KAN
Komite Akreditasi Nasional

PERSYARATAN TAMBAHAN AKREDITASI LABORATORIUM DIGITAL FORENSIK

KAN K-01.09

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF
ilac-MRA
APAC
ASIA PACIFIC ACCREDITATION COOPERATION

DAFTAR ISI

Persyaratan Tambahan Akreditasi
Laboratorium Digital Forensik

1. Lingkup

Dokumen ini merupakan persyaratan tambahan akreditasi laboratorium digital forensik sesuai dengan SNI ISO/IEC 17025:2017. Dokumen ini harus dipelajari bersamaan dengan SNI ISO/IEC 17025:2017 Persyaratan Umum Kompetensi Laboratorium Pengujian dan Kalibrasi dan peraturan perundangan yang terkait.

Laboratorium digital forensik dalam hal ini adalah laboratorium yang melakukan pemeriksaan barang bukti elektronik/digital (akuisisi/disk imaging, ekplorasi dan analisis) terhadap barang bukti elektronik/digital (sampel) untuk mendukung kegiatan investigasi. Barang bukti elektronik/digital dapat berupa fisik maupun non fisik yang tidak terbatas pada:

- Media penyimpanan digital yang digunakan dalam komputer standar seperti *hard drive*, *floppy disk*, optik dan *magneto optical disk*, perangkat data dengan fungsi yang serupa;
- Ponsel, *Personal Digital Assistant* (PDA), Perangkat Elektronik Personal, dan kartu memori;
- Sistem navigasi;
- Kamera digital dan kamera video (termasuk CCTV);
- Komputer standar dengan koneksi jaringan;
- Jaringan berdasarkan TCP / IP dan protokol digital lainnya; perangkat audio perekam
- Perangkat dengan fungsi yang serupa seperti di atas.
- Informasi dan/atau Dokumen elektronik, contoh berupa file dokumen berbasis text, spreadsheet/database, dan multimedia (audio, video, dan gambar)
- *Internet of Things device*

Klasifikasi produk dalam lingkup pengujian digital forensik sesuai dengan Lampiran 1 serta penulisan ruang lingkup pada laboratorium digital forensik mengikuti Lampiran 2.

2. Acuan Normatif

a. Undang Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik
b. ISO/IEC 17025:2017 *General requirements for the competence of testing and calibration laboratories*
c. SNI ISO/IEC 27037: 2014 Teknologi Informasi – Teknik keamanan – Pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital
d. ISO/IEC 27043: 2015 *Information technology — Security techniques — Incident investigation principles and processes*
e. KAN Pd-01.05 *Guidelines on Forensic Science Laboratories*

3. Istilah dan Definisi

- Perangkat Elektronik/Digital adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi/dokumen Elektronik.
- Akuisisi adalah proses penyalinan data dalam sebuah rangkaian yang telah ditetapkan.
- Nilai *hash* adalah rangkaian bit yang merupakan keluaran dari fungsi hash.
- *Timestamp* adalah parameter varian waktu yang menunjukkan titik waktu tertentu yang patuh pada referensi waktu yang umum.

4. Persyaratan Umum

Sesuai dengan Persyaratan di ISO/IEC 17025:2017

5. Persyaratan Struktural

Sesuai dengan Persyaratan di ISO/IEC 17025:2017

6. Persyaratan Sumber Daya

6.1 Personel

1. Personel yang berwenang dalam pemeriksaan, pemberian opini dan atau interpretasi termasuk presentasi barang bukti harus memiliki kompetensi pemeriksaan digital forensik.
2. Personel yang melakukan presentasi harus memiliki pengetahuan mengenai sisi

hukum yang terkait dalam kasus yang ditangani.

3. Manajemen laboratorium harus memastikan bahwa semua personel telah menerima pelatihan yang memadai dan kompeten dalam pelaksanaan pemeriksaan dan pengoperasian peralatan, dalam hal ini perangkat keras (*hardware*) dan atau perangkat lunak (*software*) yang digunakan serta terkait presentasi hasil pemeriksaan barang bukti.
4. Personel harus memiliki program pelatihan yang diperlukan dan atau pengalaman dalam sub-disiplin yang sesuai, tidak terbatas pada Pengetahuan dasar dalam hal ilmu forensik dan digital forensik serta pengatahuan tambahan sesuai dengan ruang lingkup pengujian lab digital forensic yang diajukan.
5. Pemeriksa digital forensik memiliki kompetensi yang diakui oleh lembaga nasional melalui antara lain LSP ataupun lembaga internasional, atau melalui surat keputusan atau surat tugas dari instansi masing-masing. Kompetensi yang didapat melalui Pendidikan formal ataupun informal di sampaikan melalui CV yang relevan dari pemeriksa digital forensik.
6. Laboratorium harus memelihara kompetensi personel, dengan melakukan pelatihan, pemutakhiran (*refreshment*), atau *technical briefing* yang membahas mengenai update metode, produk baru, maupun kasus unik, dan pengetahuan bersama termasuk terkait presentasi hasil pemeriksaan barang bukti.

6.2 Fasilitas dan Kondisi Lingkungan

1. Akses ke area operasional organisasi harus dikendalikan dan dibatasi.
   Rekaman catatan dari semua pengunjung ke area operasional organisasi harus dipelihara.
2. Area penyimpanan barang bukti elektronik/digital harus aman untuk mencegah pencurian atau gangguan dan harus ada akses terbatas yang terkendali. Kondisi penyimpanan harus seperti untuk mencegah kehilangan, kerusakan dan kontaminasi dan untuk menjaga integritas dan identitas bukti.
3. Laboratorium harus menjaga lingkungan yang aman atau lokasi barang bukti elektronik/digital (sample) yang dikoleksi atau disimpan.
4. Fasilitas preservasi bukti tidak boleh terpapar dari medan magnet, debu, getaran, kelembaban atau elemen lingkungan lainnya (seperti suhu ekstrim atau kelembapan udara) yang dapat merusak informasi/dokumen elektronik yang potensial sebagai temuan pemeriksaan di dalam fasilitas.
5. Lingkungan uji laboratorium harus memiliki kontrol yang memadai untuk

melindungi perangkat keras dan atau perangkat lunak yang digunakan.

6.3 Peralatan

1. Peralatan yang digunakan untuk pengujian/pemeriksaan harus mencakup perangkat keras dan atau perangkat lunak, termasuk alat uji yang **tidak dikenakan kalibrasi.**
2. Laboratorium harus melakukan penetapan dan penerapan standar keamanan setiap perangkat, dengan melakukan pemutakhiran sistem operasi, *firmware*.
3. Setiap alat (termasuk *software*) memiliki *logbook* (catatan) yang merekam setiap pemutakhiran, perbaikan, pemindahan lokasi, dan lain-lain.
4. Laboratorium harus melakukan verifikasi atau inspeksi kelaikan alat secara berkala dan setelah digunakan di luar fasilitas laboratorium.

6.4 Ketertelusuran Metrologi

Not Applicable

6.5 Produk dan layanan yang disediakan secara eksternal

Sesuai dengan Persyaratan di ISO/IEC 17025:2017

7. Persyaratan Proses

7.1 Kaji ulang tender dan kontrak

Sesuai dengan Persyaratan di ISO/IEC 17025:2017

7.2 Seleksi, verifikasi dan validasi metode

1. Laboratorium harus memastikan bahwa metode pengujian yang digunakan adalah edisi yang mutakhir kecuali metode tersebut tidak sesuai atau tidak mungkin untuk digunakan.
2. Laboratorium harus memverifikasi metode standar untuk menunjukkan bahwa metode tersebut dapat memenuhi kinerja yang diperlukan. Laboratorium harus memvalidasi metode non standar, metode yang dikembangkan dan metode standar yang digunakan diluar lingkup pengujian atau dimodifikasi, metode dari publikasi ilmiah atau dokumen resmi yang dikeluarkan oleh Lembaga tertentu yang relevan dan kompeten.

3. Jika pengembangan metode diperlukan, kegiatan tersebut harus direncanakan dan harus diserahkan kepada personel yang mempunyai kemampuan dibidangnya. Selama pengembangan metode berlangsung, evaluasi harus dilakukan secara periodik untuk memastikan bahwa kebutuhan *customer* masih terpenuhi. Modifikasi terhadap rencana pengembangan harus disetujui dan disahkan.
4. Jika terdapat perubahan pada metode yang divalidasi, pengaruh dari perubahan tersebut harus ditentukan dan jika diketahui mempengaruhi validasi aslinya maka harus dilakukan validasi metode yang baru.
5. Tata cara validasi dilakukan sesuai dengan referensi misalnya dokumen dari SWGDE tentang *Recommended Guidelines for Validation Testing*.

7.3 Pengambilan contoh (sampling)

Kegiatan pengambilan contoh atau sampling pada dasarnya dilakukan ketika mendapatkan dua hal, yaitu area yang luas dan jumlah yang banyak. Dalam hal ini, keterwakilan sampel pada digital forensik adalah *clear* dan *limited*, tidak ada *wide area* dan *big data* sehingga tidak perlu ada pengambilan contoh (sampling).

Namun, untuk kasus-kasus tertentu yang kaitannya dengan data-data yang berasal dari database besar yang perlu keterwakilan data, dapat dilakukan sesuai dengan prosedur yang diacu oleh laboratorium.

7.4 Penanganan item uji

1. Prosedur untuk penerimaan barang bukti harus memastikan bahwa sedapat mungkin, barang-barang yang disimpan dalam fasilitas yang disegel dengan benar.
2. Barang bukti yang tercatat secara elektronik harus dijaga dari proses apapun yang menyebabkan perubahan permanen. Ketika pengolahan dan/atau analisis diperlukan, salinan harus dibuat.
3. Pengoperasian perangkat keras dan sistem perangkat lunak yang menjadi bagian dari barang bukti elektronik/digital (sample) dapat dilakukan jika tidak ada metode alternatif yang dapat digunakan untuk mengakses informasi pada barang bukti tersebut. Dalam hal ini, proses pemeriksaan semacam itu harus dibuatkan prosedur dan rekaman secara jelas serta tetap memperhatikan aspek utama dari integritas informasi yang tersimpan pada barang bukti tersebut.

4. Rekaman rantai proses barang bukti/*chain of custody* (misal; tanda tangan, tanggal, waktu, deskripsi bukti/sampel) harus dipelihara.

7.5 Rekaman Teknis

1. Laboratorium harus mengelola rekaman yang terkait dengan setiap kasus dalam pemeriksaan.
2. Informasi yang dimasukkan dalam rekaman kasus harus didokumentasikan dengan tepat dan dapat mencakup, namun tidak terbatas pada, rekaman komunikasi apapun dengan pelanggan (verbal ataupun tertulis), peninjauan kontrak, pemeriksaan dan pengujian yang diminta dan kesepakatan dengan pelanggan, penerimaan barang bukti, uraian barang bukti termasuk pembungkusan dan segel, surat perintah panggilan sidang, rekaman pengamatan dan hasil-hasil pengujian/pemeriksaan, rujukan ke prosedur yang digunakan, diagram, cetakan (*print-out*), foto, video.
3. Kebijakan retensi rekaman harus mempertimbangkan persyaratan hukum yang berlaku.
4. Rekaman *chain of custody* harus dikelola dari saat penerimaan barang bukti (sampel) hingga pemrosesan ke penyimpanan dan dimana dapat diterapkan hingga saat dikembalikan ke klien yang menyerahkan, atau pembuangan.
5. Rekaman terkait dengan *chain of custody* harus dipertahankan sesuai dengan persyaratan untuk rekaman kasus.

7.6 Evaluasi Ketidakpastian Pengukuran

Not Applicable

7.7 Jaminan Keabsahan Hasil

1. Laboratorium harus memiliki prosedur untuk memantau keabsahan hasil pengujian/pemeriksaan.
2. Jaminan keabsahan hasil harus direncanakan dan dikaji ulang, yang dapat dilakukan dengan:
   a) pengulangan pengujian menggunakan metode yang sama atau berbeda;
   b) uji banding di dalam dan antar laboratorium;
   c) pengujian terhadap “*blind-samples*”

3. Laboratorium harus memantau kinerjanya dengan membandingkan dengan hasil laboratorium lain, jika tersedia dan sesuai, dapat berupa partisipasi dalam uji profisiensi dan/atau dalam perbandingan antar laboratorium selain uji profisiensi.
4. Laboratorium yang melakukan uji banding dengan laboratorium lain harus:
   a) Memiliki prosedur terkait uji banding antar laboratorium
   b) Harus ada specimen (sampel) sesuai dengan ruang lingkup yang diajukan dalam lingkup akreditasi. Specimen yang dimaksud dapat berupa fisik (barang bukti secara fisik seperti, *handphone*, komputer, dll) maupun non fisik (hasil salinan atau hasil *disk imaging*). Barang bukti yang dipertukarkan merupakan barang bukti yang sudah selesai/sudah tutup kasus hukum.
   c) Laboratorium dapat menentukan peralatan yang digunakan secara jelas termasuk jenis *hardware* dan *software* yang dipakai dan versinya.
5. Hasil uji banding diarsipkan sebagai rekaman yang memuat paling sedikitnya informasi mengenai ruang lingkup, specimen, peralatan yang digunakan, hasil dan kesimpulan. Laboratorium dapat memasukkan nilai *hash*, *timestamp* jika diperlukan.

7.8 Pelaporan hasil

1. Jenis dan jumlah informasi yang diperlukan dalam laporan dapat bergantung pada sistem hukum yang berlaku.
2. Laporan yang diterbitkan harus lengkap dan dapat mengandung interpretasi jika diperlukan.
3. Laboratorium harus memiliki prosedur dan kriteria untuk menentukan kapan dan sejauh mana tinjauan teknis dari suatu laporan perlu dilakukan. Tinjauan teknis sebaiknya dilakukan oleh orang yang memenuhi kualifikasi dengan kompetensi yang tepat untuk mengkonfirmasi validitas dari hasil. Kesimpulan harus dibahasakan dengan tepat.

7.9 Keluhan

Sesuai dengan Persyaratan di ISO/IEC 17025:2017

7.10 Pekerjaan yang tidak sesuai

Sesuai dengan Persyaratan di ISO/IEC 17025:2017

7.11 Pengendalian pengelolaan data dan informasi

Sesuai dengan Persyaratan di ISO/IEC 17025:2017

8. Persyaratan Sistem Manajemen

Sesuai dengan Persyaratan di ISO/IEC 17025:2017

LAMPIRAN 1

Tabel 1. Klasifikasi Produk Lingkup Digital Forensik

Kelompok Produk	Sub Kelompok Produk	Representatif Produk
Barang bukti elektronik/digital	Barang bukti elektronik/digital Fisik	Komputer
		Mobile devices (HP dan simcard)
		Media penyimpanan digital (*hard drive*, *floppy disk*, optik dan *magneto optical disk)*
	Barang bukti elektronik/digital Non Fisik	Cloud
		Email
	Multimedia	Audio
		Video
		Images

LAMPIRAN 2

Tabel 2. Penulisan Ruang Lingkup Pada Laboratorium Digital Forensik

Bidang Pengujian	Bahan atau Produk yang diuji	Jenis pengujian atau sifat yang diukur	Metode pengujian atau Teknik yang digunakan
Forensik	Mengikuti tabel 1	Identifikasi, koleksi, akuisisi dan preservasi	Sesuai Metode Laboratorium
Forensik	Mengikuti tabel 1	Akuisisi	Sesuai Metode Laboratorium
Forensik	Mengikuti tabel 1	Analisa	Sesuai Metode Laboratorium