuisisi data dan perangkat serta penilaian risiko.

Koleksi perangkat digital

- Mengetahui peralatan yang dibutuhkan dalam pembungkusan bukti digital dan implementasinya,
- Mampu melindungi bukti digital dari ancaman lingkungan, serta
- Menjamin keutuhan informasi

Akuisisi bukti digital

- Menerapkan persyaratan akuisisi bukti digital potensial secara logis;
- Memastikan proses dapat diulang, dapat diaudit, dapat diproduksi kembali, dan dapat dipertahankan;
- Lingkup area meliputi akuisisi pada sistem dalam keadaan menyala, akuisisi sistem dalam keadaan mati, dan jaringan.

Preservasi bukti digital

- Menerapkan dan menilai persyaratan untuk preservasi bukti digital potensial, memahami faktor-faktor dan parameter yang mempengaruhi akurasinya;
- Lingkup area meliputi metodologi, pengelolaan rantai pengawasan, penanganan perangkat komputer dan penanganan media penyimpanan digital.

Kompetensi DEFR

Identifikasi bukti digital

Koleksi perangkat digital

Akuisisi bukti digital

Preservasi bukti digital

Mengetahui

- Penggunaan TI secara umum dan pengadministrasian dalam beragam jenis perangkat TI dan perangkat jaringan;
- Prosedur investigasi di tempat kejadian perkara;
- Penentuan kondisi perangkat;
- Nilai dari informasi yang memiliki kekuatan pembuktian;
- Perangkat dan informasi berkaitan dengan forensik jaringan.

Memahami

- Konfigurasi log dan konfigurasi sistem/aplikasi;
- Identifikasi log sistem dan aplikasi meliputi log email, log web, log akses, file kata kunci, file konfigurasi sistem, informasi IP komputer host;
- Fungsionalitas dan keterkaitan perangkat;
- Dampak dari bukti volatil dan nonvolatil.

Menerapkan

- Analisis khusus;
- Penginterpretasian log untuk deteksi intrusi dalam mengidentifikasi sistem lainnya yang terkena dampak;
- Pengidentifikasian kata kunci yang dibutuhkan untuk masing-masing perangkat sebelum koleksi;
- Pengidentifikasian diagram jaringan dan mekanisme kontrol akses untuk memahami keterkaitan;
- Pengidentifikasian keterkaitan antara alamat IP dan alamat MAC untuk konfirmasi perangkat.

Kompetensi DEFR (2)

Identifikasi bukti digital

Koleksi perangkat digital

Akuisisi bukti digital

Preservasi bukti digital

Mengetahui	Memahami	Menerapkan
• Pengumpulan data secara umum dengan mempertimbangkan aspek keselamatan; • Prinsip dan perancangan peralatan dasar; • Penentuan metode terbaik dalam pengumpulan untuk mempreservasi informasi semaksimal mungkin yang berkaitan dengan kejadian perkara.	• Perumusan dan pelaksanaan proses koleksi; • Pengumpulan bukti; • Penulisan dokumen bukti; • Rantai pengawasan bukti (*chain of custody*); • Pengendalian kualitas dari proses koleksi bukti; • Cara wawancara tersangka	• Optimasi proses koleksi; • Pendokumentasian bukti yang tidak dapat diakuisisi karena berbagai kendala; • Pengumpulan kata kunci, dongle, dan informasi lain yang dibutuhkan untuk melakukan analisis di laboratorium

Kompetensi DEFR (3)

Identifikasi bukti digital

Koleksi perangkat digital

Akuisisi bukti digital

Preservasi bukti digital

Mengetahui	Memahami	Menerapkan
• Informasi yang tersedia dalam perangkat digital, database, dokumen yang dihasilkan sistem, data yang dihasilkan pengguna, dan data volatil; • Struktur file sistem UNIX dan Windows serta komponennya; • Dampak dari data volatile.	• Persyaratan media penyimpanan; • Pelaksanaan prosedur akuisisi bit per bit (imaging) (seperti akuisisi media penyimpanan baik keseluruhn dan parsial); • Prosedur akuisisi pada sistem dalam keadaan menyala; • Prosedur akuisisi pada sistem dalam keadaan mati; • Pembuatan nilai hash	• Akuisisi pada media penyimpanan digital meliputi dan tidak terbatas pada RAID, database, perangkat, dan perangkat miniatur; • Pemahaman keterkaitan dan dampak dari metode akuisisi yang berbeda-beda.

Kompetensi DEFR (4)

Identifikasi bukti digital

Koleksi perangkat digital

Akuisisi bukti digital

Preservasi bukti digital

Mengetahui	Memahami	Menerapkan
• Persyaratan dan prosedur pengelolaan *chain of custody* sebagai persyaratan/aspek legal; • Dampak lingkungan seperti kelembapan, temperatur dan guncangan atas perangkat digital; • Persyaratan opsi pembungkusan, transportasi, dan penyimpanan.	• Cara pembuatan dokumen audit bukti; • Penentuan parameter dokumen audit bukti; • Penjaminan keamanan informasi, ancaman, kerentanan dan pengendalian untuk bukti digital.	• Tindakan pengamanan bukti digital, dalam bentuk perangkat besar sampai perangkat miniatur genggam; • Prosedur untuk mendokumentasikan rincian bukti.

Tujuan Standar Kompetensi Forensik Digital dalam skema ISO 27037

- Agar personel mampu mengidentifikasi dan mengelola risiko serta konsekuensi dari tindakan potensial ketika berhadapan dengan bukti digital;
- Agar personel dapat memenuhi prinsip dan kualifikasi bukti digital yang relevan, diandalkan, dan cukup;
- Untuk memastikan bahwa proses dan prosedur yang benar diikuti ketika menangani bukti digital potensial agar preservasi dari bukti digital yang dilakukan memiliki kekuatan pembuktian;
- Untuk memastikan bahwa organisasi dapat menggunakan bukti digital potensial.

Rekomendasi: Pemetaan RSKKNI Forensik Digital skema ISO 27037

Tujuan Utama	Fungsi Kunci	Fungsi Utama	Fungsi Dasar
Melakukan pemeriksaan bukti digital sesuai dengan prinsip-prinsip dasar, standar, dan metodologi forensik digital untuk mendukung investigasi dalam rangka pengungkapan kasus-kasus pidana dan perdata secara ilmiah dan dapat dipertanggungjawakan secara hukum	Membangun sistem manajemen forensik digital		
	Melakukan persiapan dan perencanaan kegiatan forensik digital		
	Melakukan proses perolehan bukti digital	**Melakukan identifikasi bukti fisik dan logik yang relevan**	1) Melakukan persiapan proses pengumpulan bukti digital di lokasi berkoordinasi dengan penyidik (pengamanan lokasi, penunjukan identitas dan surat tugas, identifikasi saksi/PIC, pengumpulan informasi dari saksi/PIC) 2) Melakukan proses identifikasi perangkat digital potensial (fisik) yang relevan dengan kasus 3) Melakukan proses identifikasi bukti logik seperti dokumen dan informasi digital (non fisik) yang relevan dengan kasus
		Melakukan koleksi bukti digital dengan memastikan jaminan keutuhannya	1) Melakukan akuisisi bukti digital di lokasi jika dibutuhkan 2) Melakukan pengumpulan dan pengamanan perangkat digital dengan memastikan jaminan keutuhannya (perolehan secara legal, pelabelan, dokumentasi, pengepakan, pengiriman) 3) Melakukan koleksi bukti digital dengan cara lain sesuai dengan prosedur apabila tidak dapat dilakukan akuisisi atau koleksi secara langsung.
	Melakukan analisa, interpretasi, dan presentasi bukti digital dengan memastikan proses preservasi terpenuhi	**Menerapkan dan menilai persyaratan untuk preservasi bukti digital potensial**	1) Menerapkan preservasi bukti digitak potensial berupa perangkat digital. 2) Menerapkan preservasi barang bukti digital potensial berupa data digital.

Simpulan

- Standar Kompetensi Forensik Digital dalam skema ISO 27037 sangat penting dalam rangka memberikan pedoman penanganan bukti digital, yang meliputi kegiatan identifikasi, koleksi, akuisisi dan preservasi bukti digital agar dapat memiliki kekuatan pembuktian.

Why people should know digital forensics

- Every human action in cyberspace will leave a trace.
- When someone commits a cybercrime, it can be traced through a digital footprint.
- How do we do it? The answer is through digital forensics.
- Imagine when many people know digital forensics, then maybe they will think 1000 times to commit the crime.
- Finally, our life will be more peaceful and beautiful …

izazi@forensor.com
izazi.mubarok@afdi.or.id
+62 852 8647 0009