KPK Komisi Pemberantasan Korupsi
Pusat Edukasi Antikorupsi Cipta • Karya • Berdaya
kemitraan partnership
THE PARTNERSHIP FOR GOVERNANCE REFORM
AFDI ASOSIASI FORENSIK DIGITAL INDONESIA

WEBINAR BBE5

MANAJEMEN PENGELOLAAN BUKTI ELEKTRONIK

Komisi Pemberantasan Korupsi
Laboratorium Barang Bukti Elektronik

Apa ada Standar Pengelolaan Bukti Elektronik?

Prinsip-prinsip Penanganan Bukti Elektronik

National Institute of Justice (NIJ) DOJ-USA

Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.

Persons conducting an examination of digital evidence should be trained for that purpose

Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.

Through all of this, the examiner should be cognizant of the need to conduct an accurate and impartial examination of the digital evidence.

Association of Chief Police Officer (UK)

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

Penanganan Bukti Elektronik

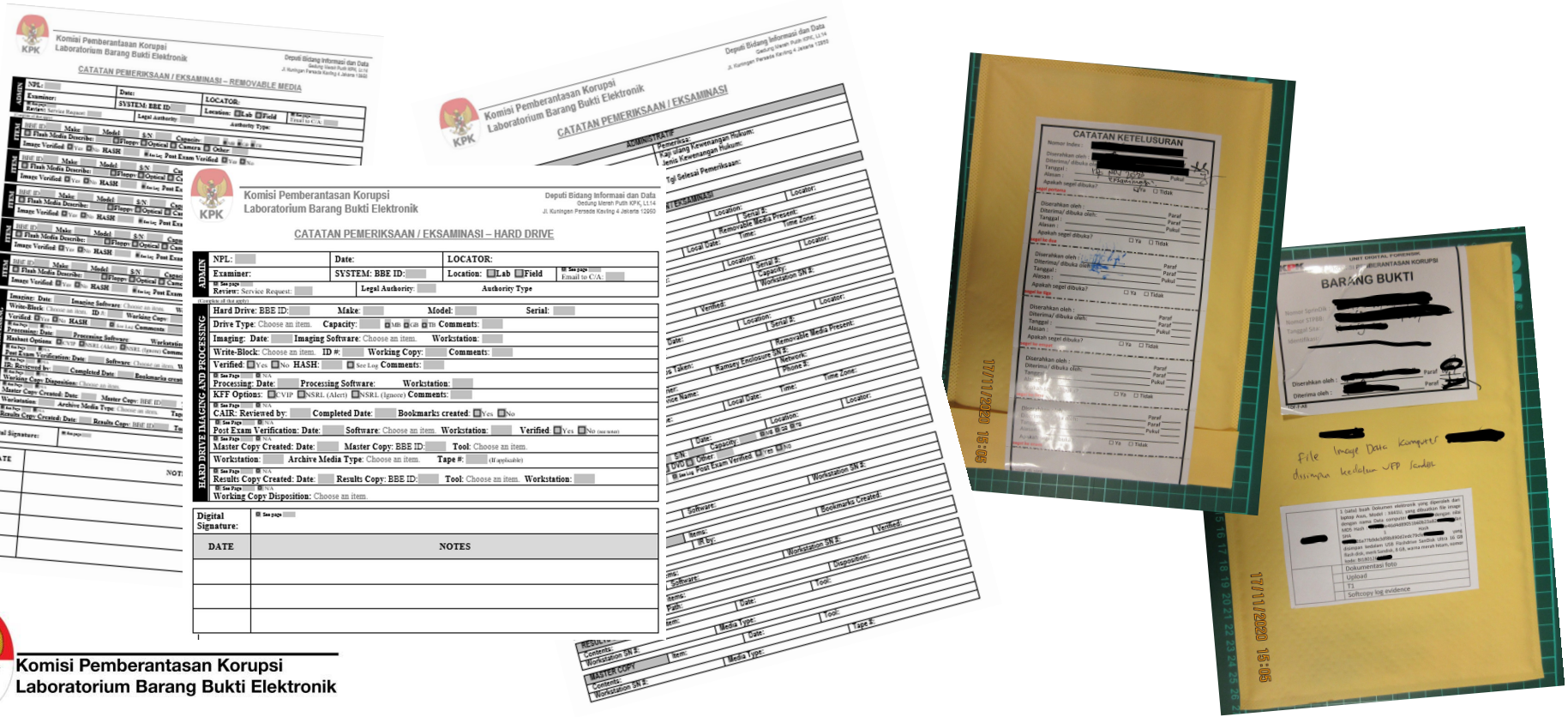
Penanganan Awal (First Responder)	Pemeriksaan/Eksaminasi	Presentasi/Pembuktian	Eksekusi Putusan
Identifikasi, Koleksi, Akuisisi, Preservasi Bukti Elektronik dengan panduan SNI ISO/IEC 27037. Field Search, termasuk kegiatan olah TKP, penggeledahan dan penyitaan	Proses ekstraksi data dan pembuatan salinan/image forensik digital (Master dan Working Copy); Data recovery, Search (hashset filtering), Find, and Extract; Analysis: Timeline, Windows Forensics Analysis, MacOS, Android, iOS, Sqlite Database, Malware, User Attribution, dll	Presentasi/pembuktian sebagai alat bukti petunjuk, keterangan ahli, atau alat bukti surat. Pembuktian yang terkait delik pada pasal sangkaan. Testimoni ahli di persidangan	Penghapusan Data Elektronik untuk Bukti Elektronik yang dirampas Negara/Bukti yang harus dimusnahkan. Re-eksaminasi Bukti Elektronik untuk putusan terlampir dalam berkas perkara/dipergunakan untuk perkara lain

Dasar Kewenangan Hukum (Legal Authority)

01	Proses Bukti Elektronik dengan izin Pengadilan/Dewas	• Surat Perintah Penggeledahan • Surat Perintah Penyitaan • Surat Perintah Pengadilan lainnya
02	Proses Bukti Elektronik tanpa izin Pengadilan/Dewas	• Surat Pernyataan Persetujuan • Surat Penerimaan Resiko Tindakan • Surat Pernyataan lainnya
03	Proses Bukti Elektronik BMN	• Surat Resmi Permohonan kepada Instansi • Berita Acara Pinjam Pakai beserta tanda terimanya
04	Proses Bukti Elektronik Tak Bertuan	• Surat Perintah Tugas • Berita Acara Penemuan Barang • Berita Acara Inspeksi Mendadak (SIDAK)
05	Proses Bukti Elektronik kondisi lainnya	• Surat resmi dengan dasar hukum perundang-undangan yang berlaku.

Dokumentasi dan Catatan Ketelusuran

Dokumentasi dan Catatan Ketelusuran



Kritikal/Formil vs Non Kritikal/Materil

Prosedur

Kritikal/Formil: Jika tidak dilakukan dengan tepat mungkin akan berdampak tidak diterimanya bukti elektronik di pengadilan

- Pemeriksaan Fisik dan SI dan HI
- Sterilisasi Media Penyimpanan
- Sistem Proteksi Akses Tulis
- Penyalinan membuat Image forensik
- Analisa untuk Opini Pendapat Ahli

Peralatan

Kritikal/Formil: Peralatan Forensik Digital yang perlu dilakukan validasi/verifikasi kinerja secara berkala

- Peralatan Sistem Proteksi Akses Tulis
- Drive Duplicator / Imaging
- Forensic Workstation

BBE

Kritikal/Formil: BBE yang dapat dilakukan pembuatan salinan forensik digital dengan nilai hash identik

- Kritikal/Formil: Hard Disk non SSD, USB Flash disk, micro SD, dll
- Non Kritikal/Materil: SSD, RAM, Mobile Device

Best Practices

Forensic Telecommunications Services

Netherlands Forensic Institute
Ministry of Justice and Security

Best Practices

Layanan LBBE:

- Field Search, penanganan awal BBE/layanan luar Laboratorium.
- Layanan KIOSK, proses Search/Find/Extract mandiri.
- Preview in Lab, review bukti elektronik sebelum diajukan untuk dieksaminasi.
- Investigative Review System, proses pencarian, tagging, commenting terhadap dokumen/informasi elektronik hasil eksaminasi sementara.

Program Pelatihan dan Kompetensi Personel (Pelatihan dan Sertifikasi Personel baik dari Internal maupun Eksternal);

Program Validasi Peralatan Forensik Digital (CFTT-NIST)

Best Practices

Hal-hal yang berlaku untuk semua tindakan terhadap bukti elektronik:

- Memastikan adanya dasar kewenangan hukum (legal authority) sebelum melakukan tindakan;
- Menentukan pendekatan teknis/operasional (situasi dan kondisi);
- Menentukan peralatan-peralatan yang sesuai (valid, sah dan legal);
- Menentukan prosedur-prosedur yang digunakan (SOP dan referensi best practices).

Kompetensi Personel

FE	**Pemeriksa Forensik (Forensic Examiner)**	• Certified Forensic Computer Examiner (CFCE) • Certified Computer Examiner (CCE) • Encase Forensic Examiner (EnCE) • Cellebrite Certified Mobile Examiner (CCME)
FT	**Petugas Teknis Forensik (Forensic Technician)**	• Program Pelatihan dan Kompetensi Internal (Digital Forensic Examiner 1) • Cellebrite Certified Physical Analyzer (CCPA) • Cellebrite Certified Operator (CCO)
FR	**Penanganan Awal BBE (First Responder)**	• Program Pelatihan dan Kompetensi Internal (Digital Forensic Examiner 1) • CompTia A+ IT Technician (CompTia A+) • Oxygen Forensic Certification (OFC) • Cellebrite Mobile Forensic Fundamental (CMFF)

Manajemen Laboratorium BBE

Struktur Organisasi LBBE-KPK

- Kepala LBBE-KPK (Manajer Teknis/Koordinator Operasional)
  - Manajer Pelatihan dan Kompetensi Personel LBBE-KPK
    - Spesialis Pelatihan Personel
    - Spesialis Kompetensi Personel
  - Manajer Mutu LBBE-KPK
    - Spesialis Administrator Sistem Mutu
    - Spesialis Engineer Sistem Mutu
  - Manajer Operasional Tim 1
    - Pemeriksa Forensik (*Forensic Examiner*)
    - Tenaga Forensik Digital (*Forensic Technician*)/DES
    - DEFR LBBE-KPK
  - Manajer Operasional Tim 2
    - Pemeriksa Forensik (*Forensic Examiner*)
    - Tenaga Forensik Digital (*Forensic Technician*)/DES
    - DEFR LBBE-KPK
  - Manajer Operasional Tim 3
    - Spesialis BBE/*Evidence Control Technician* (ECT)
    - Spesialis Perbekalan dan Peralatan LBBE
    - Spesialis Administratif Pelayanan LBBE
- DEFR Eksternal LBBE-KPK
- DEFR Eksternal LBBE-KPK
- DEFR Eksternal LBBE-KPK
- DEFR Eksternal LBBE-KPK

ECT: *Evidence Control Technician*, Personel Pengendalian BBE di lingkungan LBBE-KPK
DEFR: *Digital Evidence First Responder* (ISO 27037) personel dgn level kompetensi *First Responder*
DES: *Digital Evidence Specialist* (ISO 27037) personel dgn level kompetensi *Forensic Technician*
DEFR Eksternal LBBE-KPK:
Pegawai KPK diluar LBBE-KPK (Petugas PBB, Penyelidik, Penyidik, JPU, dll) yang sudah mendapatkan pelatihan dan sertifikasi DEFR dari Program Pelatihan dan Kompetensi Personel LBBE-KPK

Personel Validasi Metode & Peralatan:
Manajer Operasional Tim 3

Terima Kasih