PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA
NOMOR TAHUN
TENTANG
TATA CARA PENANGANAN PERTAMA BUKTI ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA,

DRAFT DRAFTDRAFT

Menimbang : a. bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah berdasarkan ketentuan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2019 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

b. bahwa Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum didalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan;

c. bahwa belum ada~~nya~~ pedoman ~~baku~~ terkait penanganan pertama Bukti Elektronik yang menjadi acuan bagi seluruh kementerian atau lembaga dan instansi penegak hukum;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Men`teri Komunikasi dan Informatika tentang Tata Cara Penanganan Pertama Bukti Elektronik;

Mengingat : 1. Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 595);

DRAFT

3. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Nomor 166 Tahun 2008, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);

4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);

5. Peraturan Presiden Republik Indonesia Nomor 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 96);

6. Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2016 tentang Administrasi Penyidikan dan Penindakan Tindak Pidana di Bidang Teknologi Informasi dan Transaksi Elektronik (Berita Negara Republik Indonesia Tahun 2016 Nomor 709);

7. Peraturan Menteri Komunikasi dan Informatika Nomor 12 Tahun 2021 tentang Organisasi dan Tata Kerja

Kementerian Komunikasi dan Informatika (Berita Negara Republik Indonesia Tahun 2021 Nomor 1120);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA TENTANG TATA CARA PENANGANAN PERTAMA BUKTI ELEKTRONIK.

DRAFT

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Bukti Elektronik adalah Sistem Elektronik, Perangkat Elektronik, dan/atau Media Penyimpan Elektronik yang didalamnya terdapat Informasi Elektronik dan/atau Dokumen Elektronik yang dapat diandalkan sebagai alat bukti.
2. Alat Bukti Elektronik adalah Informasi Elektronik dan/atau Dokumen Elektronik yang digunakan sebagai alat bukti dalam peradilan sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2019 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
3. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
4. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik,

optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

5. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
6. Perangkat Elektronik adalah peralatan elektronik yang digunakan untuk memproses dan/atau menyimpan Informasi Elektronik dan/atau Dokumen Elektronik.
7. Media Penyimpanan Elektronik adalah tempat tersimpannya Informasi Elektronik dan/atau Dokumen Elektronik.
8. Identifikasi adalah proses yang meliputi pencarian, pengenalan, dan dokumentasi Bukti Elektronik potensial.
9. Koleksi adalah proses mengumpulkan Sistem Elektronik, Perangkat Elektronik, dan/atau Media Penyimpan Elektronik yang mengandung Bukti Elektronik potensial.
10. Akuisisi Informasi Elektronik dan/atau Dokumen Elektronik yang selanjutnya disebut Akuisisi adalah proses penyalinan Informasi Elektronik dan/atau Dokumen Elektronik dalam sebuah rangkaian yang telah ditetapkan.
11. Preservasi adalah proses mempertahankan dan melindungi integritas dan/atau kondisi asli dari Bukti Elektronik potensial.
12. Penangan Pertama Bukti Elektronik (*Digital Evidence First Responder – DEFR*) yang selanjutnya disebut PPBE adalah pegawai~~/~~ berkompeten atau ahli yang diberi tugas melakukan penanganan pertama terhadap Bukti Elektronik yang meliputi Identifikasi, Koleksi, Akuisisi,

dan Preservasi Bukti Elektronik dengan tanggung jawab menangani bukti tersebut.

13. Spesialis Bukti Elektronik (*Digital Evidence Specialist – DES*) yang selanjutnya disebut SBE adalah pegawai berkompeten atau ahli yang melaksanakan tugas seorang PPBE dan memiliki pengetahuan, keterampilan, dan kemampuan khusus untuk menangani berbagai permasalahan teknis dalam penanganan Bukti Elektronik yang sesuai dengan kebutuhan penanganan perkara.
14. Salinan Bukti Elektronik adalah salinan Informasi dan/atau Dokumen Elektronik terverifikasi yang dihasilkan dari Sistem Elektronik, Perangkat Elektronik, dan/atau Media Penyimpan Elektronik.
15. Nilai *Hash* adalah rangkaian bit yang merupakan keluaran dari fungsi *hash*.
16. Rantai Pengawasan (*Chain of Custody*) adalah dokumen atau serangkaian dokumen terkait yang merincikan aktivitas yang dilakukan terhadap Bukti Elektronik, mulai dari tahap Identifikasi, Koleksi, Akuisisi, analisis dan laporan dalam rangka mengidentifikasi akses sampai dengan pergerakan Bukti Elektronik pada waktu tertentu.
17. Penyalinan per-bit (*Imaging*) adalah proses pembuatan salinan pada level bit (identik) dari Sistem Elektronik, Perangkat Elektronik, dan/atau Media Penyimpan Elektronik.

Pasal 2

Penanganan terhadap Bukti Elektronik dilakukan dengan memperhatikan integritas atau keutuhan data, perlindungan terhadap privasi, kerahasiaan, dan kelancaran layanan publik, sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 3

Ruang lingkup Peraturan Menteri ini meliputi:

a. prinsip dasar Bukti Elektronik;
b. tahapan penanganan pertama Bukti Elektronik;

c. penjelasan personel yang terlibat dalam penanganan Bukti Elektronik;
d. Rantai Pengawasan (*Chain of Custody*) Bukti Elektronik;
e. penjaminan kerahasian data; dan
f. ketentuan minimum alat dan perangkat yang disiapkan.

BAB II
PRINSIP DASAR BUKTI ELEKTRONIK

Pasal 4

(1) Penanganan pertama terhadap Bukti Elektronik harus memenuhi 3 (tiga) prinsip dasar:
    a. relevansi;
    b. keandalan; dan
    c. kecukupan.
(2) Relevansi sebagaimana dimaksud pada ayat (1) huruf a menunjukkan adanya hubungan langsung antara Bukti Elektronik dan perkara yang sedang ditangani.
(3) Keandalan sebagaimana dimaksud pada ayat (1) huruf b menunjukkan bahwa Bukti Elektronik memberikan hasil yang sama melalui pemeriksaan yang berulang dan/atau metode yang berbeda.
(4) Kecukupan sebagaimana dimaksud pada ayat (1) huruf c menunjukkan bahwa Bukti Elektronik yang dikumpulkan memenuhi kebutuhan dan tujuan dari pengumpulan Bukti Elektronik.

BAB III
TAHAPAN PENANGANAN PERTAMA BUKTI ELEKTRONIK

Pasal 5

(1) Tahapan penanganan pertama Bukti Elektronik yakni:
    a. Identifikasi;
    b. Koleksi;
    c. Akuisisi; dan
    d. Preservasi.

(2) Proses Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan dengan tujuan:
   a. mengenali Sistem Elektronik, Perangkat Elektronik, dan Media Penyimpanan Elektronik yang berisi Informasi Elektronik dan/atau Dokumen Elektronik potensial yang relevan dengan perkara;
   b. membuat daftar prioritas Bukti Elektronik potensial yang relevan dengan perkara untuk dikoleksi terlebih dahulu; dan
   c. mengidentifikasi kemungkinan adanya Bukti Elektronik potensial yang tersembunyi.

(3) Proses Koleksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan ketentuan sebagai berikut:
   a. bukti yang dikoleksi merupakan bukti yang berdasarkan hasil penilaian Identifikasi sebagaimana dimaksud pada ayat (2) diduga berhubungan langsung dengan perkara;
   b. pelaksanaan Koleksi Bukti Elektronik tidak mengganggu kepentingan publik; dan
   c. melakukan penilaian terhadap faktor yang relevan dengan perkara yang sedang ditangani berdasarkan panduan sebagaimana tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(4) Proses Akuisisi terhadap Bukti Elektronik harus dilakukan dengan ketentuan sebagai berikut:
   a. menggunakan metode yang dapat menghasilkan Salinan Bukti Elektronik (Penyalinan per-bit (*Imaging*)) yang dapat diverifikasi keakuratannya (verifikasi Nilai *Hash*); dan
   b. menggunakan cara yang paling aman untuk menghindari perubahan Informasi Elektronik dan/atau Dokumen Elektronik sepanjang memungkinkan.

(5) Proses Preservasi terhadap Bukti Elektronik harus dilakukan dengan ketentuan sebagai berikut:

a. memberikan pengamanan yang memadai untuk melindungi integritas dan keaslian Bukti Elektronik potensial serta Rantai Pengawasan (*Chain of Custody*); dan

b. dilakukan sejak proses Identifikasi.

(6) Pelaksanaan proses Identifikasi, Koleksi, Akuisisi, dan Preservasi harus didokumentasikan secara akurat dan memadai.

(7) Dalam hal pelaksanaan Akuisisi dan Preservasi mengakibatkan adanya perubahan yang tidak mungkin dihindari terhadap Bukti Elektronik, Dokumentasi sebagaimana dimaksud pada ayat (6) harus memuat penjelasan mengenai~~:~~

a. pemilihan cara dan metode yang diperlukan yang mengakibatkan perubahan tersebut; dan

~~b.~~ perubahan yang terjadi akibat pemilihan cara dan metode sebagaimana dimaksud pada huruf a.

Pasal 6

(1) Panduan pelaksanaan proses Identifikasi, Koleksi, Akuisisi, dan Preservasi Bukti Elektronik tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(2) Dalam hal penanganan pertama Bukti Elektronik tidak memenenuhi ketentuan sebagaimana dimaksud dalam Peraturan Menteri ini, maka Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetak dari Bukti Elektronik tersebut tidak dapat dijadikan alat bukti yang sah.

BAB IV

PERSONEL

Pasal 7

Personel yang melakukan penanganan pertama Bukti Elektronik sebagaimana dimaksud dalam Peraturan Menteri ini meliputi PPBE dan SBE.

Pasal 8

(1) PPBE sebagaimana dimaksud dalam Pasal 7 harus memenuhi kualifikasi:
    a. memiliki latar belakang pendidikan paling rendah diploma 3 (tiga) atau yang disetarakan;
    b. telah lulus sertifikasi terkait Identifikasi, Koleksi, Akuisisi, dan Preservasi Bukti Elektronik yang diterbitkan oleh lembaga sertifikasi sesuai dengan tugas penanganan Bukti Elektronik yang sedang ditangani; dan
    c. memiliki pengalaman paling sedikit 1 (satu) tahun terlibat dalam penanganan~~:~~ Identifikasi, Koleksi, Akuisisi, dan Preservasi Bukti Elektronik.
(2) Dalam hal belum tersedianya lembaga sertifikasi yang membidangi Identifikasi, Koleksi, Akuisisi, dan Preservasi Bukti Elektronik sesuai dengan Bukti Elektronik yang sedang ditangani maka PPBE harus paling rendah telah menyelesaikan pelatihan terkait dengan Identifikasi, Koleksi, Akuisisi, dan Preservasi Bukti Elektronik yang diselenggarakan oleh institusi pendidikan, pemerintah, atau asosiasi profesi sesuai dengan tugas penanganan Bukti Elektronik yang sedang ditangani.

Pasal 9

SBE sebagaimana dimaksud dalam Pasal 7 harus memenuhi kualifikasi:

a. sudah menjadi PPBE paling sedikit 3 (tiga) tahun;
b. memiliki pengalaman paling sedikit 3 (tiga) tahun terlibat dalam melakukan analisis Bukti Elektronik; dan
c. memiliki latar belakang pendidikan paling rendah strata 1 (satu) atau yang disetarakan.

Pasal 10

(1) Pelaksanaan Identifikasi, Akuisisi, Koleksi, dan/atau Preservasi, harus didasarkan pada surat perintah resmi

bagi personel dari pejabat yang berwenang dan didasarkan pada:

a. persetujuan dari pemilik atau pihak yang menguasai Sistem Elektronik; atau
b. surat izin atau penetapan dari pengadilan.

(2) Dalam hal pelaksanaan Identifikasi, Akuisisi, Koleksi, dan/atau Preservasi untuk kepentingan penegakan hukum pidana dalam keadaan yang sangat perlu dan mendesak dilaksanakan sesuai dengan ketentuan dalam hukum acara pidana.

BAB V
RANTAI PENGAWASAN (*CHAIN OF CUSTODY*)

Pasal 11

(1) Dalam rangka menjaga integritas data, setiap penanganan pertama Bukti Elektronik harus dilengkapi dengan Rantai Pengawasan (*Chain of Custody*).

(2) Rantai Pengawasan (*Chain of Custody*) paling sedikit memuat:

a. identitas bukti;
b. aktivitas yang dilakukan terhadap bukti;
c. waktu pelaksanaan aktivitas dan orang yang melakukan aktivitas;
d. alasan pemeriksaan;
e. perubahan yang terjadi (jika ada); dan
f. tanda tangan.

(3) PPBE dan SBE wajib membuat Rantai Pengawasan (*Chain of Custody*) pada tahap Identifikasi, Akuisi, dan Koleksi.

(4) Dalam hal PPBE dan/atau SBE menyerahkan Bukti Elektronik kepada pihak lain maka:

a. PPBE atau SBE menyerahkan Rantai Pengawasan (*Chain of Custody*) yang telah dibuatnya kepada pihak lain tersebut sebagai penerima;
b. penerima wajib memperbarui Rantai Pengawasan (*Chain of Custody*); dan/atau

c. pada perkara pidana, Penyidik yang melimpahkan Bukti Elektronik kepada penuntut umum harus menyerahkan Rantai Pengawasan (*Chain of Custody*) yang dibuat oleh PPBE, SBE, dan Penyidik.

BAB VI
PENJAMINAN KERAHASIAAN DATA

Pasal 12

(1) Bukti Elektronik yang sedang dilakukan proses Identifikasi, Akuisisi, Koleksi, dan analisis untuk penanganan suatu perkara tertentu tidak boleh digunakan untuk penanganan perkara lain.
(2) PPBE dan SBE wajib memiliki prosedur untuk memfilter pencarian Bukti Elektronik yang relevan dengan penanganan perkara yang sedang dilakukan.
(3) PPBE dan SBE wajib mencatat pelaksanaan prosedur dan menjamin kerahasiaan data.

BAB VII
KETENTUAN MINIMUM ALAT DAN PERANGKAT YANG DISIAPKAN

Pasal 13

(1) Alat dan perangkat yang digunakan untuk melakukan Akuisisi dan analisis merupakan alat dan perangkat yang diakui atau diterima oleh:
    a. instansi atau lembaga resmi yang membidangi standardisasi alat dan perangkat forensik digital; atau
    b. komunitas dan/atau asosiasi nasional, regional, dan internasional di bidang teknologi informasi dan/atau forensik digital.
(2) Daftar minimal alat dan perangkat yang digunakan dalam proses Identifikasi, Akuisisi, Koleksi, dan Preservasi tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

BAB VIII

KETENTUAN PERALIHAN

Pasal 14

Pada saat Peraturan Menteri ini mulai berlaku, kementerian atau lembaga dan instansi penegak hukum yang telah menyelenggarakan penanganan pertama Bukti Elektronik sebelum diundangkannya Peraturan Menteri ini, wajib menyesuaikan dengan Peraturan Menteri ini paling lambat 1 (satu) tahun sejak Peraturan Menteri ini diundangkan.

BAB IX

KETENTUAN PENUTUP

Pasal 15

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA,

DRAFTDRAFTDRAFT

JOHNNY G. PLATE

Diundangkan di Jakarta
pada tanggal

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

DRAFTDRAFTDRAFT

BENNY RIYANTO

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2021 NOMOR

LAMPIRAN I
PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA
NOMOR TAHUN 2021
TENTANG
TATA CARA PENANGANAN PERTAMA BUKTI ELEKTRONIK

PANDUAN UNTUK
IDENTIFIKASI, KOLEKSI, AKUISISI, DAN PRESERVASI BUKTI ELEKTRONIK

1 Ruang Lingkup

Peraturan Menteri ini memberikan pedoman untuk kegiatan yang spesifik dalam menangani Bukti Elektronik atau disebut juga bukti digital, yaitu Identifikasi, Koleksi, Akuisisi, dan Preservasi Bukti Elektronik yang dapat memiliki nilai kekuatan pembuktian. Panduan ini memberikan panduan kepada individu dalam menghadapi situasi umum sepanjang proses penanganan Bukti Elektronik dan membantu organisasi dalam prosedur penegakan disiplinnya serta dalam memudahkan pertukaran Bukti Elektronik potensial antar jurisdiksi.

Peraturan Menteri ini memberikan panduan untuk perangkat dan/atau fungsi berikut yang digunakan dalam berbagai keadaan:

a. media penyimpanan digital yang digunakan dalam komputer standar seperti perangkat keras, *floppy disk*, optik, dan *magneto optical disk*, serta perangkat data dengan fungsi yang serupa;
b. ponsel, *personal digital assistant* (PDA), perangkat elektronik personal, dan kartu memori;
c. sistem navigasi;
d. kamera digital dan kamera video (termasuk *closed circuit television* (CCTV));
e. komputer standar dengan koneksi jaringan;
f. jaringan berdasarkan *transmission control protocol* (TCP)/*internet protocol* (IP) dan protokol digital lainnya; dan

g. perangkat dengan fungsi yang serupa seperti perangkat dan/atau fungsi sebagaimana dimaksud dalam huruf a sampai dengan huruf f.

Catatan:

a. Daftar perangkat di atas adalah daftar indikatif dan tidak menyeluruh.
b. Keadaan yang dimaksud meliputi perangkat yang disebutkan di atas dalam berbagai bentuk. Sebagai contoh, sistem otomotif dapat mencakup sistem navigasi ~~mobile~~, penyimpanan data, dan sistem sensor.

2 Acuan Normatif

Panduan ini mengacu kepada ISO SNI/IEC 27037:2012 *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.*

3 Definisi

Definisi berikut ini sebagaimana dimaksud dalam Pasal 1 dan definisi tambahan yang dipergunakan dalam Lampiran I Panduan untuk Identifikasi, Koleksi, Akuisisi, dan Preservasi Bukti Elektronik~~.~~:

3.1 Akuisisi Informasi Elektronik dan/atau Dokumen Elektronik yang selanjutnya disebut Akuisisi adalah proses penyalinan Informasi Elektronik dan/atau Dokumen Elektronik (data) dalam sebuah rangkaian yang telah ditetapkan.

Catatan: produk dari Akuisisi adalah salinan Bukti Elektronik potensial.

3.2 *Allocated Space* adalah area pada media digital, meliputi memori utama, yang digunakan untuk penyimpanan data, termasuk metadata.

3.3 Koleksi adalah proses mengumpulkan Sistem Elektronik, Perangkat Elektronik, dan/atau Media Penyimpan Elektronik yang mengandung Bukti Elektronik potensial.

Catatan: merupakan proses koleksi benda-benda fisik yang mengandung Bukti Elektronik potensial.

3.4 Perangkat Digital adalah peralatan elektronik yang digunakan untuk memproses atau menyimpan data digital.

3.5 Bukti Elektronik adalah Sistem Elektronik, Perangkat Elektronik, dan/atau Media Penyimpan Elektronik yang didalamnya terdapat Informasi Elektronik dan/atau Dokumen Elektronik yang dapat diandalkan sebagai alat bukti.

Catatan: merupakan informasi atau data~~,~~ yang disimpan dan/atau ditransmisikan dalam bentuk biner yang dapat diandalkan sebagai bukti.

3.6 Salinan Bukti Elektronik adalah salinan Informasi dan/atau Dokumen Elektronik terverifikasi yang dihasilkan dari Sistem Elektronik, Perangkat Elektronik, dan/atau Media Penyimpan Elektronik.

Catatan: salinan Bukti Elektronik yang telah dihasilkan untuk menjaga keandalan dari bukti dengan memasukkan Bukti Elektronik dan upaya verifikasi yang di mana metode verifikasi dapat berupa yang ditanam dalam atau independen dari alat yang digunakan dalam melakukan verifikasi tersebut.

3.7 Penangan Pertama Bukti Elektronik (*Digital Evidence First Responder – DEFR*) yang selanjutnya disebut PPBE adalah pegawai berkompeten atau ahli yang bertanggung jawab menangani Bukti Elektronik dengan tugas melakukan penanganan pertama terhadap Bukti Elektronik yang meliputi Identifikasi, Koleksi, Akuisisi, dan Preservasi Bukti Elektronik.

Catatan:

a. PPBE merupakan individu yang berwenang, terlatih, dan berkualifikasi untuk bertindak terlebih dahulu di tempat kejadian perkara untuk melakukan Koleksi dan Akuisisi Bukti Elektronik dengan tanggung jawab menangani bukti tersebut.

b. Kewenangan, pelatihan, dan kualifikasi adalah persyaratan yang diperlukan untuk menghasilkan Bukti Elektronik 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.

3.8 Spesialis Bukti Elektronik (*Digital Evidence Specialist* – DES) yang selanjutnya disebut SBE adalah pegawai berkompeten atau ahli yang melaksanakan tugas seorang PPBE dan memiliki pengetahuan, keterampilan, dan kemampuan khusus untuk menangani berbagai permasalahan teknis dalam penanganan Bukti Elektronik yang sesuai dengan kebutuhan penanganan perkara.

Catatan:

a. SBE merupakan individu yang dapat melaksanakan tugas PPBE dan memiliki pengetahuan, keterampilan, dan kemampuan khusus untuk menangani berbagai permasalahan teknis.

b. SBE dapat memiliki keterampilan khusus tambahan seperti Akuisisi jaringan, Akuisisi RAM, dan pengetahuan mengenai perangkat lunak sistem operasi atau *Mmainframe*.

3.9 Media Penyimpanan Digital merupakan perangkat perekam data digital. Media Penyimpanan Digital ini mempunyai kesamaan arti dan fungsi dengan Media Penyimpanan Elektronik.

[Diadaptasi dari ISO / IEC 10027: 1990]

3.10 Preservasi adalah proses mempertahankan dan melindungi integritas dan/atau kondisi asli dari Bukti Elektronik potensial.

3.11 Fasilitas Preservasi bukti adalah lingkungan yang aman atau lokasi penyimpanan bukti yang dikoleksi atau yang diakuisisi.

Catatan:

Fasilitas Preservasi bukti tidak boleh terpapar dari medan magnet, debu, getaran, kelembapan, atau elemen lingkungan lainnya (seperti suhu ekstrem atau kelembapan udara) yang dapat merusak Bukti Elektronik potensial di dalam fasilitas.

3.12 Nilai *Hash* adalah rangkaian bit yang merupakan keluaran dari fungsi *hash.*

[ISO/IEC 10118-1: 2000]

3.13 Identifikasi adalah proses yang meliputi pencarian, pengenalan, dan dokumentasi Bukti Elektronik potensial.

3.14 Penyalinan per-Bit (*Imaging*) adalah proses pembuatan salinan pada level bit (identik) dari Sistem Elektronik, Perangkat Elektronik, dan/atau Media Penyimpan Elektronik/Media Penyimpanan Digital.

Catatan:

a. Salinan level bit (identik) disebut juga sebagai salinan fisik.

b. Contoh: Ketika menyalin utuh perangkat keras, PPBE juga akan menyalin data yang telah dihapus.

3.15 Periferal adalah perangkat yang melekat pada perangkat digital untuk memperluas fungsionalitasnya.

3.16 Reabilitas (Keandalan) adalah sifat konsisten dari perilaku dan hasil yang diharapkan.

3.17 Dapat Diulang adalah sifat dari sebuah proses yang dilakukan untuk mendapatkan hasil pengujian yang sama pada lingkungan pengujian yang sama (komputer, perangkat keras, modus operasi yang sama, dan lain-lain).

3.18 Dapat Diproduksi Ulang adalah sifat sebuah proses untuk mendapatkan hasil pengujian yang sama pada lingkungan pengujian yang berbeda (komputer, perangkat keras, operator yang berbeda, dan lain-lain).

3.19 Perusakan (*Spoliation*) adalah tindakan membuat atau membiarkan terjadinya perubahan pada Bukti Elektronik potensial yang mengurangi nilai kekuatan pembuktian.

3.20 Pengubahan (*Tampering*) adalah tindakan membuat atau membiarkan terjadinya perubahan yang disengaja pada Bukti Elektronik (antara lain Perusakan (*Spoliation*) yang disengaja atau dengan tujuan tertentu).

3.21 Waktu Sistem adalah waktu yang dihasilkan oleh jam sistem dan digunakan oleh sistem operasi, bukan waktu yang dihitung oleh sistem operasi.

3.22 Penanda Waktu adalah parameter varian waktu yang menunjukkan titik waktu tertentu yang patuh pada referensi waktu yang umum. [ISO/IEC 11770-1:1996].

3.23 Unallocated *Space* adalah area pada media digital, meliputi memori utama, yang belum dialokasikan oleh sistem operasi, dan yang tersedia untuk penyimpanan data, termasuk metadata.

3.24 Validasi adalah konfirmasi, melalui tersedianya pembuktian yang objektif, yaitu bahwa persyaratan untuk penggunaan yang disengaja atau aplikasi yang spesifik telah dipenuhi.

[ISO / IEC 27004: 2009]

3.25 Fungsi Verifikasi adalah fungsi yang digunakan untuk memverifikasi bahwa 2 (dua) set data adalah identik.

Catatan:

a. Tidak ada 2 (dua) set data yang tidak identik dapat menghasilkan kecocokan yang identik dari fungsi verifikasi.

b. Fungsi Verifikasi biasa diimplementasikan menggunakan fungsi *hash* seperti MD5, SHA1, dan lain-lain, tapi metode lain dapat digunakan.

3.26 Data Volatil adalah data yang rentan terhadap perubahan dan dapat dengan mudah dimodifikasi.

Catatan:

Perubahan dapat berupa mematikan sumber daya atau melewati sebuah medan magnet. Data Volatil juga termasuk data yang berubah seiring dengan perubahan kondisi sistem. Contohnya termasuk data yang tersimpan dalam RAM dan alamat IP dinamis.

4 Daftar Singkatan

AVI	*Audio Video Interleave*
CCTV	*Closed Circuit Television*
CD	*Compact Disk*
DNA	*Deoxyribonucleic Acid*
DVD	*Digital Video/ Versatile Disk*
ESN	*Electronic Serial Number*
GPS	*Global Positioning System*
GSM	*Global System for Mobile Communication*
IMEI	*International Mobile Equipment Identity*
IP	*Internet Protocol*
ISIRT	*Information Security Incident Response Team*
LAN	*Local Area Network*

MD5	*Message-Digest Algorithm* 5
MP3	*MPEG Audio Layer* 3
MPEG	*Moving Picture Experts Group*
NAS	*Network Attached Storage*
PDA	*Personal Digital Assistant*
PED	*Personal Electronic Device*
PIN	*Personal Identification Number*
PUK	*PIN Unlock Key*
RAID	*Redundant Array of Independent Disks*
RAM	*Random Access Memory*
RFID	*Radio Frequency Identification*
SAN	*Storage Area Network*
SHA	*Secure Hash Algorithm*
SIM	*Subscriber Identity Module*
USB	*Universal Serial Bus*
UPS	*Uninterruptible Power Supply*
USIM	*Universal Subscriber Identity Module*
UV	*Ultraviolet*
Wi-Fi	*Wireless Fidelity*

5 Ikhtisar

5.1 Konteks Untuk Koleksi Bukti Elektronik

Bukti Elektronik dapat diperlukan untuk digunakan dalam beberapa skenario yang berbeda, masing-masing memiliki porsi pertimbangan yang berbeda antara kualitas pembuktian, ketepatan waktu analisis, pemulihan layanan dan biaya Koleksi Bukti Elektronik. Oleh karena itu, organisasi diharuskan memiliki proses penentuan prioritas yang mengidentifikasi kebutuhan dan porsi pertimbangan kualitas pembuktian, ketepatan waktu, dan pemulihan layanan sebelum menugaskan sumber daya PPBE. Proses penentuan prioritas meliputi pelaksanaan evaluasi terhadap benda yang tersedia untuk menentukan kekuatan pembuktian yang mungkin dimiliki dan urutan Bukti Elektronik potensial yang harus dikoleksi, diakuisisi, atau dipreservasi. Penentuan prioritas dilakukan untuk meminimalkan risiko Bukti Elektronik potensial dirusak dan memaksimalkan nilai pembuktian dari Bukti Elektronik yang dikoleksi.

5.2 Prinsip Bukti Elektronik

Bukti Elektronik diatur oleh tiga prinsip dasar: relevansi, keandalan, dan kecukupan. Ketiga prinsip ini penting bagi semua investigasi, bukan hanya agar Bukti Elektronik dapat diterima di pengadilan. Bukti Elektronik dinyatakan relevan ketika dapat digunakan untuk membuktikan suatu keterkaitan dari kasus tertentu yang sedang diinvestigasi. Investigasi yang dimaksud yakni meliputi penyelidikan, penelitian, dan penyidikan. Pemahaman umum yang sudah dikenal luas dari prinsip keandalan adalah "untuk memastikan Bukti Elektronik yang dimaksud adalah memang Bukti Elektronik tersebut". Tidak selalu menjadi keharusan bagi PPBE untuk mengoleksi semua data atau untuk membuat salinan utuh dari Bukti Elektronik yang asli. Kecukupan berarti bahwa PPBE perlu mengoleksi Bukti Elektronik potensial yang cukup untuk memungkinkan unsur-unsur perkara diperiksa atau diselidiki secara memadai. Memahami konsep ini penting bagi PPBE untuk memprioritaskan upaya yang tepat ketika waktu atau biaya menjadi pertimbangan. Selain itu, PPBE harus memastikan bahwa Koleksi Bukti Elektronik potensial sesuai dengan hukum dan peraturan perundang-undangan, seperti yang dipersyaratkan dalam keadaan tertentu.

Semua proses yang akan digunakan oleh PPBE dan SBE harus telah divalidasi sebelum penggunaan. Jika validasi dilakukan secara eksternal, PPBE atau DES harus memverifikasi bahwa validasi telah sesuai untuk penggunaan khusus mereka terhadap proses dan lingkungan dan keadaan di mana proses tersebut akan digunakan. PPBE atau SBE juga harus:

a. mendokumentasikan semua tindakan;
b. menentukan dan menerapkan sebuah metode untuk memperlihatkan keakuratan dan keandalan dari salinan Bukti Elektronik potensial dibandingkan dengan sumber aslinya; dan
c. memahami bahwa tindakan Preservasi Bukti Elektronik potensial tidak selalu bisa berada dalam kondisi yang kondusif.

5.3 Persyaratan Untuk Penanganan Bukti Elektronik

5.3.1 Umum

Terdapat 4 (empat) aspek utama dalam penanganan Bukti Elektronik÷ yakni dapat diaudit, dapat di-justifikasi, baik dapat diulang ataupun diproduksi ulang bergantung pada keadaan tertentu. Pengumpulan Bukti Elektronik dalam dilakukan melalui Tindakan Akuisisi dan/atau Koleksi.

Contoh penerapan prinsip sebagaimana dimaksud dalam klausul 5.2 yakni :

a) Relevansi: Harus dapat ditunjukkan bahwa Bukti Elektronik yang diperoleh relevan dengan investigasi yaitu yang mengandung informasi berguna dalam membantu investigasi atas insiden tertentu dan ada alasan yang kuat sehingga Bukti Elektronik tersebut diperoleh. Melalui audit dan justifikasi, PPBE harus dapat mendeskripsikan prosedur yang diikuti dan menjelaskan proses pengambilan keputusan untuk memperoleh setiap Bukti Elektronik;
b) Keandalan: Semua proses yang digunakan dalam penanganan Bukti Elektronik potensial harus dapat diaudit dan dapat diulang. Hasil dari penerapan proses tersebut harus dapat diproduksi ulang; dan
c) Kecukupan: PPBE harus mempertimbangkan bahwa bukti yang dikoleksi telah cukup untuk melaksanakan proses investigasi yang tepat. Melalui audit dan justifikasi, PPBE harus dapat memberikan petunjuk jumlah bukti secara total yang perlu dipertimbangkan dan prosedur yang digunakan untuk menentukan jumlah dan jenis bukti yang diakuisisi.

5.3.2 *Auditability* (Dapat Diaudit)

Penilai independen atau pihak berwenang yang berkepentingan lainnya harus dimungkinkan untuk dapat mengevaluasi tindakan yang dilakukan oleh PPBE dan SBE. Ini dapat dilakukan dengan adanya dokumentasi yang memadai untuk semua tindakan yang dilakukan. PPBE dan SBE harus dapat menjustifikasi proses pengambilan keputusan dalam memilih langkah yang dilakukan. Proses yang

dilakukan oleh PPBE dan SBE harus tersedia bagi penilai independen untuk menentukan bahwa ketepatan metode ilmiah, teknik atau prosedur telah diterapkan.

5.3.3 Dapat Diulang

Kemampuan dapat diulang dibuktikan ketika hasil tes yang sama dapat dihasilkan dalam kondisi sebagai berikut:

a. Menggunakan prosedur pengukuran dan metode yang sama;
b. Menggunakan peralatan yang sama dan dalam kondisi yang sama; dan
c. Dapat diulang setiap saat setelah pengujian awal.

Seorang PPBE yang terampil dan berpengalaman seharusnya dapat melakukan semua proses yang dijelaskan dalam dokumentasi dan memperoleh hasil yang sama, tanpa panduan atau interpretasi. PPBE harus memperhatikan bahwa dapat ditemukan situasi di mana pengujian tidak memungkinkan untuk diulang, misalnya ketika perangkat keras asli telah disalin dan dikembalikan untuk digunakan, atau ketika bukti tersebut terkait dengan memori volatil. Pada kasus ini, PPBE harus memastikan proses Akuisisi dapat diandalkan. Untuk memenuhi persyaratan dapat diulang, kontrol kualitas dan dokumentasi proses harus dibuat.

5.3.4 Dapat Diproduksi Ulang

Kemampuan dapat diproduksi ulang dibuktikan ketika hasil tes yang sama dapat dihasilkan dalam kondisi sebagai berikut:

a. Menggunakan metode pengukuran yang sama;
b. Menggunakan peralatan yang berbeda dan dalam kondisi yang berbeda; dan
c. Dapat diproduksi ulang setiap saat setelah pengujian awal.

5.3.5 Dapat Dijustifikasi

PPBE harus dapat menjustifikasi semua tindakan dan metode yang digunakan dalam menangani Bukti Elektronik potensial. Justifikasi dapat dibuktikan

dengan menunjukkan bahwa keputusan merupakan pilihan terbaik untuk mendapatkan semua Bukti Elektronik potensial. PPBE atau SBE lain dapat pula menunjukkan hal ini dengan berhasil melakukan produksi ulang atau memvalidasi tindakan dan metode yang digunakan.

Demi pertimbangan terbaik bagi organisasi, maka organisasi sebaiknya mempekerjakan PPBE atau SBE yang menguasai keterampilan inti dan kompetensi seperti yang dijelaskan dalam Lampiran A tentang deskripsi kemampuan dan kompetensi inti PPBE dari Panduan ini. Hal ini akan memastikan bahwa proses dan prosedur yang benar diikuti ketika menangani Bukti Elektronik potensial untuk memastikan Preservasi aktual dari Bukti Elektronik yang memiliki kekuatan pembuktian. Hal ini juga akan memastikan bahwa organisasi dapat menggunakan Bukti Elektronik potensial, misalnya, dalam prosedur penegakan disiplin organisasi tersebut atau dalam memudahkan pertukaran Bukti Elektronik potensial antar wilayah.

CATATAN Kompetensi yang dijelaskan dalam Lampiran A tentang deskripsi kemampuan dan kompetensi inti PPBE terbatas pada fungsi PPBE yang sejalan dengan peran SBE sebagaimana didefinisikan dalam klausul 3.8.

5.4 Proses Penanganan Bukti Elektronik

5.4.1 Ikhtisar (*Overview*)

Meskipun proses penanganan Bukti Elektronik yang lengkap juga meliputi tindakan lainnya (misalnya presentasi, penyelesaian, dll), ruang lingkup Standar Nasional ini hanya berkaitan dengan proses penanganan awal yang terdiri dari Identifikasi, Koleksi, Akuisisi, dan Preservasi Bukti Elektronik potensial.

Bukti Elektronik pada dasarnya bersifat rapuh. Bukti Elektronik dapat berubah, diubah, atau rusak karena penanganan atau pemeriksaan yang tidak tepat. Personal yang menangani Bukti Elektronik harus kompeten untuk mengidentifikasi dan mengelola risiko serta konsekuensi dari tindakan potensial ketika berhadapan dengan Bukti Elektronik. Kegagalan dalam menangani perangkat digital dengan cara yang tepat dapat menyebabkan Bukti Elektronik potensial yang terdapat pada perangkat digital tersebut tidak dapat digunakan.

PPBE dan SBE harus mengikuti prosedur yang terdokumentasi untuk memastikan integritas dan keandalan Bukti Elektronik potensial dapat

dipertahankan. Prosedur harus meliputi pedoman penanganan sumber Bukti Elektronik potensial dan harus mencakup prinsip dasar berikut:

a. Meminimalkan penanganan Perangkat Elektronik asli atau Bukti Elektronik potensial;
b. Memperhitungkan perubahan apapun dan mendokumentasikan tindakan yang diambil (hingga tahap ketika seorang ahli mampu memberikan penilaian terkait keandalan);
c. Mematuhi aturan pedoman bukti lokal; dan
d. PPBE dan SBE tidak boleh melakukan tindakan melebihi kompetensi mereka.

Bukti Elektronik harus dipreservasi dengan mematuhi prinsip fundamental dan persyaratan penanganan Bukti Elektronik. Khususnya dalam kondisi ketika perubahan tidak dapat dihindari untuk dilakukan, maka semua tindakan dan alasan harus terdokumentasi. Setiap proses penanganan Bukti Elektronik, yaitu Identifikasi, Koleksi, Akuisisi dan Preservasi, dibahas secara lebih rinci dalam klausul selanjutnya.

5.4.2 Identifikasi

Bukti Elektronik direpresentasikan dalam bentuk fisik dan logis. Bentuk fisik meliputi representasi data dalam sebuah perangkat berwujud. Bentuk logis dari Bukti Elektronik potensial mengacu pada representasi virtual dari data di dalam perangkat.

Proses Identifikasi melibatkan pencarian, pengenalan, dan dokumentasi Bukti Elektronik potensial. Proses Identifikasi harus mengenali Media Penyimpanan Elektronik dan perangkat pemrosesan yang berisi Bukti Elektronik potensial yang relevan dengan perkara. Proses ini juga mencakup tindakan memprioritaskan Koleksi bukti berdasarkan sifat mudah berubah dari bukti tersebut. Sifat mudah berubah dari data harus diidentifikasi untuk memastikan urutan yang benar dari proses Koleksi dan Akuisisi demi meminimalkan kerusakan pada Bukti Elektronik potensial dan untuk mendapatkan alat bukti terbaik. Sebagai tambahan, proses harus mengidentifikasi kemungkinan adanya Bukti Elektronik potensial yang tersembunyi. PPBE dan SBE harus menyadari bahwa tidak semua jenis Media Penyimpanan Elektronik dapat dengan mudah diidentifikasi dan ditemukan, misalnya untuk teknologi komputasi awan, NAS dan SAN - semua menambahkan komponen virtual ke dalam proses Identifikasi.

PPBE harus melakukan pencarian menyeluruh atas bukti yang dapat berisi Bukti Elektronik potensial secara sistematis. Perangkat digital dengan jenis berbeda-beda yang mungkin mengandung Bukti Elektronik dapat dengan mudah terabaikan (misalnya dikarenakan ukurannya yang kecil), tersamarkan atau tercampur dengan bukti lainnya yang tidak relevan.

Klausul 6.1 dan 6.6 memberikan informasi lebih lanjut mengenai aspek rantai pengawasan (*chain of custody*), pembungkusan dan pelabelan dalam Identifikasi Bukti Elektronik. Klausul 7 merincikan pedoman yang relevan untuk contoh khusus dari proses Identifikasi, Koleksi, Akuisisi dan Preservasi Bukti Elektronik.

5.4.3 Koleksi

Setelah perangkat digital yang mengandung Bukti Elektronik potensial telah diidentifikasi, PPBE dan SBE harus memutuskan untuk mengkoleksi atau mengakuisisi pada proses berikutnya. Terdapat beberapa faktor penentu untuk hal tersebut, yang dibahas secara lebih rinci dalam klausul 7. Keputusan harus berdasarkan pada kondisi saat itu.

Koleksi adalah proses penanganan Bukti Elektronik ketika perangkat yang berisi Bukti Elektronik potensial dipindahkan dari lokasi asli ke laboratorium atau lingkungan lain yang terkendali untuk Akuisisi dan analisis selanjutnya. Perangkat yang berisi Bukti Elektronik potensial mungkin berada di salah satu dari dua keadaan; ketika sistem dalam kondisi menyala atau ketika sistem dalam kondisi mati. Pendekatan dan alat yang berbeda diperlukan, bergantung pada keadaan perangkat tersebut.

Proses ini meliputi pendokumentasian seluruh pendekatan, serta pembungkusan perangkat sebelum dipindahkan. Penting bagi PPBE dan SBE untuk mengumpulkan bukti apapun yang mungkin berhubungan dengan Informasi Elektronik potensial (misalnya kertas dengan catatan *password*, stasiun dok atau replikator *port* dan konektor daya untuk perangkat sistem tertanam). Bukti Elektronik potensial dapat hilang atau rusak jika tidak menerapkan perawatan secara hati-hati. PPBE dan SBE harus mengadopsi metode Koleksi terbaik yang dimungkinkan, berdasarkan situasi, biaya dan waktu, serta mendokumentasikan keputusan dalam menggunakan suatu metode tertentu.

CATATAN 1 Pemindahan media penyimpanan digital tidak selalu direkomendasikan dan PPBE harus yakin bahwa mereka kompeten untuk

memindahkan media penyimpanan, dan memahami saat yang tepat dan diizinkan untuk melakukannya.
CATATAN 2 Rincian dari perangkat digital yang tidak dikoleksi harus didokumentasikan dengan justifikasinya.

5.4.4 Akuisisi

Proses Akuisisi menghasilkan salinan Bukti Elektronik (misalnya perangkat keras utuh, partisi, *file* terpilih) dan dokumentasi metode yang digunakan dan tindakan yang dilakukan. PPBE harus mengadopsi metode Akuisisi yang sesuai berdasarkan situasi, biaya dan waktu, serta mendokumentasikan keputusan untuk menggunakan metode atau alat tertentu dengan tepat.
Metode yang digunakan untuk mengakuisisi Bukti Elektronik potensial harus didokumentasikan secara jelas dan rinci, dan sepanjang pelaksanaannya, dapat diproduksi ulang atau dapat diverifikasi oleh PPBE yang kompeten. PPBE atau SBE harus mengakusisi Bukti Elektronik potensial dengan cara yang paling tidak merusak untuk menghindari perubahan data digital sepanjang dimungkinkan. Dalam menerapkan proses ini PPBE harus mempertimbangkan metode yang paling tepat untuk digunakan. Jika proses berakibat pada perubahan yang tidak dapat dihindari terhadap data digital, maka tindakan yang dilakukan harus didokumentasikan untuk memberikan justifikasi perubahan data.
Metode Akuisisi yang digunakan harus menghasilkan salinan Bukti Elektronik dari Bukti Elektronik potensial atau perangkat digital yang mengandung Bukti Elektronik potensial. Baik sumber asli maupun salinan Bukti Elektronik harus diverifikasi dengan fungsi verifikasi yang telah terbukti keakuratannya yang dapat diterima oleh pihak yang akan menggunakan bukti tersebut. Sumber asli dan setiap salinan Bukti Elektronik harus menghasilkan hasil fungsi verifikasi yang sama.
Pada kondisi ketika proses verifikasi tidak dapat dilakukan, misalnya ketika mengakuisisi sistem yang sedang berjalan, salinan asli mengandung *bad sector*, atau jangka waktu Akuisisi terbatas. Pada contoh tersebut, PPBE harus menggunakan metode terbaik yang tersedia dan dapat menjustifikasi serta mempertahankan pemilihan metode. Jika penyalinan tidak dapat diverifikasi, maka perlu didokumentasikan dan diberikan justifikasi. Jika diperlukan, metode Akuisisi yang digunakan harus dapat memperoleh *allocated* dan *unallocated space*.

CATATAN 1 Ketika proses verifikasi tidak dapat dilakukan pada sumber secara utuh karena disebabkan kesalahan pada sumbernya, maka verifikasi boleh menggunakan bagian-yang diyakini dapat terbaca.

Ada kemungkinan terdapat kondisi di mana tidak memungkinkan atau diperbolehkan untuk membuat salinan Bukti Elektronik dari sebuah sumber bukti, seperti ketika sumber terlalu besar. Dalam hal ini, PPBE dapat melakukan Akuisisi logis, yang targetnya hanya tipe data, direktori atau lokasi yang spesifik. Hal ini umumnya terjadi pada tingkat *file* dan partisi. Selama pelaksanaan Akuisisi logis, *active file* dan *allocated space non-file-based* pada media penyimpanan digital dapat disalin; *file* yang sudah dihapus dan *unallocated space* tidak dapat disalin, tergantung pada metode yang digunakan. Kondisi lain dimana penggunaan metode ini dapat berguna ialah ketika sistem penting atau vital terlibat sehingga tidak dapat dimatikan.

5.4.5 Preservasi

Bukti Elektronik potensial harus dipreservasi untuk menjamin kegunaannya dalam investigasi. Melindungi integritas dari bukti menjadi hal yang penting. Proses Preservasi melibatkan pengamanan Bukti Elektronik potensial dan perangkat Elektronik yang mengandung Bukti Elektronik potensial dari perusakan (*spoliation*) atau pengubahan (*tampering*). Proses Preservasi harus dimulai dan dipertahankan dalam seluruh proses penanganan Bukti Elektronik, sejak dari Identifikasi perangkat digital yang mengandung Bukti Elektronik potensial.

Dalam kondisi terbaik, seharusnya tidak ada perusakan (*spoliation*) terhadap data itu sendiri ataupun metadata yang terkait dengannya (misalnya tanggal dan penanda waktu). PPBE harus mampu menunjukkan bahwa bukti belum diubah sejak dikoleksi atau diakuisisi, atau memberikan alasan dan tindakan yang didokumentasikan jika perubahan tidak dapat dihindari.

CATATAN Bukti Elektronik potensial harus dipreservasi dengan cara yang menjamin kerahasiaan data.

6 Komponen Kunci Identifikasi, Koleksi, Akuisisi Dan Preservasi Bukti Elektronik

6.1 Rantai Pengawasan (*Chain of Custody*)

Dalam setiap investigasi, PPBE harus mampu memberikan justifikasi pada semua data dan perangkat yang diakuisisi pada saat berada dalam pengawasan PPBE. Catatan rantai pengawasan (*Chain of custody record*) adalah dokumen yang mengidentifikasi kronologi pemindahan dan penanganan Bukti Elektronik potensial. Catatan ini harus dibuat mulai dari proses Koleksi atau Akuisisi. Hal ini biasanya akan diselesaikan dengan menelusuri riwayat bukti sejak berhasil dilakukan Identifikasi, Koleksi atau Akuisisi oleh tim investigasi hingga status dan lokasi saat ini.

Catatan rantai pengawasan adalah dokumen atau serangkaian dokumen terkait yang merincikan rantai pengawasan dan catatan atas siapa yang bertanggung jawab untuk menangani Bukti Elektronik potensial, baik dalam bentuk Informasi Elektronik dan/atau Dokumen Elektronik atau format lain (seperti catatan kertas). Tujuan menjaga catatan rantai pengawasan adalah untuk memungkinkan teridentifikasinya akses dan pemindahan Bukti Elektronik potensial pada titik waktu tertentu. Catatan rantai pengawasan itu sendiri dapat terdiri lebih dari satu dokumen, misalnya untuk Bukti Elektronik potensial seharusnya terdapat dokumen kontemporer yang merekam Akuisisi data digital ke perangkat tertentu, pemindahan dari perangkat tersebut dan dokumentasi merekam ekstraksi atau salinan Bukti Elektronik potensial susulan untuk tujuan analisis atau lainnya. Catatan rantai pengawasan minimal harus berisi informasi berikut:

a. Tanda pengenal bukti yang unik;
b. Siapa yang mengakses bukti dan waktu serta lokasi terjadinya;
c. Siapa yang memeriksa bukti di dalam dan di luar dari fasilitas Preservasi bukti dan kapan hal itu terjadi;
d. Mengapa bukti tersebut diperiksa (kasus dan tujuan) dan otoritas yang relevan, jika ada;
e. Setiap perubahan yang tidak dapat dihindari pada Bukti Elektronik potensial, serta nama individu yang bertanggung jawab karenanya dan justifikasi untuk pengubahan.

Rantai pengawasan harus dipertahankan selama masa daluwarsa Bukti Elektronik belum berakhir dan dipreservasi dalam jangka waktu tertentu setelah berakhirnya masa daluwarsa Bukti Elektronik. Rantai pengawasan harus diterapkan sejak saat perangkat digital dan/atau Bukti Elektronik potensial diakuisisi dan tidak boleh dikompromis.

6.2 Tindakan Pencegahan di Lokasi Kejadian

6.2.1 Umum (*General*)

PPBE harus melakukan tindakan untuk mengamankan dan melindungi lokasi Bukti Elektronik potensial segera setelah mereka tiba di lokasi. Tindakan yang dilakukan harus sesuai dengan peraturan perundang-undangan:

a. Mengamankan dan memegang kendali area yang berisi perangkat;
b. Menentukan siapa individu yang bertanggung jawab di lokasi;
c. Memastikan individu dijauhkan dari perangkat dan daya listrik;
d. Mendokumentasikan siapa saja yang memiliki akses ke lokasi dan siapa saja yang diduga memiliki alasan untuk terlibat dengan tempat kejadian perkara;
e. Jika perangkat dalam keadaan menyala jangan mematikannya dan jika perangkat dalam keadaan mati jangan menyalakannya;
f. Jika memungkinkan, dokumentasikan (misalnya sketsa, foto atau video) tempat kejadian perkara, semua komponen dan kabel dalam posisi semula. Jika tidak ada kamera dan/atau kamera video yang tersedia, gambar sketsa denah sistem dan beri label pada port dan kabel sehingga sistem dapat divalidasi dan direkonstruksi di kemudian hari; dan
g. Jika diperbolehkan, lakukan pencarian di area untuk barang-barang seperti catatan tempel (*sticky note*), buku harian, kertas, komputer *notebook*, atau perangkat keras dan manual perangkat lunak dengan rincian yang penting tentang perangkat seperti *password* dan PIN.

CATATAN 1 PPBE perlu menyadari bahwa Bukti Elektronik potensial mungkin tidak selalu berada di lokasi yang jelas, seperti penyimpanan yang terdistribusi atau tervirtualisasi.

PPBE harus paham sedari dini akan semua risiko yang terlibat dalam melakukan semua proses selama investigasi. Keamanan personel dan Bukti

Elektronik potensial di tempat kejadian perkara harus menjadi bahan pertimbangan.

6.2.2 Personel

Melakukan penilaian risiko terhadap keamanan personel sebelum memulai proses merupakan hal penting karena keselamatan personel yang terlibat dalam proses merupakan sesuatu yang vital. Hal yang harus dipertimbangkan dalam menilai risiko terhadap personel meliputi, namun tidak terbatas pada hal berikut:

a. Keberadaan Individu yang diselidiki di lokasi dan kecenderungan individu untuk melakukan kekerasan.
b. Waktu dilaksanakannya kegiatan operasional.
c. Dapat diisolasinya tempat kejadian perkara dari kerumunan orang.
d. Keberadaan senjata di sekitar tempat kejadian perkara.
e. Keberadaan bahaya fisik pada individu.
f. Kemungkinan adanya bahaya kerusakan fisik yang dapat ditimbulkan oleh perangkat jika ditangani dengan cara yang tidak tepat.
g. timbulnya kerusakan atau gangguan psikologis yang terjadi akibat proses pengkoleksian bahan.
h. Keamanan tempat kejadian perkara.
i. Kemungkinan timbulnya risiko potensial dari area sekitar tempat kejadian perkara.
j.

6.2.3 Bukti Elektronik Potensial

PPBE harus berhati-hati ketika menggunakan alat bantu khusus untuk mengoleksi atau mengakuisisi Bukti Elektronik potensial. Tidak menghitung risiko sebelum bertindak dapat berujung pada hilangnya sebagian atau seluruh Bukti Elektronik potensial disebabkan oleh teknologi yang diterapkan selama proses Koleksi atau Akuisisi. Risiko harus dinilai untuk mengurangi peluang pada gugatan untuk kerusakan.

Penilaian risiko melibatkan evaluasi risiko yang sistematis dan potensi dampak yang mungkin dimiliki pada investigasi Bukti Elektronik. Aspek yang perlu dipertimbangkan saat penilaian risiko untuk Bukti Elektronik potensial meliputi, namun tidak terbatas pada hal berikut:

a. Penentuan jenis metode Koleksi / Akuisisi yang akan digunakan;
b. Penentuan kebutuhan peralatan yang diperlukan di tempat kejadian perkara;
c. Tingkat volatilitas data dan informasi yang berkaitan dengan Bukti Elektronik potensial;
d. Kemungkinan untuk dilakukannya akses jarak jauh ke perangkat digital dan kemungkinan timbulnya ancaman pada integritas bukti akibat akses jarak jauh ke perangkat digital tersebut;
e. Identifikasi risiko jika terjadi kerusakan data / peralatan;
f. Identifikasi terhadap kemungkinan adanya gangguan data; dan
g. Kemungkinan perangkat digital telah dikonfigurasi untuk menghancurkan (misalnya menggunakan sebuah bom-logis), merusak atau mengaburkan data jika dimatikan atau diakses dengan cara yang tidak terkendali.

6.3 Peran Dan Tanggung Jawab

Peran PPBE meliputi Identifikasi, Koleksi, Akuisisi dan Preservasi Bukti Elektronik potensial di tempat kejadian perkara. Di dalamnya termasuk pembuatan laporan Koleksi dan Akuisisi, namun tidak perlu sampai laporan analisis. Peran PPBE juga memastikan integritas dan keaslian Bukti Elektronik potensial. Dalam memenuhi perannya, PPBE harus memiliki pengalaman, keterampilan dan pengetahuan yang memadai dalam menangani Bukti Elektronik potensial. Hal ini sangat penting karena Bukti Elektronik potensial dapat dengan mudah rusak.

PPBE juga mungkin memerlukan bantuan dari personel dukungan teknis di bidang terkait. Peran dari SBE termasuk memberikan dukungan teknis kepada PPBE dalam mengidentifikasi, mengoleksi, mengakuisisi dan mempreservasi Bukti Elektronik potensial di tempat kejadian perkara. SBE memberikan bantuan keahlian khusus untuk PPBE. Matriks kompetensi untuk PPBE (lihat Lampiran A) berfungsi sebagai panduan untuk mengidentifikasi tingkat kompetensi PPBE yang relevan.

6.4 Kompetensi

PPBE dan/atau SBE harus memiliki kompetensi teknis dan hukum yang relevan (misalnya yang terdapat dalam Lampiran A) dan harus mampu menunjukkan bahwa mereka terlatih dengan baik serta memiliki pemahaman teknis dan hukum yang memadai untuk menangani Bukti Elektronik potensial secara tepat. Termasuk pemahaman tentang proses dan metode yang tepat untuk penanganan potensi sumber Bukti Elektronik. Pelatihan yang memadai akan memungkinkan PPBE untuk menangani perangkat digital yang berpotensi mengandung Bukti Elektronik. Memiliki rangkaian alat terbaik tidak akan menjamin kualitas Bukti Elektronik jika PPBE tidak kompeten dalam menjalankan tugas.

PPBE bertanggung jawab untuk menangani Bukti Elektronik sesuai dengan ketentuan peraturan perundang-undangan. PPBE dan/atau ₱SBE harus mampu menunjukkan bahwa mereka kompeten untuk menangani Bukti Elektronik potensial menggunakan peralatan dan metode yang terpilih. PPBE harus mampu memberikan bukti kompetensi mereka secara berkesinambungan.

Beberapa prasyarat untuk PPBE adalah sebagai berikut:

a. Harus terlatih dengan cukup dan tepat untuk menangani perangkat digital dalam konteks kegiatan investigasi;
b. Harus menunjukkan dan memelihara keterampilan serta kompetensi kepada pihak yang berwenang di bidang penanganan Bukti Elektronik potensial yang relevan; dan
c. PPBE dan institusi bertanggung jawab memastikan bahwa PPBE terlatih dengan cukup dan dapat mempertahankan keterampilan dan kompetensi.

6.5 Tindakan Yang Bertanggung Jawab

Hindari tindakan yang bisa berujung pada perusakan Bukti Elektronik potensial yang tersimpan dalam perangkat digital disebabkan oleh tindakan yang disengaja atau tidak disengaja. Misalnya, paparan medan magnet dapat merusak Bukti Elektronik potensial yang terkandung dalam media penyimpanan magnetik. PPBE tidak boleh mengakses perangkat digital, seperti melakukan *dump memory* dari perangkat digital yang menyala, kecuali mereka telah

memiliki kompetensi yang diperlukan dan dengan menggunakan proses yang andal dan tervalidasi.

Ada beberapa situasi di mana tidak memungkinkan untuk mengoleksi atau mengakuisisi Bukti Elektronik potensial. PPBE harus mempertimbangkan situasi berikut, namun tidak hanya terbatas pada:

a. Ketika tidak ada hak hukum atau otorisasi untuk mengoleksi perangkat elektronik;
b. Ketika terdapat kewajiban untuk menggunakan metode lain (misalnya untuk menghindari gangguan pada bisnis);
c. Ketika PPBE ingin merekam modus operasi tersangka pada saat terjadinya penyalahgunaan sistem;
d. Ketika perangkat elektronik *mission-critical* bagi bisnis tidak dapat mentoleransi penghentian;
e. Ketika ukuran fisik dari perangkat elektronik terlalu besar, seperti server di pusat data atau sistem RAID;
f. Ketika perangkat elektronik yang kritis bagi keselamatan akan membahayakan hidup jika dihentikan; dan
g. Ketika perangkat elektronik juga melayani pihak yang tidak terlibat.

6.6 Dokumentasi

Dokumentasi menjadi sangat penting ketika menangani perangkat digital yang mengandung Bukti Elektronik potensial. PPBE harus mematuhi hal berikut saat melakukan dokumentasi:

a. Setiap tindakan yang dilakukan harus didokumentasikan. Pendokumentasian ini dimaksudkan untuk memastikan bahwa tidak ada tindakan yang tertinggal selama proses Identifikasi, Koleksi, Akuisisi dan Preservasi. Hal ini juga dapat sangat membantu dalam investigasi lintas batas wilayah di mana Bukti Elektronik potensial yang dikoleksi dari negara lain dapat ditelusuri.
b. PPBE harus peka terhadap pengaturan waktu dan tanggal jika perangkat elektronik dalam keadaan menyala. Bandingkan pengaturan waktu dengan sumber waktu yang terpercaya, seperti waktu yang disinkronisasikan dengan sumber waktu yang terpercaya dan dapat dilacak. Pengaturan waktu ini harus didokumentasikan dan dicatat jika ditemukan perbedaan. Beberapa sistem membutuhkan interaksi pengguna untuk mendapatkan informasi pengaturan waktu dan tanggal.

PPBE harus berhati-hati untuk tidak memodifikasi sistem. Hanya personel yang terlatih dengan cukup yang dapat mengambil informasi pengaturan ini.

c. PPBE harus mendokumentasikan semua yang terlihat pada layar perangkat elektronik: program dan proses aktif, beserta dengan nama-nama dokumen yang terbuka. Dokumentasi ini harus mencakup deskripsi dari apa yang terlihat mengingat beberapa program berbahaya dapat menyamar sebagai perangkat lunak yang dikenal.
d. Setiap perpindahan perangkat elektronik harus didokumentasikan sesuai dengan peraturan perundang-undangan.
e. Mendokumentasikan semua pengenal unik dari perangkat elektronik dan bagian-bagian yang terkait seperti nomor seri dan tanda-tanda yang unik.

Contoh satu rangkaian dokumentasi minimal dalam penanganan Bukti Elektronik terdapat pada Lampiran B.

6.7 Pengarahan

6.7.1 Umum

Sangat penting bahwa PPBE dan SBE diberikan pengarahan yang cukup oleh otoritas yang berwenang apabila akan melakukan tugas-tugas mereka, dengan mematuhi segala peraturan perundang-undangan terkait kerahasiaan dan batasan pemeriksaan. Penting untuk mengadakan sesi pengarahan yang formal untuk memahami perkara, apa yang diharapkan dan tidak diharapkan selama investigasi, dan penekanan kembali terhadap pengubahan (*tampering*) atau perusakan (*spoliation*) bukti. Pengarahan harus cukup memadai untuk PPBE dan SBE agar mereka dapat mempersiapkan diri dengan baik dalam melaksanakan peran dan tanggung jawabnya; sehingga proses ekstraksi dari semua Bukti Elektronik potensial yang terkait dapat dipastikan.

6.7.2 Pengarahan Khusus Bukti Elektronik

Sebuah sesi pengarahan yang secara eksplisit berfokus pada panduan yang spesifik pada Bukti Elektronik diperlukan untuk menginformasikan PPBE mengenai rincian yang berkaitan dengan investigasi. Selama sesi pengarahan, PPBE dan SBE harus diberikan informasi yang relevan dan petunjuk yang rinci

terkait dengan Bukti Elektronik potensial yang akan dikoleksi atau diakuisisi. Hal ini termasuk:

a. Jenis perkara (jika diketahui);
b. Tanggal dan waktu perkara (jika diketahui);
c. Rencana investigasi (koleksi dan/atau Akuisisi, aktivitas jaringan yang diketahui, kebutuhan data volatil yang diketahui, dll);
d. Mempertimbangkan lokasi dan cara Bukti Elektronik potensial disimpan atau dipindahkan setelah Koleksi atau Akuisisi;
e. Peralatan khusus yang diperlukan untuk mengakuisisi Bukti Elektronik potensial;
f. Bukti Elektronik potensial yang berhubungan dengan tipe investigasi tertentu;
g. Perlengkapan dan panduan yang berhubungan dengan perangkat elektronik;
h. Mengingatkan PPBE dan SBE untuk menonaktifkan *Bluetooth* atau Wi-Fi pada ponsel dan/atau komputer mereka sehingga mereka tidak secara sengaja berinteraksi dengan perangkat digital, kecuali untuk ponsel dan/atau komputer yang digunakan untuk mendeteksi koneksi;
i. Pentingnya dokumentasi pada setiap tahapan investigasi; dan
j. Peraturan perundang-undangan atau faktor lainnya yang dapat mencegah Koleksi perangkat dan Bukti Elektronik potensial yang dikandungnya.

Pengarahan khusus ini dapat merupakan bagian dari sesi pengarahan umum seperti yang dijelaskan dalam klausul 6.7.1.

6.7.3 Pengarahan Khusus Pada Personel

Sebuah sesi pengarahan yang secara eksplisit berfokus pada panduan yang spesifik pada personel diperlukan untuk menginformasikan PPBE mengenai aspek-aspek yang berkaitan dengan pihak yang terlibat dalam investigasi. Selama sesi pengarahan, tim investigasi akan dilengkapi dengan instruksi mengenai personel. Hal ini termasuk:

a. Tugas, peran dan tanggung jawab anggota tim investigasi di tempat kejadian perkara;
b. Identifikasi kebutuhan personel lain yang terlibat (tenaga medis, penyidik forensik biologis, dll) dalam investigasi;
c. Mewajibkan anggota tim untuk tidak menerima bantuan teknis dari individu yang tidak berwenang; dan

d. Mewajibkan anggota tim untuk mengikuti prosedur secara ketat dalam meminimalkan risiko perusakan Bukti Elektronik potensial, seperti menghindari penggunaan alat atau bahan yang dapat menghasilkan atau memancarkan listrik statis atau medan magnet karena dapat merusak atau menghancurkan Bukti Elektronik potensial.

Pengarahan khusus ini dapat menjadi bagian dari sesi pengarahan umum seperti yang dijelaskan dalam klausul 6.7.1.

6.7.4 Insiden *real-time*

Sangat diharapkan bahwa investigasi suatu insiden harus direncanakan terlebih dahulu, tetapi terdapat kondisi (misalnya ketika insiden sedang terjadi dan sedang ditanggapi secara *real time*) di mana perencanaan yang utuh tidak dimungkinkan. Dalam situasi ini, tim harus mendapatkan arahan tentang strategi dan taktik awal untuk investigasi dan diperbolehkan untuk mengembangkan strategi dan taktik baru dalam menanggapi kondisi yang terjadi. Informasi tentang insiden tersebut, seiring dengan perkembangan insiden yang dimaksud, harus disebarkan dalam tim secepat mungkin untuk memastikan keputusan atas tindakan yang harus dilakukan dapat diambil secara efisien dan dapat dipertanggungjawabkan.

6.7.5 Informasi Pengarahan Lainnya

Selain Bukti Elektronik dan personel, informasi penting lainnya yang harus diarahkan kepada PPBE dan SBE meliputi:

a. Penetapan wilayah yang diinvestigasi, termasuk nama organisasi, alamat dan peta lokasi (jika tersedia);
b. Surat perintah tugas;
c. Rincian surat perintah penggeledahan dan surat kuasa lainnya yang berlaku untuk investigasi, termasuk batasan penggeledahan dan penyitaan;
d. Aspek hukum dan implikasinya;
e. Kerangka waktu investigasi;
f. Peralatan yang perlu dibawa ke tempat kejadian perkara investigasi;
g. Informasi logistik; dan
h. Potensi konflik kepentingan.

PPBE harus menghindari situasi di mana tuduhan-tuduhan terhadap bias yang melekat (*inherent bias*) dapat ditujukan kepadanya. Contoh bias yang melekat adalah ketika PPBE menyalin satu komputer saja dan tidak yang lainnya (yang kemudian diketahui mengandung bukti yang dapat dikecualikan (*exculpatory evidence*)) berdasarkan pemahaman yang terbentuk oleh pengarahan.

6.8 Memprioritaskan Koleksi dan Akuisisi

Dalam memprioritaskan Koleksi atau Akuisisi Bukti Elektronik potensial, adalah suatu keharusan bagi PPBE untuk memahami alasan Bukti Elektronik potensial tersebut dikoleksi atau diakuisisi. Sebagai prinsip umum, PPBE harus berusaha untuk memaksimalkan jumlah data yang dipreservasi dari tindakan Koleksi dan Akuisisi. Namun, ada saatnya perlu untuk memprioritaskan perangkat elektronik berdasarkan tingkat volatil dan/atau relevansi atau potensi kekuatan pembuktian. Perangkat elektronik dengan relevansi yang tinggi atau potensi kekuatan pembuktian adalah yang paling memungkinkan berisi data yang berkaitan langsung dengan insiden yang sedang diselidiki.

Pemberian prioritas berdasarkan volatilitas hanya dapat diterapkan jika keadaan tertentu dari kasus yang sedang diselidiki membutuhkan pemberian prioritas tersebut. Bukti Elektronik potensial dapat dibagi menjadi dua kategori: volatil dan non-volatil. Data volatil dapat dengan mudah dihancurkan atau dihilangkan selamanya jika pemeliharaan yang tepat untuk melindungi data tidak diterapkan. Sebagai contoh, melepaskan sumber daya dari perangkat elektronik dapat mengakibatkan hilangnya data volatil. Data non-volatil tetap berada di media meskipun sumber daya telah dilepaskan. Karena beberapa jenis Bukti Elektronik mungkin memiliki jangka hidup yang pendek, Bukti Elektronik potensial dapat dengan mudah diubah atau dirusak. Ketika tidak jelas apakah perangkat elektronik berisi Bukti Elektronik potensial, atau perangkat elektronik mana yang lebih relevan daripada yang lain, mungkin diperlukan pemeriksaan terhadap perangkat tersebut sebelum Koleksi dengan menggunakan sebuah proses untuk menentukan prioritas. Perangkat elektronik yang dipertimbangkan untuk dikoleksi meliputi, namun tidak terbatas pada; peralatan TI dan media penyimpanan digital, sistem CCTV, PED, sistem otomotif, sistem kontrol dan elektronik yang diimprovisasi. Akuisisi Bukti Elektronik potensial yang paling volatil dilakukan pertama seperti RAM, *swap space*, proses yang berjalan, dll. PPBE harus memiliki pemahaman mendalam untuk memberikan prioritas sesuai dengan sifat volatilnya.

Setelah Identifikasi, PPBE harus:

a. Memprioritaskan Bukti Elektronik potensial yang akan hilang selamanya jika sumber daya dilepaskan; dan
b. Mengambil tindakan cepat untuk mengoleksi dan mengakuisisi data ~~ini~~ dengan metode yang tervalidasi.

CATATAN 1 Beberapa data volatil dapat berubah karena faktor-faktor yang meliputi namun tidak terbatas pada lokasi, waktu dan perubahan pada perangkat elektronik sekitar - memastikan data tersebut dipreservasi sebelum memindahkan perangkat.

CATATAN 2 Perangkat Elektronik mengandung Bukti Elektronik dapat menjadi sumber bukti fisik (misalnya sidik jari, DNA, dll). PPBE perlu berhati-hati untuk tidak merusak bukti tersebut dan berkoordinasi dengan pengumpul bukti yang relevan sebelum melanjutkan ke kegiatan berikutnya.

CATATAN 3 Ketika diduga terdapat enkripsi atau *malware*, sangat diperlukan untuk memeriksa data volatil.

Dalam situasi-situasi ini, waktu dapat menjadi faktor yang membatasi dalam sebuah investigasi. Dalam kasus ini, preferensi sebaiknya diberikan kepada Bukti Elektronik potensial yang telah diidentifikasi sebagai Bukti Elektronik yang relevan pada insiden tertentu.

6.9 Pemeliharaan Bukti Elektronik Yang Potensial

6.9.1 Ikhtisar

Dalam mempreservasi Bukti Elektronik potensial yang diakuisisi dan perangkat elektronik yang dikoleksi selama pembungkusan, penting untuk mengamankan perangkat-perangkat elektronik tersebut dengan cara yang mampu mengeliminasi bahaya perusakan atau pengubahan. Perusakan (*spoliation*) dapat berakibat dari pengaruh magnetik, degradasi listrik, panas, kelembapan yang tinggi atau rendah, serta guncangan dan getaran. Pengubahan (*tampering*) dapat diakibatkan dari tindakan membuat atau membiarkan pengubahan pada Bukti Elektronik potensial yang disengaja. Oleh karena itu penting untuk melindungi Bukti Elektronik potensial sebaik mungkin, dan menggunakan data asli sesedikit mungkin. Adalah hal yang penting bahwa PPBE terbiasa dengan persyaratan pembungkusan (*packaging*) yang diatur dalam poin 6.9.3.

6.9.2 Preservasi Bukti Elektronik Potensial

Semua perangkat digital yang dikoleksi dan Bukti Elektronik potensial yang diakuisisi harus dilindungi sedapat mungkin dari kehilangan, pengubahan atau perusakan. Kegiatan yang paling penting dalam proses Preservasi adalah untuk menjaga integritas dan keaslian Bukti Elektronik potensial dan rantai pengawasan.

Perangkat digital yang dikoleksi dan Bukti Elektronik potensial yang diakuisisi harus disimpan dalam fasilitas Preservasi bukti yang menerapkan kontrol keamanan fisik seperti sistem kontrol akses, sistem pengawasan atau sistem deteksi intrusi atau lingkungan yang terawasi lainnya untuk Preservasi Bukti Elektronik. Tujuan utama dari keamanan fisik adalah untuk melindungi dan mencegah kehilangan, kerusakan dan pengubahan, serta dapat diaudit.

Perangkat digital yang dikoleksi harus dibungkus atau ditempatkan dalam kemasan memadai yang sesuai dengan sifat dasar perangkat untuk menghindari kontaminasi dari perangkat digital sebelum dipindahkan ke lokasi lain. Kemasan yang tahan guncangan dapat digunakan untuk menghindari kerusakan fisik komponen perangkat.

a. PPBE harus mempertimbangkan kepekaan perangkat digital terhadap listrik statis. Jika hal tersebut menjadi perhatian, perangkat harus diamankan dalam kantong anti-statis.
b. Sistem unit utama dan komputer *notebook* harus diamankan dalam wadah yang memadai untuk menghindari pengubahan atau perusakan Bukti Elektronik potensial yang mungkin berada di dalamnya.

CATATAN Penggunaan kantong *Faraday*, atau kemasan pelindung Gelombang Radio lainnya, dapat mempercepat pengurasan baterai ponsel. Oleh karena itu diperlukan tersedianya daya cadangan ke perangkat tersebut ketika berada di dalam kantong, jika cadangan sumber daya tersebut tersedia.

6.9.3 Pembungkusan Perangkat Digital Dan Bukti Elektronik Yang Potensial

6.9.3.1 Tindakan Utama: Pembungkusan Bukti Elektronik Potensial

Tindakan utama harus dilakukan kecuali ada alasan yang tepat untuk tidak melakukannya. Hal ini juga dapat dikatakan sebagai tindakan minimum yang

harus diambil. Selama pembungkusan, PPBE harus memperhatikan dan melaksanakan tindakan utama sebagai berikut:

a. Tidak menyentuh pita magnetik, melainkan pita diangkat dengan tempat atau area pelindungnya yang diketahui tidak mengandung data (misalnya tepi *disk* optik). Hal ini sebaiknya hanya dilakukan jika PPBE memakai sarung tangan bebas serat.

   CATATAN Area tertentu dari media penyimpanan yang diketahui tidak berisi data bergantung pada tipe media. Menjadi tanggung jawab PPBE untuk mengidentifikasi teknologi terkini dan dapat melakukan penanganan media penyimpanan.

b. Untuk memastikan Identifikasi yang benar, PPBE harus memberikan label pada semua Bukti Elektronik potensial. Format pelabelan ditentukan oleh masing-masing instansi penegak hukum. PPBE harus terbiasa, dan mematuhi, persyaratan yang berlaku dalam hal ini. PPBE harus memberi label semua Bukti Elektronik potensial, perangkat digital yang dikoleksi dan bagian perangkat keras terkait dengan bukti, dengan label yang jelas. Label tersebut akan diketahui jika diubah. Label tidak boleh ditempatkan langsung pada bagian mekanik dari perangkat digital, tidak menutupi atau menyembunyikan informasi penting untuk Identifikasi. Semua Bukti Elektronik potensial dalam perangkat yang telah dikoleksi harus diakuisisi dan disimpan dengan cara tertentu untuk memastikan integritas bukti.
c. Bila memungkinkan, perangkat digital dengan penutup dan komponen yang dapat dipindahkan harus disegel dengan label. PPBE harus menandatangani label sebagai segel sehingga akan diketahui jika label tersebut mengalami perubahan.
d. Perangkat yang melekat dengan baterai dengan data yang volatil harus diperiksa secara berkala untuk memastikan bahwa perangkat selalu memiliki sumber daya yang cukup.
e. Mengidentifikasi dan mengamankan perangkat digital dalam wadah yang sesuai dengan sifat dasar perangkat untuk menghindari pengubahan, pe~~ng~~rusakan atau potensi ancaman lainnya.
f. Komputer dan perangkat digital harus dibungkus sedemikian rupa untuk mencegah kerusakan dari guncangan, getaran, ketinggian, panas, dan pengaruh gelombang radio selama pemindahan.
g. Media penyimpanan magnetik harus disimpan dalam kemasan yang tidak terpengaruh pada magnet, anti-statis dan anti radiasi.

h. Perangkat digital juga dapat mengandung bukti laten, bukti jejak atau bukti biologis. Dengan demikian, kegiatan yang tepat harus dilakukan untuk menjaga Bukti Elektronik potensial. Penyalinan bit per bit Bukti Elektronik harus dilakukan setelah proses pengumpulan bukti laten, bukti jejak, dan bukti biologis dilakukan pada perangkat tersebut. Namun, keputusan untuk memprioritaskan pengumpulan bukti harus dievaluasi secara menyeluruh untuk menjaga bukti.

6.9.3.2 Kegiatan Tambahan: Pembungkusan Bukti Elektronik Potensial

Kegiatan tambahan mengacu pada kegiatan yang sangat direkomendasikan untuk dilakukan. Selama pembungkusan, PPBE harus memperhatikan dan melaksanakan kegiatan tambahan berikut, jika memungkinkan:

a. Gunakan sarung tangan bebas serat dan memastikan bahwa tangan dalam keadaan bersih dan kering;
b. Lindungi perangkat digital dari pengaruh sumber elektromagnetik (misalnya radio komunikasi polisi, speaker, mesin *X-ray*). Lingkungan pembungkusan harus bebas dari listrik statis;
c. Lingkungan pembungkusan harus bebas dari debu, minyak dan polutan kimia yang meningkatkan kerusakan akibat oksidasi dan kondensasi kelembapan pada lapisan magnetik;
d. Meminimalkan kemungkinan induksi magnet pada pita (transfer sinyal dari satu lilitan pita ke lilitan yang berdekatan), yang dapat terjadi ketika kaset yang disimpan dalam waktu lama tanpa penggunaan aktif, sehingga mengakibatkan kualitas sinyal yang buruk;
e. Bila perlu, daerah pembungkusan harus bebas dari sinar UV. UV dapat menyebabkan degradasi DNA atau merusak beberapa jenis media. PPBE harus mempertimbangkan apakah UV menimbulkan risiko ke Bukti Elektronik yang potensial sebelum memilih area pembungkusan; dan
f. Perangkat digital harus sangat dilindungi dari *thermal shock* (kejutan panas).

6.9.4 Pemindahan Bukti Elektronik Yang Potensial

PPBE harus mempreservasi perangkat digital yang telah dikoleksi dan Bukti Elektronik potensial yang telah diakuisisi selama pemindahan. Bukti Elektronik potensial tidak boleh ditinggal tanpa pengawasan selama proses pemindahan. PPBE harus menjaga rantai pengawasan sepanjang proses pemindahan untuk mencegah kemungkinan pengubahan atau perusakan, menjaga integritas dan

keaslian perangkat digital serta Bukti Elektronik potensial. Jika proses pemindahan Bukti Elektronik potensial tidak dilakukan oleh PPBE atau SBE, maka dianjurkan menerapkan enkripsi terhadap Bukti Elektronik potensial.

CATATAN PPBE harus memastikan bahwa pengkoleksian informasi yang sensitif atau pribadi sesuai peraturan perundang-undangan.

Selama pembungkusan dan pemindahan, PPBE harus menyadari kemungkinan adanya aliran listrik statis yang dapat merusak kekuatan pembuktian dari Bukti Elektronik potensial. PPBE harus memastikan bahwa komputer dan perangkat digital dibungkus dengan aman selama pemindahan untuk mencegah kerusakan dari guncangan dan getaran.

Proses pemindahan harus memungkinkan adanya suatu lingkungan yang kondusif dan terkendali. Tingkat kelembapan udara, kelembapan dan suhu harus sesuai untuk perangkat digital. Hindari menyimpan Bukti Elektronik potensial dan perangkat digital dalam kendaraan pengangkut untuk waktu yang lama dan hindari dari sinar UV.

Dalam kondisi PPBE atau SBE tidak dapat mengantarkan bukti, pemindahan bukti harus tetap memastikan keamanan dari Bukti Elektronik potensial serta menjaga keberlangsungan dari rantai pengawasan.

7 Contoh Identifikasi, Koleksi, Akuisisi Dan Preservasi

7.1 Komputer, Perangkat Periferal Dan Media Penyimpanan Digital

7.1.1 Identifikasi

7.1.1.1 Pencarian Dan Dokumentasi Lokasi Fisik Kejadian Perkara

Dalam konteks klausul ini, komputer dianggap sebagai perangkat digital independen (yang berdiri sendiri) yang menerima, mengolah dan menyimpan data, serta mengeluarkan hasil. Perangkat komputer ini tidak terhubung ke jaringan, tetapi dapat dihubungkan ke perangkat periferal seperti *printer*, *scanner*, *webcam,* pemutar MP3, sistem GPS, perangkat RFID dan sebagainya. Sebuah perangkat digital yang memiliki penghubung jaringan, tetapi tidak terhubung pada saat Koleksi atau Akuisisi, harus dianggap (untuk tujuan keseragaman) sebagai komputer independen. Jika komputer dengan penghubung jaringan, tetapi tidak ditemukan kejelasan apakah terdapat koneksi, diperlukan tindakan untuk mengidentifikasi kemana saja perangkat dikoneksikan di masa lalu yang paling akhir (*recent past*).

Biasanya tempat kejadian perkara akan berisi berbagai jenis media penyimpanan digital. Media penyimpanan digital digunakan untuk menyimpan data dari perangkat digital dan memiliki kapasitas memori yang berbeda. Contoh

media penyimpanan digital meliputi namun tidak terbatas pada *hard drive portable* eksternal*, flash drive*, CD, DVD, *disk Blu-ray*, disket, kaset magnetik dan kartu memori.

Sebelum Akuisisi atau Koleksi dapat dilakukan, aspek keselamatan atas Bukti Elektronik potensial harus dipertimbangkan. Aspek-aspek tersebut dijelaskan dalam klausul 6.2.1 dan 6.2.2. PPBE harus berhati-hati, untuk memastikan bahwa perangkat independen tidak baru saja terhubung pada jaringan. Jika diduga perangkat independen terlihat seolah baru saja diputuskan dari jaringan, PPBE harus memperlakukannya sebagai perangkat jaringan, untuk memastikan bahwa bagian-bagian lain dari jaringan ditangani dengan tepat. Paling sedikit PPBE harus memperhatikan dan melaksanakan hal berikut:

a. PPBE harus mendokumentasikan jenis dan merek perangkat digital yang digunakan dan mengidentifikasi semua komputer dan perangkat periferal yang perlu diakuisisi atau dikoleksi selama tahap awal ini. Nomor seri, nomor lisensi dan tanda identitas lainnya (termasuk kerusakan fisik) harus didokumentasikan sedapat mungkin.
b. Pada tahap Identifikasi, status komputer dan perangkat periferal harus tetap dalam keadaan awal (*as it is*). Jika komputer atau perangkat periferal dalam keadaan mati, tidak boleh dinyalakan. Jika komputer atau perangkat periferal dalam keadaan menyala, PPBE tidak boleh mematikannya karena dapat merusak Bukti Elektronik potensial.
c. Jika komputer dalam keadaan menyala, PPBE harus memotret atau membuat dokumen tertulis dari apa yang ditampilkan pada layar. Setiap dokumen tertulis harus mencakup deskripsi dari apa yang sebenarnya terlihat (misalnya perkiraan posisi tampilan layar, aplikasi yang sedang berjalan dan isi aplikasi tersebut).
d. Sebuah perangkat dengan baterai yang kemungkinkan akan kehabisan daya, harus diisi tenaganya untuk memastikan informasi tidak hilang. PPBE harus mengidentifikasi dan mengoleksi pengisi baterai dan kabel selama fase ini.
e. PPBE juga harus mempertimbangkan penggunaan detektor sinyal nirkabel untuk mendeteksi dan mengidentifikasi sinyal nirkabel dari perangkat nirkabel yang mungkin disembunyikan. Terdapat kemungkinan kasus di mana detektor sinyal nirkabel tidak digunakan karena kendala biaya dan waktu, dan PPBE harus mendokumentasikan hal tersebut. Jika terdapat perangkat jaringan yang ditemukan, PPBE harus melanjutkannya dengan proses penanganan bukti seperti yang dijelaskan

dalam dokumen ini pada klausul 7.2.2.2. Di mana proses pemindaian aktif (yaitu penyiaran dan/atau penggalian) untuk perangkat jaringan akan digunakan, perangkat pemindaian harus dimatikan setelah penilaian karena dimungkinkan terjadinya interaksi antara perangkat tersebut dengan perangkat lain di tempat kejadian perkara. Anggota tim harus ingat bahwa perangkat tertentu di tempat kejadian perkara dapat mendeteksi keberadaan perangkat pemindaian aktif dan penggunaan pemindaian aktif dapat memicu tindakan yang dapat merusak Bukti Elektronik potensial, dan, dalam keadaan ekstrim, dapat mengaktivasi perangkap tersembunyi.

CATATAN 1 Jika terdapat banyak perangkat digital di tempat kejadian perkara, PPBE harus mempertimbangkan urgensi untuk menyalakan perangkat digital yang dibutuhkan dalam menentukan relevansi perangkat dengan investigasi. Hal ini dilakukan dengan memperhitungkan waktu proses dan biaya yang akan dikeluarkan jika perangkat digital yang tidak relevan diakuisisi. Jika perangkat dinyalakan untuk evaluasi di tempat kejadian perkara, PPBE harus memastikan bahwa seluruh tindakan yang dilakukan tercatat.

CATAAN 2 Pertimbangan untuk mempertahankan perangkat digital dalam keadaan menyala atau tidak ditentukan kepada tingkat prioritas volatil dan relevansi. Jika PPBE memutuskan bahwa informasi yang paling kritikal adalah informasi non-volatil di dalam *disk*, maka pada sistem yang sedang beroperasi, layar konsolnya difoto dan steker listriknya dilepaskan. Jika informasi yang relevan ada di dalam memori (bukti volatil), maka sangat penting untuk membiarkan sistem dalam keadaan menyala untuk pelaksanaan Akuisisi.

7.1.1.2 Koleksi Bukti Non-Digital

PPBE harus mempertimbangkan proses Koleksi bukti non-digital. Untuk melaksanakannya, ketua tim harus mengidentifikasi individu yang bertanggung jawab atas fasilitas di tempat kejadian perkara. Individu tersebut kemungkinan dapat memberikan informasi dan dokumentasi tambahan seperti *password* perangkat digital dan rincian lain yang relevan. PPBE harus mendokumentasikan nama dan tugas individu tersebut.

Kemungkinan PPBE juga harus mengumpulkan beberapa bukti dengan wawancara kepada individu yang memiliki informasi yang berguna atau relevan tentang Bukti Elektronik potensial atau perangkat digital yang akan dikoleksi. Setiap tanggapan harus didokumentasikan secara akurat. Individu yang dimaksud dapat meliputi administrator sistem, pemilik perangkat dan pengguna komputer dan perangkat periferal. Selama pengumpulan bukti lisan ini, PPBE

dapat meminta informasi seperti konfigurasi sistem dan *password* administrator/*root*. Informasi tambahan tersebut dapat bermanfaat dalam tahap analisis Bukti Elektronik potensial. Wawancara tersebut harus didokumentasikan untuk memastikan rinciannya akurat dan pernyataan yang didokumentasikan tidak dapat diubah. Dalam melakukan pengumpulan bukti non-digital PPBE harus memperhatikan ketentuan peraturan perundang-undangan.

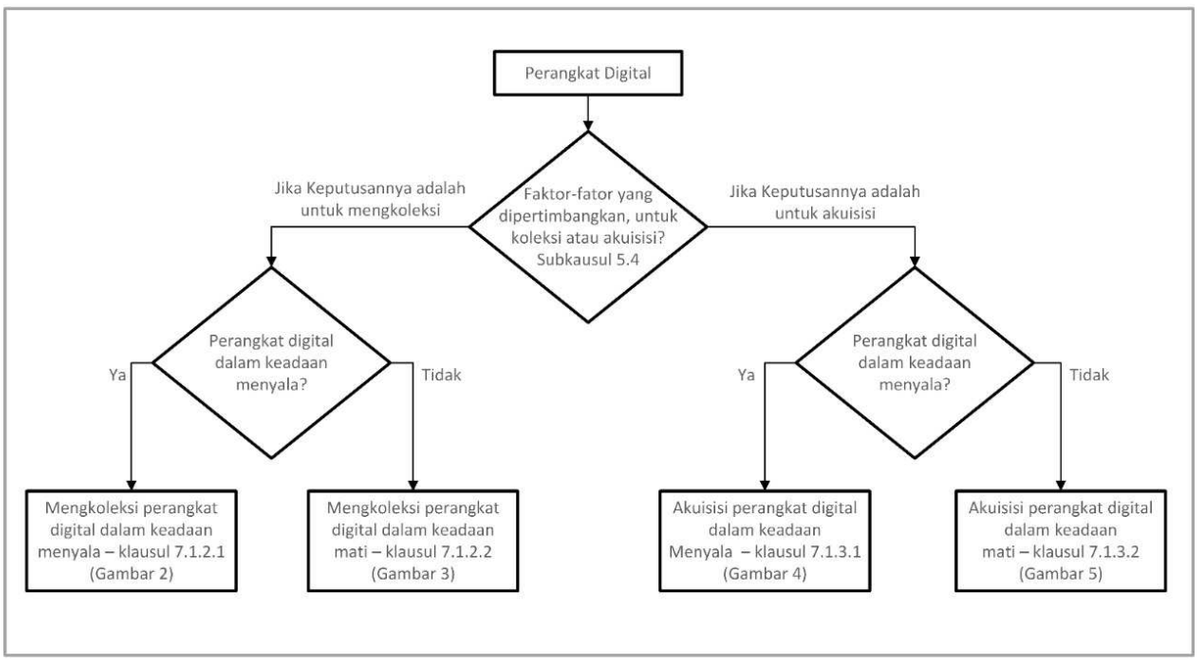
7.1.1.3 Proses Pengambilan Keputusan Untuk Koleksi Atau Akuisisi

Dalam proses pengambilan keputusan untuk mengoleksi perangkat digital atau mengakuisisi Bukti Elektronik potensial, paling sedikit harus mempertimbangkan faktor ~~hal~~ berikut:

a. Tingkat volatilitas Bukti Elektronik potensial yang dibahas dalam klausul 5.4.2 dan 6.8;
b. *Disk* yang di enkripsi seluruhnya atau sebagian di mana kata sandi atau kunci mungkin berada sebagai data volatil~~e~~ di RAM, pada token eksternal, *smart card*, perangkat atau media lain;
c. Kekritisan dari sistem yang dibahas dalam klausul 5.4.4, 7.2.1.2 dan 7.1.3.4;
d. Peraturan perundang-undangan; dan
e. Sumber daya seperti ukuran penyimpanan yang diperlukan, ketersediaan personel, dan batasan waktu.

Gambar 1 menjelaskan gambaran proses pengambilan keputusan untuk melakukan Koleksi atau Akuisisi.

Gambar 1 - Panduan untuk pengambilan keputusan apakah mengoleksi atau mengakuisisi Bukti Elektronik potensial



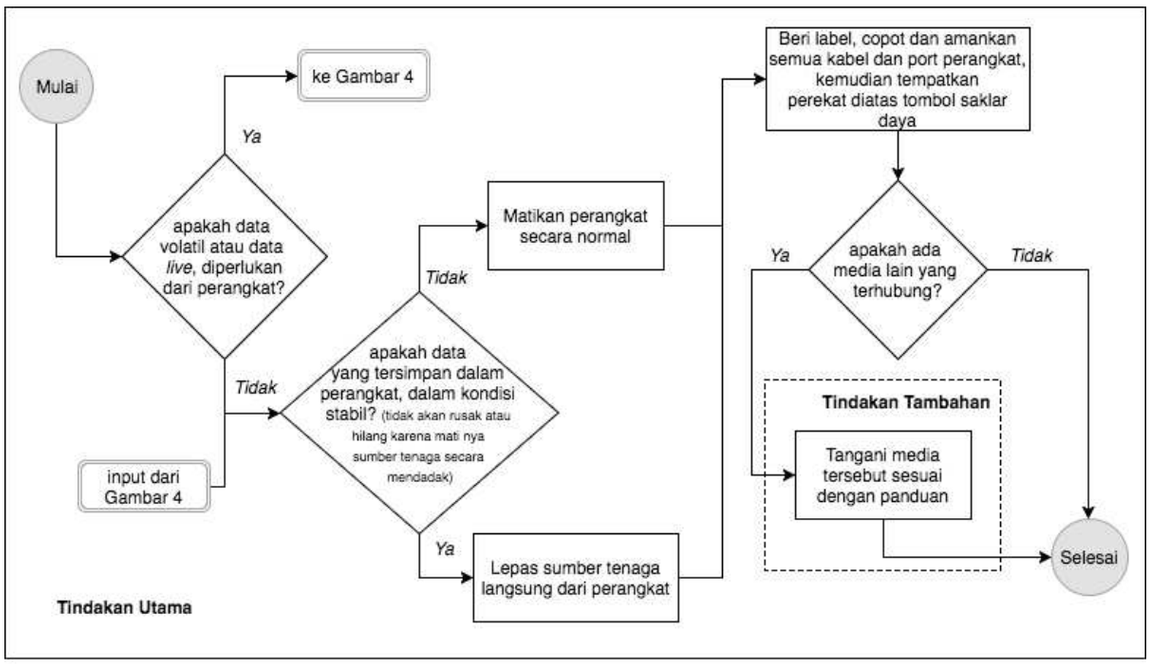
7.1.2 Koleksi

7.1.2.1 Perangkat Digital Dalam Keadaan Menyala

7.1.2.1.1 Ikhtisar

PPBE dapat mengikuti sejumlah pedoman Koleksi apabila perangkat digital dalam keadaan menyala. Tidak semua pedoman tersebut ideal dan tepat untuk setiap kasus; beberapa pedoman hanya relevan untuk kasus-kasus tertentu. Karenanya, pedoman dapat dikategorikan menjadi tindakan utama dan tindakan tambahan. Tindakan utama harus diterapkan dalam segala situasi, sementara tindakan tambahan harus diterapkan ketika relevan dan memungkinkan untuk diterapkan, tergantung pada perangkat atau keadaan khusus. Gambar 2 menjelaskan tindakan utama dan tindakan tambahan yang berlaku untuk mengoleksi perangkat digital dalam keadaan menyala.

DRAFTDRAFTDRAFT



Gambar 2 - Panduan untuk Koleksi perangkat digital dalam keadaan menyala

Menjadi tanggung jawab PPBE untuk mengetahui teknologi terkini dan terbiasa melakukan penanganan media penyimpanan.

7.1.2.1.2 Tindakan Utama: *Koleksi* Perangkat Digital Dalam Keadaan Menyala.

Tindakan utama berikut harus diikuti oleh PPBE dalam semua kasus yang melibatkan Bukti Elektronik potensial. Pedoman ini berlaku ketika PPBE telah memutuskan bahwa sebuah perangkat digital yang dalam keadaan menyala harus dikoleksi:

a. Mempertimbangkan untuk mengakuisisi data volatil perangkat digital dan kondisi saat sistem sebelum dimatikan. Kunci enkripsi dan data krusial lainnya mungkin berada dalam memori aktif, atau dalam memori tidak aktif yang belum terhapus. Pertimbangkan Akuisisi logis ketika terdapat dugaan enkripsi. Dalam hal dilakukan akuisisi logis harus diingat bahwa sistem operasi komputer yang sedang menyala kemungkinan tidak dapat dipercaya, sehingga harus mempertimbangkan penggunaan peralatan yang terpercaya dan tervalidasi.
b. Konfigurasi perangkat digital dapat menentukan apakah PPBE harus mematikan perangkat melalui prosedur administratif normal, atau dengan menarik steker dari soket listrik. PPBE harus berkonsultasi dengan SBE untuk menentukan pendekatan terbaik berdasarkan kondisi tertentu. Jika keputusan yang dibuat adalah menarik steker, PPBE harus melepaskan kabel sumber daya dengan terlebih dahulu melepaskan ujung

yang terpasang ke perangkat digital dan bukan ujung yang melekat pada soket. Harus dipahami bahwa perangkat yang terhubung ke UPS dapat terubah datanya jika kabel listrik dilepaskan dari soket dan bukan dari perangkat.

CATATAN 1 Jika daya dilepaskan dari perangkat digital yang dalam keadaan menyala, Bukti Elektronik potensial yang tersimpan dalam volume terenkripsi tidak akan dapat diakses, kecuali kunci deskripsi diperoleh. Data *realtime* yang berpotensi memiliki nilai juga dapat hilang, dapat berujung pada gugatan kerusakan atau hilangnya nyawa manusia, seperti data perusahaan atau perangkat digital yang mengendalikan peralatan medis. Dengan demikian, PPBE harus memastikan bahwa data volatil telah dikoleksi sebelum melepas sumber daya.

CATATAN 2 Terdapat perangkat keras yang memungkinkan perangkat digital dalam keadaan menyala terputus dari listrik dan dipindahkan ke UPS *portable* tanpa mengganggu aliran daya ke perangkat. Terdapat juga *mouse-jigglers* yang dapat digunakan untuk mencegah pengaktifan *screensaver*. Kedua perangkat tersebut berguna saat berhadapan dengan perangkat digital dalam keadaan menyala yang di mana enkripsi kemungkinan sedang aktif. Ketika perangkat digital dalam keadaan menyala dikoleksi, ketersediaan daya harus dipertahankan, pembungkusan dan pemindahan sistem yang sedang berjalan harus memperhatikan permasalahan terkait dengan ketersediaan pendingin, perlindungan dari guncangan mekanik, dll.

c. Memberi label, melepaskan dan mengamankan semua kabel dari perangkat digital serta melabeli *port* sehingga sistem dapat direkonstruksikan kembali pada tahap berikutnya.
d. Jika diperlukan tempatkan segel di atas sakelar daya untuk mencegah perubahan kondisi sakelar. Perhatikan dengan saksama apakah keadaan sakelar telah didokumentasikan sebelum perekaman atau pemindahan.

7.1.2.1.3 Kegiatan Tambahan: Koleksi Perangkat Digital Dalam Keadaan Menyala

Berikut adalah kegiatan tambahan yang relevan bergantung pada konfigurasi perangkat digital tertentu.

a. Jika perangkat adalah komputer *notebook,* pastikan data volatil diakuisisi sebelum mengeluarkan baterai. PPBE harus melepaskan baterai sumber daya utama terlebih dahulu, dibandingkan menekan tombol daya komputer *notebook* untuk mematikannya. PPBE juga harus memperhatikan jika adaptor daya tersedia, dan jika ada, lepaskan adaptor daya setelah baterai dilepaskan.

   CATATAN 1 Tindakan menekan tombol daya perangkat digital dapat saja dikonfigurasi untuk menjalankan sebuah kode program yang dapat mengubah informasi atau menghapus informasi dari sistem sebelum mati atau untuk memperingatkan sistem-sistem terhubung bahwa terjadi peristiwa tidak terduga sehingga sistem tersebut menghapus data yang berkekuatan pembuktian sebelum teridentifikasi. Dapat juga dikonfigurasi untuk memicu sebuah perangkat yang ditujukan untuk menimbulkan bahaya fisik pada PPBE dan individu lain yang hadir.

b. Menempatkan segel di atas slot *floppy disk*, jika tersedia.
c. Memastikan bahwa pemutar CD atau DVD dimasukkan kembali pada tempatnya; perhatikan apakah pemutar kosong, berisi *disk*, atau tidak dapat diketahui; dan tempelkan segel pada slot *drive* tertutup untuk mencegahnya terbuka.

CATATAN 2 Jika terdapat media *bootable* yang terpasang yang kemudian ketika mesin dinyalakan ada kemungkinan di *boot* dari media tersebut, bukan dari *hard drive* (atau *flash drive* alat forensik). Hal ini bergantung pada pengaturan komputer BIOS.

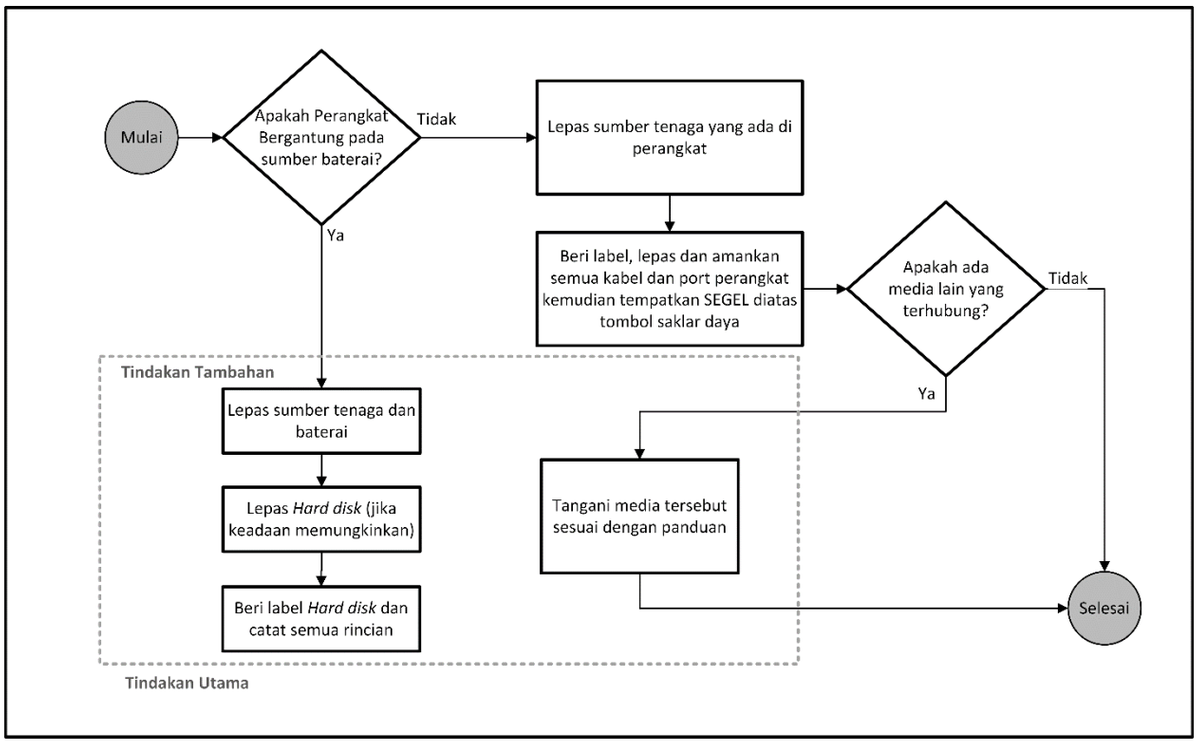
PPBE harus melakukan Koleksi bukti non-digital sesuai dengan peraturan perundang-undangan untuk memastikan bahwa bukti dapat diterima.

7.1.2.2 Perangkat Digital Dalam Keadaan Mati

7.1.2.2.1 Ikhtisar

PPBE dapat mengikuti sejumlah pedoman Koleksi Bukti Elektronik dalam kondisi mati. Tidak semua kegiatan yang terdapat dalam panduan ini relevan dalam segala situasi. Dengan demikian harus dibedakan antara tindakan-tindakan yang berlaku di semua kasus (tindakan utama) dan yang hanya berlaku dalam kasus tertentu (tindakan tambahan). Gambar 3 menggambarkan

tindakan utama dan tindakan tambahan yang berlaku untuk Koleksi perangkat digital dalam kondisi mati.



Gambar 3 - Panduan Untuk Koleksi Perangkat Digital Dalam Keadaan Mati

Menjadi tanggung jawab PPBE untuk mengetahui teknologi terkini dan terbiasa dengan pedoman penanganan media penyimpanan.

7.1.2.2.2 Tindakan Utama: Koleksi Perangkat Digital Dalam Kondisi Mati

Berikut adalah tindakan utama yang direkomendasikan untuk Koleksi perangkat digital dalam kondisi mati:

a. Lepaskan kabel sumber daya dengan terlebih dahulu melepaskan ujung yang terpasang ke perangkat digital dan bukan ujung yang melekat pada soket;
b. Cabut dan amankan semua kabel dari perangkat digital dan beri label pada *port* sehingga sistem dapat direkonstruksi pada tahap berikutnya; dan
c. Tempatkan segel di atas sakelar daya jika diperlukan untuk mencegah perubahan kondisi sakelar. Pertimbangkan apakah keadaan sakelar telah didokumentasikan secara memadai sebelum diberi segel atau dipindahkan.

CATATAN Dalam kebanyakan kasus, media penyimpanan tidak boleh dilepaskan dari perangkat digital hingga saat akan diakuisisi, karena dengan

melepaskannya dapat meningkatkan risiko rusak atau tertukar dengan media penyimpanan lain. SOP teknis penanganan media penyimpanan harus ada dan diikuti.

7.1.2.2.3 Kegiatan Tambahan: Koleksi Perangkat Digital Dalam Keadaan Mati

Berikut adalah kegiatan tambahan yang relevan dengan Koleksi perangkat digital dalam keadaan mati, bergantung pada konfigurasi perangkat digital yang spesifik:

a. Pertama, pastikan bahwa komputer *notebook* benar-benar dalam keadaan mati karena beberapa perangkat kemungkinan hanya dalam mode *standby*. Waspada terhadap beberapa komputer *notebook* yang dapat dinyalakan dengan membuka tutupnya. Selanjutnya lepaskan baterai sumber daya utama dari komputer *notebook*.
b. Jika kondisi lapangan memaksa *hard drive* untuk dilepaskan, PPBE harus berhati-hati terhadap *ground* listrik perangkat digital untuk mencegah listrik statis merusak *hard drive*. Jika tidak ada kondisi memaksa, *hard drive* tidak boleh dilepaskan di lapangan. Beri label pada *hard drive* tersebut sebagai *disk* tersangka dan dokumentasikan semua rincian seperti pembuat, nama model, nomor seri dan ukuran *hard drive*.
c. Tempatkan segel di atas slot *floppy disk*, jika tersedia.
d. Pastikan bahwa penggerak CD atau DVD *drive* dimasukkan kembali pada tempatnya; perhatikan apakah penggerak *drive* kosong, berisi *disk*, atau tidak terperiksa; dan tempelkan segel pada slot *drive* tertutup untuk mencegahnya terbuka.

CATATAN Jika terdapat media *bootable* dibiarkan terhubung pada komputer *notebook* yang kemudian komputer *notebook* tersebut dinyalakan, proses *booting* dapat berasal dari media *bootable* tersebut dibanding dari *hard drive* (atau *flash drive* alat forensik) bergantung pada pengaturan komputer BIOS.

7.1.3 Akuisisi

7.1.3.1 Perangkat Digital Dalam Keadaan Menyala

7.1.3.1.1 Ikhtisar

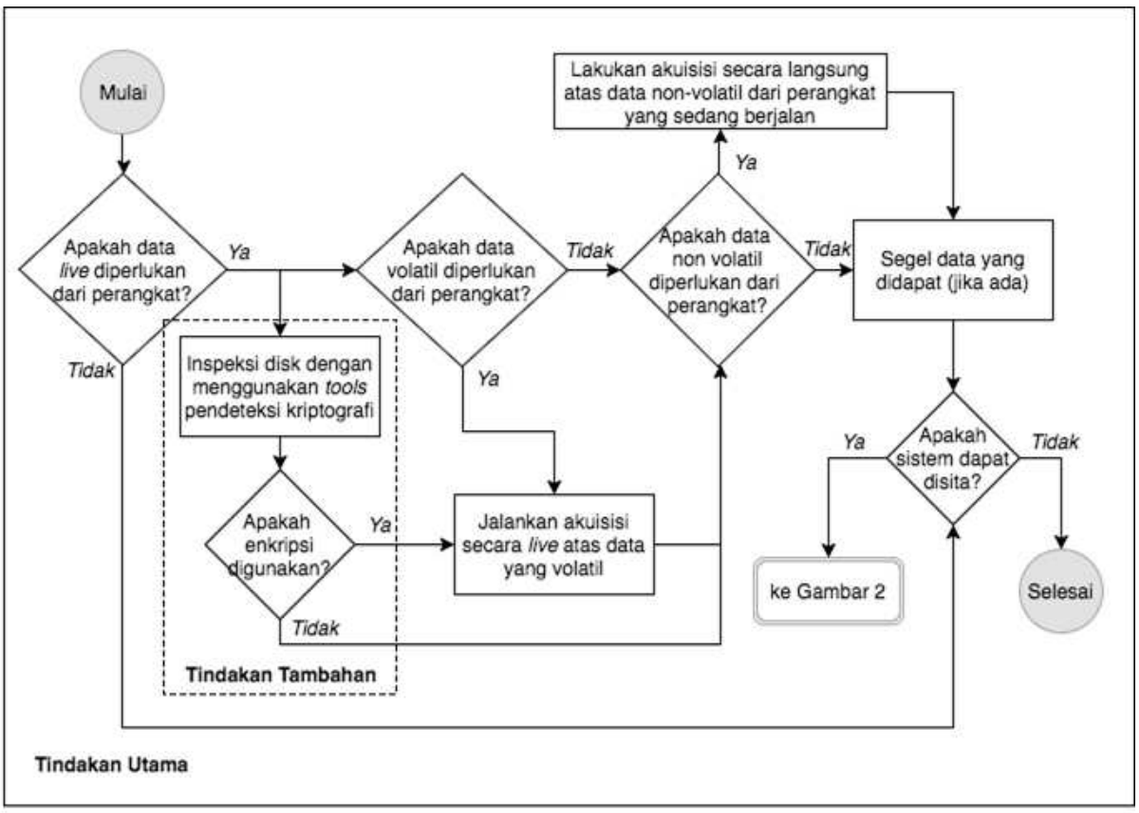
Terdapat tiga skenario di mana Akuisisi perlu dilakukan: ketika perangkat digital dalam keadaan menyala, ketika perangkat digital dalam keadaan mati dan ketika perangkat digital dalam keadaan menyala tetapi tidak dapat dimatikan (seperti perangkat digital *mission-critical*). Dalam semua skenario ini, PPBE diwajibkan untuk membuat salinan Bukti Elektronik yang akurat dari media

penyimpanan perangkat digital yang diduga mengandung Bukti Elektronik potensial.

Jika salinan utuh (*image*) tidak dapat diperoleh, salinan akurat dari *file* tertentu yang diduga mengandung Bukti Elektronik potensial dapat dilakukan. Idealnya, baik salinan master maupun salinan kerja (*working copy*) lain yang terverifikasi harus dihasilkan. Salinan master tidak boleh digunakan kembali kecuali diperlukan untuk melakukan verifikasi isi dari salinan kerja lain atau untuk menghasilkan pengganti salinan kerja menyusul terjadinya kerusakan pada salinan kerja pertama.

PPBE dapat mengikuti sejumlah pedoman Akuisisi apabila perangkat digital bukti ditemukan dalam keadaan menyala. Tidak setiap pedoman ideal dan tepat untuk semua kasus; beberapa pedoman hanya relevan untuk kasus-kasus tertentu. Oleh karena itu, tindakan dapat dikategorikan menjadi tindakan utama atau tindakan tambahan. Perhatian harus diberikan terhadap kemungkinan bahwa sistem dalam keadaan menyala dapat masuk ke dalam mode *screensaver* atau kunci otomatis dan harus diperhatikan kemungkinan adanya perubahan ketika melakukan usaha untuk mencegah terjadinya *screensaver* atau kunci otomatis. Sebagai contoh, penggunaan perangkat lunak *mouse-jiggler* akan mengakibatkan *entry key* USB ke dalam *registry* dan kemungkinan besar akan terjadi modifikasi terhadap langkah apapun yang dilakukan. Menggunakan metode yang andal akan meminimalkan implikasi dari tindakan yang dilakukan. Gambar 4 menggambarkan tindakan utama dan tindakan tambahan yang dilakukan pada saat Akuisisi perangkat digital dalam keadaan menyala.

DRAFT DRAFT DRAF



Gambar 4 - Panduan Untuk Akuisisi Perangkat Digital Dalam Keadaan Menyala

7.1.3.1.2 Tindakan Utama: *Akuisisi* Perangkat Digital Dalam Keadaan Menyala

Berikut adalah tindakan utama yang harus diikuti oleh PPBE dalam semua kasus yang melibatkan Akuisisi Bukti Elektronik potensial pada perangkat digital dalam keadaan menyala:

a. Pertama, pertimbangkan Akuisisi Bukti Elektronik potensial yang mungkin akan hilang jika perangkat digital dimatikan. Hal ini dikenal sebagai data volatil contohnya data yang tersimpan pada RAM, proses yang sedang berjalan, koneksi jaringan dan pengaturan tanggal atau waktu. Dalam keadaan di mana diperlukan untuk mengakuisisi data non-volatil dari perangkat yang sedang berjalan, harus dipertimbangkan melakukan Akuisisi pada sistem dalam keadaan menyala.

b. Melakukan Akuisisi langsung (*live acquisition*) dibutuhkan untuk memperoleh *live data* dari perangkat yang sedang berjalan. Akuisisi langsung pada data volatil di RAM memungkinkan pemulihan informasi berharga seperti status jaringan, aplikasi terdeskripsi dan kata kunci. Akuisisi langsung dapat dilakukan pada konsol atau dari jarak jauh melalui

jaringan. Prosesnya berbeda, dan membutuhkan penggunaan rangkaian perangkat yang berbeda.

c. PPBE tidak boleh mempercayai program pada sistem. Untuk alasan tersebut, sepanjang memungkinkan, direkomendasikan agar PPBE memakai peralatan terpercaya (binari statis) yang dimiliki. PPBE harus berkompeten untuk menggunakan alat tervalidasi dan berkompeten untuk memperhitungkan efek penggunaan alat tersebut pada sistem (misalnya berpindahnya Bukti Elektronik potensial, isi dari memori yang berjalan ketika perangkat lunak dijalankan dll). Semua tindakan yang dilakukan dan perubahan yang dihasilkan pada Bukti Elektronik potensial harus didokumentasikan dan dipahami. Jika efek yang mungkin terjadi tidak dapat dipastikan dengan dimasukkannya alat ke dalam sistem atau perubahan yang dihasilkan tidak dapat ditentukan dengan pasti, hal ini juga harus didokumentasikan.
d. Ketika mengakuisisi data volatil, jika dimungkinkan PPBE harus menerapkan penggunaan wadah *file* logis (*logical file container*) dan mendokumentasikan nilai *hash*-nya segera setelah wadah tersebut berisi *file* data volatil. Ketika hal tersebut tidak dimungkinkan, wadah seperti *file* ZIP harus digunakan dan kemudian *file* ini harus di-*hash* dan didokumentasikan nilainya. Wadah *file* yang dihasilkan harus disimpan pada media penyimpanan digital yang telah dipersiapkan (diformat) untuk tujuan ini.
e. Jalankan proses penyalinan (*imaging*) pada media penyimpanan non-volatil yang sedang berjalan (*live*) dengan menggunakan perangkat penyalinan yang tervalidasi. Salinan Bukti Elektronik yang dihasilkan harus disimpan pada media penyimpanan digital yang telah dipersiapkan untuk tujuan ini. Lebih diutamakan untuk menggunakan media penyimpanan digital baru, penggunaan salinan Bukti Elektronik dari proses yang tervalidasi memastikan integritas data ketika direkonstruksi. Oleh karena itu, media penyimpanan digital yang telah disanitasi dapat memenuhi ketentuan integritas data. Jika salinan utuh (*image*) harus disimpan dalam wadah *file* logis, PPBE harus memastikan salinan utuh tidak dapat berubah atau rusak.

CATATAN Dalam situasi ketika perangkat terkunci, akses fisik dapat dilakukan melalui cara mengakses memori secara langsung, misalnya *Firewire Interface*.

7.1.3.1.3 Kegiatan Tambahan: Akuisisi Perangkat Digital Dalam Keadaan Menyala.

Berikut adalah kegiatan tambahan yang relevan pada Akuisisi perangkat digital dalam keadaan menyala, tergantung pada konfigurasi perangkat digital yang spesifik:

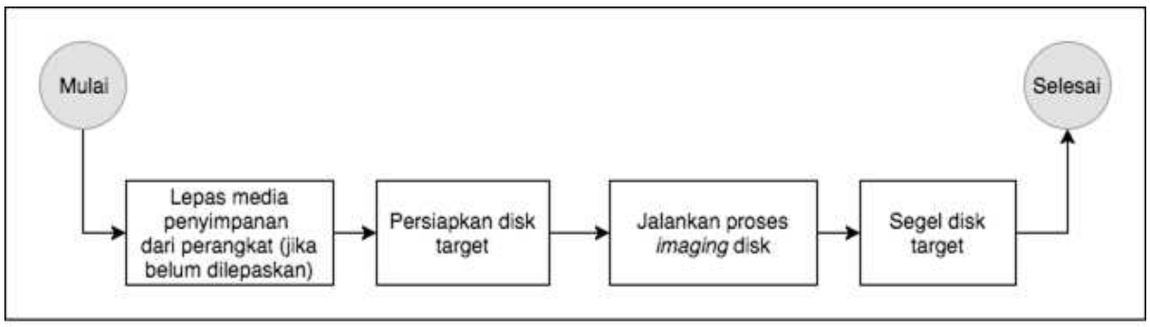
a. Pertimbangkan Akuisisi data volatil dalam RAM ketika diduga adanya penggunaan enkripsi. Pertama-tama cek kemungkinan penggunaan enkripsi dengan memeriksa *raw disk* atau menggunakan perangkat pendeteksi kripto. Jika terdapat enkripsi, perlu diingat bahwa sistem operasi komputer yang dalam keadaan menyala mungkin tidak dapat dipercaya dan pertimbangkan penggunaan alat-alat sesuai yang terpercaya dan tervalidasi;
b. Menggunakan acuan waktu yang terpercaya dan dokumentasikan waktu pada setiap tindakan yang dilakukan; dan
c. Sepatutnya untuk mengasosiasikan PPBE dengan Bukti Elektronik potensial yang diakuisisinya, dengan menggunakan tanda tangan digital, biometrik dan fotografi.

CATATAN Tindakan menekan tombol daya perangkat digital dapat dikonfigurasi untuk menjalankan sebuah *script* yang dapat mengubah informasi dan/atau menghapus informasi dari sistem sebelum mati atau untuk memperingatkan sistem-sistem terhubung bahwa terjadi peristiwa tidak terduga sehingga sistem tersebut menghapus data yang memiliki kekuatan pembuktian sebelum diidentifikasi. Dapat juga dikonfigurasi untuk memicu sebuah perangkat yang ditujukan untuk menimbulkan bahaya fisik pada PPBE dan individu lain yang hadir.

7.1.3.2 Perangkat Digital Dalam Keadaan Mati

7.1.3.2.1 Ikhtisar

Lebih mudah menangani perangkat digital dalam keadaan mati dibandingkan dengan perangkat digital dalam keadaan menyala karena tidak ada kebutuhan untuk mengakuisisi data volatil. Gambar 5 menggambarkan kegiatan yang dilakukan untuk Akuisisi perangkat digital dalam keadaan mati.



Gambar 5 - Panduan Untuk Akuisisi Perangkat Digital Dalam Keadaan Mati

7.1.3.2.2 Akuisisi Perangkat Digital Dalam Keadaan Mati

Berikut adalah kegiatan untuk melakukan Akuisisi ketika perangkat digital yang ditemukan dalam keadaan mati:

a. Pastikan perangkat tersebut benar-benar dalam keadaan mati;
b. Jika dinilai tepat, lepaskan media penyimpan dari perangkat digital yang dalam keadaan mati apabila belum dilepaskan. Beri label pada media penyimpanan tersebut sebagai media penyimpanan tersangka dan dokumentasikan semua rincian seperti pembuat, nama model, nomor seri dan ukuran penyimpanan; dan
c. Menjalankan proses penyalinan dengan menggunakan alat penyalinan yang tervalidasi untuk menghasilkan salinan Bukti Elektronik dari disk tersangka.

CATATAN Dalam kebanyakan kasus, media penyimpanan tidak boleh dilepas dari perangkat digital hingga dilakukan akuisisi karena melepaskannya dapat meningkatkan risiko rusak atau tertukar dengan media penyimpanan lainnya. SOP harus ada dan diikuti pada masing-masing instansi terkait kebutuhan pelepasan *hard disk*.

7.1.3.3 Perangkat Digital *mission-critical*

Dalam beberapa kasus, perangkat digital tidak dapat dimatikan karena merupakan sistem kritis. Contoh dari sistem ini ialah server di pusat data yang dapat juga melayani klien yang tidak terkait dengan perkara, sistem pengawasan, sistem medis dan sistem lainnya yang dapat sangat terpengaruh jika sistem terganggu atau dimatikan. Perhatian khusus harus dilakukan ketika berhadapan dengan sistem tersebut.

Bila perangkat digital tidak dapat dimatikan, maka dilakukan *live forensic* dan/atau Akuisisi parsial, seperti yang dibahas dalam klausul 7.1.3.1.2 dan 7.1.3.4.

7.1.3.4 Akuisisi Parsial

Akuisisi parsial dapat dilakukan karena beberapa alasan, seperti:

a. Sistem penyimpanan terlalu besar untuk diakuisisi (misalnya server *database*);
b. Sistem terlalu kritis untuk dimatikan;
c. Data yang akan diakuisisi mengandung data lain yang tidak relevan dan berada di dalam sistem yang sama; atau
d. Ketika dibatasi oleh otoritas hukum seperti surat perintah penggeledahan yang membatasi ruang lingkup Akuisisi.

Ketika keputusan telah dibuat untuk melakukan Akuisisi parsial, kegiatan Akuisisi harus meliputi namun tidak terbatas pada hal berikut:

a. Identifikasi Folder, file atau sistem *proprietary* lainnya yang tersedia untuk mendapatkan data yang diinginkan; dan
b. melakukan *Logical acquisition* pada data yang teridentifikasi tersebut.

7.1.3.5 Media Penyimpanan Digital

Berbagai jenis media penyimpanan digital dapat ditemukan di tempat kejadian perkara. Biasanya media-media ini memiliki data bertipe non-volatil dan dapat menjadi prioritas terendah selama Koleksi dan Akuisisi. Bukan berarti mereka tidak penting, karena dalam banyak kasus, media penyimpanan digital eksternal berisi bukti yang dicari oleh analis. PPBE harus memastikan hal berikut:

a. Memeriksa dan mendokumentasikan lokasi (misalnya tempat *drive*, kabel dan konektor, slot USB, dll), produsen, model dan nomor seri (jika ada) dari setiap media penyimpanan digital yang ditemukan;
b. Menentukan pilihan untuk mengoleksi media penyimpanan digital yang teridentifikasi atau melakukan Akuisisi di tempat kejadian perkara. Keputusan harus didasarkan pada sifat insiden dan ketersediaan sumber daya. Untuk melakukan Akuisisi media penyimpanan digital (terutama *hard disk*) di tempat kejadian perkara, lihat Gambar 4;
c. Jika PPBE memutuskan untuk mengoleksi media penyimpanan digital dan hal tersebut diperbolehkan, media yang dikoleksi harus dibungkus atau ditempatkan dalam pembungkus yang memadai;
d. Memberi label semua media penyimpanan digital dan setiap bagian yang terkait dengannya. Label bukti tidak boleh ditempatkan langsung di bagian yang bergerak pada media digital, atau menutup sehingga menyembunyikan informasi penting seperti nomor seri, nomor model dan nomor bagian. Seluruh media yang dikoleksi harus diakuisisi dan disimpan dengan cara tertentu untuk memastikan integritas media yang

dikoleksi. Bila memungkinkan bukti harus disegel dengan segel yang jelas terlihat jika diubah. PPBE atau penanggung jawab harus menandatangani label tersebut;

e. Media penyimpanan digital yang dikoleksi harus disimpan dalam lingkungan yang sesuai untuk Preservasi data; dan
f. Media penyimpanan digital yang berbeda memiliki kemampuan data retensi yang berbeda. PPBE harus paham jangka waktu maksimum yang dapat diterima sesuai dengan yang telah ditentukan oleh peraturan perundang-undangan yang relevan, yang berkaitan dengan kemampuan data retensi media penyimpanan digital.

7.1.4 Preservasi

Setelah proses Akuisisi selesai, PPBE harus menyegel data yang diakuisisi dengan menggunakan fungsi verifikasi atau tanda tangan digital untuk menentukan bahwa salinan Bukti Elektronik sama dengan aslinya. Sebagai tambahan, aspek keamanan membutuhkan kontrol yang menerapkan prinsip-prinsip menjaga kerahasiaan, integritas dan ketersediaan Bukti Elektronik potensial. Untuk melindungi terhadap perusakan, aspek lingkungan harus ditangani dengan tindakan yang sesuai. PPBE harus memastikan hal berikut:

a. Menggunakan fungsi verifikasi yang tepat untuk membuktikan bahwa *file* yang disalin sama dengan aslinya; dan
b. Mengasosiasikan PPBE dengan Bukti Elektronik potensial yang diakuisisinya, menggunakan tanda tangan digital atau biometrik, dan fotografi.

Semua perangkat digital yang dikoleksi harus dipreservasi dengan tepat. Perangkat digital dengan jenis yang berbeda memerlukan metode Preservasi yang berbeda. Bukti Elektronik potensial harus dipreservasi sepanjang umur Bukti Elektronik, sesuai dengan ketentuan peraturan perundang-undangan.

CATATAN Sebagai alternatif untuk menyegel data yang diakuisisi dengan fungsi verifikasi atau tanda tangan digital, PPBE juga dapat menggunakan fitur biometrik. Biometrik adalah metode pengenalan yang menggunakan karakteristik fisik dan perilaku untuk menentukan identitas individu. Dengan melampirkan fitur biometrik pada bukti yang diakuisisi, dapat dipastikan bahwa bukti tidak dapat dirusak tanpa mengubah fitur biometrik.

7.2 Perangkat Jaringan

7.2.1 Identifikasi

7.2.1.1 Ikhtisar

Dalam konteks klausul ini, perangkat jaringan dianggap sebagai komputer atau perangkat digital lain yang terhubung ke sebuah jaringan baik melalui kabel atau nirkabel. Perangkat jaringan ini dapat meliputi *mainframe*, server, komputer *desktop*, *access point*, *switch*, *hub*, *router,* perangkat *mobile*, PDA, PED, perangkat *Bluetooth*, sistem CCTV dan masih banyak lagi. Perhatikan jika perangkat digital merupakan perangkat jaringan, sulit untuk memastikan lokasi Bukti Elektronik potensial disimpan. Data bisa berada di manapun dalam jaringan.

Identifikasi perangkat digital termasuk komponen-komponen seperti logo manufaktur, nomor seri, *docking station* dan catu daya. PPBE dapat mempertimbangkan aspek-aspek berikut sebagai cara untuk mengidentifikasi:

a. Karakteristik perangkat: Produsen perangkat digital terkadang dapat diidentifikasi melalui karakteristik yang dapat diamati, terutama jika terdapat elemen desain yang unik.
b. Antarmuka Perangkat: Konektor daya seringkali merujuk pada produsen tertentu dan merupakan petunjuk yang dapat diandalkan untuk Identifikasi.
c. Label perangkat: Untuk perangkat *mobile* dalam keadaan mati, informasi yang diperoleh dari dalam tempat baterai dapat terlihat, terutama ketika digabungkan dengan *database* yang sesuai. Sebagai contoh, IMEI adalah 15-nomor digit yang menunjukkan produsen, tipe model, dan negara yang menyetujui perangkat GSM; ESN adalah penanda unik 32-bit yang didokumentasikan dengan aman didalam chip ponsel oleh produsen. 8-14bit pertama mengidentifikasikan produsen dan bit sisanya mengidentifikasikan nomor seri yang ditetapkan.
d. *Reverse lookup*: Jika nomor telepon dari ponsel diketahui, *reverse lookup* dapat digunakan untuk mengidentifikasi operator jaringan.

Karena perangkat *mobile* umumnya berukuran kecil, PPBE harus lebih teliti untuk mengidentifikasi semua jenis perangkat *mobile* yang mungkin relevan terhadap kasus. PPBE harus mengamankan tempat kejadian perkara yang diduga dan memastikan bahwa tidak ada individu yang memindahkan perangkat *mobile* atau perangkat digital lainnya dari tempat kejadian perkara. Perangkat digital yang mungkin mengandung Bukti Elektronik harus dilindungi dari pihak yang tidak berwenang.

CATATAN Dalam beberapa kasus, jaringan komunikasi tidak boleh terganggu. Beritahukan pihak yang berwenang tentang kemungkinan adanya masalah yang dapat terjadi (misalnya jangan memberitahukan sembarang pihak terkait penonaktifan perangkat).

7.2.1.2 Pencarian Dan Dokumentasi Tempat Kejadian Perkara

Sebelum Akuisisi atau Koleksi dapat dilakukan, tempat kejadian perkara harus didokumentasikan secara visual baik dengan foto, video atau sketsa seperti yang terlihat saat pertama kali masuk. Pemilihan metode dokumentasi harus memperhitungkan keadaan, biaya, waktu, ketersediaan sumber daya dan prioritas. PPBE harus mendokumentasikan semua barang lainnya di tempat kejadian perkara yang berpotensi relevan terhadap perkara seperti catatan/coretan, *sticky notes* buku harian, dll.

a. Selama tahap awal ini, PPBE harus mendokumentasikan jenis, merek, model dan nomor seri dari semua perangkat digital yang digunakan dan mengidentifikasi semua perangkat digital yang harus diakuisisi atau dikoleksi. Jika diperlukan, semua perangkat *mobile* dan barang-barang terkait dengannya seperti kartu memori, kartu SIM, pengisi daya, dan *docking station* yang ditemukan di tempat kejadian perkara, nomor serinya dan berbagai macam fitur yang dapat mengidentifikasikannya harus didokumentasikan dan dikoleksi. Diupayakan untuk menemukan kemasan asli dari ponsel; karena terdapat kemungkinan berisi catatan kode PIN dan PUK.
b. Jika perangkat adalah perangkat yang terhubung pada jaringan, PPBE harus mengidentifikasi layanan yang diberikan oleh perangkat untuk memahami dependensi dan untuk memastikan tingkat kekritisan perangkat dalam jaringan sebelum memutuskan melepas perangkat dari jaringan. Hal ini penting jika perangkat tersebut menjalankan fungsi *mission-critical* yang tidak dapat menoleransi *downtime* atau untuk menghindari penghancuran Bukti Elektronik potensial. Namun, jika terlihat ancaman melalui jaringan sedang berlangsung terhadap perangkat, PPBE harus membuat keputusan untuk melepaskan perangkat dari jaringan untuk melindungi Bukti Elektronik potensial.
c. Jika perangkat yang terhubung dalam jaringan adalah sistem CCTV, PPBE harus memperhatikan jumlah kamera yang terhubung ke sistem, beserta kamera yang aktif beroperasi. PPBE juga harus mencatat produsen, model dan pengaturan dasar dari sistem seperti pengaturan tampilan, pengaturan pencatatan terkini dan lokasi penyimpanan. Sehingga

memungkinkan untuk mengembalikan sistem ke keadaan semula apabila harus dilakukan pengubahan untuk memudahkan proses Koleksi dan Akuisisi.

d. Sedapat mungkin, status perangkat digital harus tetap seperti kondisi semula. Secara umum, jika perangkat digital dalam keadaan mati, maka PPBE tidak boleh menyalakannya dan jika perangkat dalam keadaan menyala, PPBE tidak boleh mematikannya. Hal tersebut dapat mencegah perusakan yang tidak perlu pada Bukti Elektronik potensial. Sebuah perangkat dengan baterai yang mungkin kehabisan daya, harus diisi dayanya untuk memastikan informasi tidak hilang. PPBE harus mengidentifikasi dan mengoleksi pengisi baterai dan kabel selama fase ini. Jika perangkat akan dipindahkan dan diperiksa di kemudian hari, sebaiknya perangkat dimatikan untuk meminimalkan potensi kerusakan pada data yang tersimpan dalam perangkat.
e. PPBE juga harus mempertimbangkan penggunaan detektor sinyal nirkabel untuk mendeteksi dan mengidentifikasi sinyal nirkabel dari perangkat nirkabel yang mungkin disembunyikan. Terdapat beberapa contoh kasus detektor sinyal nirkabel tidak digunakan karena kendala biaya dan waktu, PPBE harus mendokumentasikan hal ini.

7.2.2 Koleksi, Akuisisi Dan Pemeliharaan

7.2.2.1 Ikhtisar

PPBE harus memutuskan untuk mengkoleksi atau mengakuisisi Bukti Elektronik potensial dari perangkat digital. Pilihan tersebut harus diputuskan dengan mempertimbangkan keadaan, biaya, waktu, ketersediaan sumber daya serta prioritas.

Jika PPBE memutuskan untuk melepas perangkat, proses Koleksi atau Akuisisi Bukti Elektronik potensial akan mengikuti proses seperti yang dijelaskan dalam klausul 5.4. Pada kondisi perangkat tidak dapat diputuskan dari jaringan karena tingkat kritis fungsinya atau kecenderungan terhadap perusakan Bukti Elektronik potensial, PPBE harus melakukan Akuisisi langsung saat perangkat tetap terhubung ke jaringan.

CATATAN Hal penting bagi instansi untuk memiliki SOP penanganan bukti dengan menggunakan peralatan tervalidasi, digabungkan dengan dokumentasi yang baik serta PPBE yang telah terlatih dan berpengalaman.

Koleksi dan Akuisisi Bukti Elektronik potensial dari perangkat *mobile* jaringan merupakan proses yang rumit karena perangkat tersebut dapat berada pada beberapa kondisi dan menggunakan berbagai moda interaksi contohnya

Bluetooth, frekuensi radio, layar sentuh, dan infra merah. Selain itu, produsen perangkat *mobile* yang berbeda menggunakan jenis sistem operasi yang berbeda, mengharuskan metode Akuisisi bukti yang berbeda pula. Sebagian besar perangkat *mobile* menggunakan kartu memori, yang jika kartu memori tersebut dikeluarkan dari perangkat *mobile* dalam keadaan menyala mungkin mengganggu proses yang berjalan.

Umumnya, perangkat *mobile* seperti PDA dan ponsel harus dalam keadaan menyala agar dapat diakuisisi Bukti Elektronik potensialnya. Perangkat ini dapat terus mengubah lingkungan operasinya selama dalam keadaan menyala, misalnya, penanda waktu dapat otomatis diperbarui. Hal ini dapat menyebabkan adanya 2 (dua) salinan Bukti Elektronik dari perangkat yang sama namun tidak memenuhi fungsi verifikasi standar seperti *hashing*. Pada kondisi ini mungkin lebih tepat digunakan fungsi verifikasi alternatif yang dapat mengidentifikasi area kesamaan dan/atau perbedaan.

PPBE tidak boleh memasukkan perangkat Wi-Fi atau *Bluetooth* ke tempat kejadian perkara yang dapat mengubah informasi perangkat terkoneksi pada potensi perangkat bukti. Hal ini sangat penting khususnya jika penyidik harus mengetahui perangkat apa saja yang pernah terhubung.

Jika PPBE memutuskan untuk melakukan proses Akuisisi, perangkat jaringan harus dibiarkan terus bekerja untuk analisis lebih lanjut untuk memastikan adanya perangkat lain yang terhubung ke perangkat jaringan. PPBE harus mempertimbangkan kemungkinan sabotase oleh tersangka melalui koneksi jaringan yang aktif, sehingga dapat menentukan untuk tetap memantau sistem atau memutuskan sambungan.

7.2.2.2 Pedoman Untuk Koleksi Perangkat Jaringan

Dalam kondisi tertentu, perangkat jaringan dibiarkan tetap terhubung sehingga kegiatan pada perangkat jaringan dapat dipantau dan didokumentasikan oleh PPBE dan/atau SBE sesuai dengan kewenangannya. Apabila hal ini tidak diperlukan, perangkat harus dikoleksi seperti yang dijelaskan di bawah ini:

a. PPBE harus mengisolasi perangkat dari jaringan, ketika dapat dipastikan bahwa tidak ada data relevan yang akan tertimpa oleh tindakan ini dan tidak ada malfungsi yang terjadi pada sistem yang penting (*important system*) sebagai contoh sistem manajemen fasilitas di rumah sakit. Tindakan isolasi yang dimaksud dapat dilakukan dengan mencabut kabel dari sistem telepon atau *port* jaringan, atau menonaktifkan koneksi ke *wireless access point*.

b. Sebelum mencabut kabel, PPBE harus melacak koneksi ke perangkat digital dan memberi label pada *port* untuk melakukan rekonstruksi jaringan secara keseluruhan di kemudian hari. Perangkat dapat memiliki lebih dari satu metode komunikasi. Sebagai contoh, komputer dapat memiliki kabel LAN, modem nirkabel dan SIM *Card*. PED juga dapat terhubung ke jaringan melalui Wi-Fi, koneksi *Bluetooth* atau koneksi jaringan seluler. PPBE harus berusaha untuk mengidentifikasi semua metode komunikasi dan melakukan kegiatan yang tepat untuk melindungi dari upaya penghancuran Bukti Elektronik potensial.
c. Pada tahap ini, harus diperhatikan bahwa mencabut daya dari perangkat jaringan dapat merusak data volatil seperti proses yang sedang bekerja, koneksi jaringan dan data yang tersimpan dalam memori. Sistem operasi pada komputer *host* mungkin tidak dapat dipercaya dan melaporkan informasi yang salah. PPBE harus mengambil informasi ini menggunakan metode yang terverifikasi dan terpercaya sebelum mencabut daya dari perangkat. Setelah PPBE yakin bahwa tidak ada Bukti Elektronik potensial yang akan hilang, koneksi dari perangkat digital dapat dicabut.
d. Jika Koleksi dilakukan sebelum Akuisisi dan diketahui bahwa perangkat berisi memori volatil, perangkat harus terus menerus terhubung ke sumber daya.
e. Jika perangkat *mobile* dimatikan, perangkat tersebut dibungkus secara hati-hati, disegel dan diberi label. Hal ini untuk menghindari tindakan yang tidak disengaja atau disengaja pada tombol perangkat. Sebagai tindakan pencegahan, PPBE juga harus mempertimbangkan penggunaan kantong *Faraday* atau kotak pelindung.
f. Dalam kondisi tertentu, perangkat *mobile* harus dimatikan pada saat Koleksi untuk mencegah data tersebut diubah. Hal tersebut dapat terjadi melalui koneksi keluar dan masuk (*outgoing and incoming connection*) atau perintah yang dapat menyebabkan kerusakan Bukti Elektronik potensial.
g. Selanjutnya, masing-masing perangkat digital diperlakukan sebagai perangkat independen (lihat klausul 7.1) sampai saat diperiksa. Selama pemeriksaan, perangkat tersebut harus dianggap sebagai perangkat jaringan.

CATATAN Perangkat penyimpanan *removable* dapat digunakan sebagai media transmisi untuk mengimplementasikan suatu bentuk jaringan. PPBE harus memperhitungkan bahwa ada kemungkinan perangkat yang dikoleksi telah diimplementasikan dengan cara tersebut dan mencari informasi tentang

perangkat lain yang digunakan dalam proses perpindahan data secara fisik (*sneakernet*).

7.2.2.3 Pedoman Akuisisi perangkat jaringan

Pada kondisi perangkat terhubung dalam sebuah jaringan, terdapat kemungkinan bahwa perangkat terhubung ke lebih dari 1 (satu) jaringan fisik dan/atau virtual. Sebagai contoh, sebuah perangkat yang terlihat memiliki 1 (satu) koneksi jaringan fisik dapat saja sebenarnya menjalankan *Virtual Private Network* (VPN) dan mesin virtual dengan lebih dari 1 (satu) alamat IP. Dengan demikian, sebelum memutuskan hubungan perangkat dari jaringan, PPBE harus melakukan *logical acquisition* dari data yang berkaitan dengan koneksi jaringan virtual, (misalnya jaringan internet). Data yang diambil meliputi namun tidak terbatas pada konfigurasi IP dan tabel *routing*.

Jika perangkat jaringan diperlukan dalam keadaan menyala terus menerus, maka perangkat harus dicegah dari interaksi dengan jaringan radio nirkabel termasuk perangkat dengan GPS yang aktif. PPBE harus menggunakan metode yang diizinkan oleh peraturan perundang-undangan untuk mengisolasi sinyal radio. Harus dipastikan bahwa perangkat memiliki sumber daya yang cukup, karena metode isolasi dapat membuat perangkat mengkonsumsi daya yang lebih dalam upaya terhubung ke jaringan. Metode isolasi dapat meliputi, namun tidak terbatas pada:

a. Menggunakan perangkat *jamming* yang mampu memblokir transmisi dengan membuat gangguan yang kuat ketika perangkat memancarkan sinyal dalam rentang frekuensi yang sama dengan yang digunakan perangkat *mobile*.

   CATATAN 1 Penggunaan perangkat *jamming* harus memperhatikan peraturan perundang-undangan.

   CATATAN 2 Penggunaan perangkat *jamming* dapat menimbulkan pengaruh negatif pada kinerja perangkat elektronik seperti peralatan medis.

b. Menggunakan area kerja terlindung untuk melakukan pemeriksaan dengan aman di lokasi tertentu. Perlindungan dapat dilakukan untuk seluruh area kerja atau dengan mendirikan tenda *Faraday* yang dapat mudah berpindah-pindah. Memasukkan kabel ke dalam tenda menjadi permasalahan, karena tanpa isolasi yang tepat, kabel dapat berlaku seperti antena, menggagalkan tujuan adanya tenda. Ruang kerja juga bisa sangat terbatas.

c. Menggunakan area kerja terlindung untuk melakukan pemeriksaan dengan aman di lokasi tertentu. Area kerja yang terlindung dari frekuensi radio atau wadah (sangkar *Faraday*) dapat digunakan untuk mencegah koneksi ke jaringan.

   CATATAN 3 Semua metode pemblokiran akses nirkabel ke jaringan harus divalidasi agar digunakan pada frekuensi yang tepat. Validasi ini harus diperluas hingga pada kabel yang melewati pelindung.

d. Menggunakan sebuah (U)SIM pengganti yang meniru identitas perangkat asli dan mencegah akses jaringan oleh perangkat. Kartu-kartu ini mampu mengelabui perangkat agar menerima mereka sebagai (U)SIM asli dan memungkinkan pemeriksaan akan dilakukan dengan aman di setiap lokasi. (U)SIM harus tervalidasi untuk perangkat dan jaringan sebelum digunakan.
e. Menonaktifkan layanan jaringan dengan mengatur operator layanan *mobile* dan mengidentifikasi rincian layanan yang akan dinonaktifkan (misalnya pengenal peralatan, pengenal pelanggan, atau nomor telepon). Namun, informasi tersebut tidak selalu tersedia dengan mudah sehingga proses koordinasi dan konfirmasi dapat menunda proses pemutusan jaringan.

PPBE dapat melakukan Akuisisi langsung perangkat *mobile* sebelum melepaskan baterai (misalnya, untuk mengakses kartu SIM). Hal ini dapat dilakukan untuk mencegah hilangnya potensi informasi penting dalam RAM telepon atau untuk mempercepat proses pemeriksaan (misalnya di mana diyakini bahwa perangkat diproteksi dengan PIN dan/atau PUK yang akan membutuhkan waktu yang lama untuk mendapatkannya).

CATATAN 4 PPBE harus memastikan bahwa Koleksi dan Akuisisi Bukti Elektronik potensial sesuai dengan hukum dan peraturan perundang-undangan.

7.2.2.4 Pedoman Preservasi Perangkat Jaringan

Karena sifat perangkat digital dan Bukti Elektronik, pedoman Preservasi perangkat jaringan serupa dengan Preservasi komputer, perangkat periferal dan media penyimpanan digital. Lihat klausul 7.1.4 untuk panduan lengkap tentang Preservasi perangkat.

7.3 Koleksi, Akuisisi dan Preservasi CCTV

PPBE harus memahami bahwa pendekatan untuk mengekstrak rangkaian video yang berbasis komputer atau sistem CCTV yang melekat pada DVR berbeda dengan ekstraksi Bukti Elektronik konvensional pada komputer. Di bawah ini adalah panduan khusus untuk Akuisisi Bukti Elektronik potensial pada sistem CCTV:

a. Sebelum proses Akuisisi dimulai, PPBE harus terlebih dahulu memastikan apakah sistem mendokumentasikan rangkaian video yang akan diakuisisi. Selanjutnya, PPBE harus menentukan rentang waktu dari rekaman video yang diperlukan dan membandingkan waktu sistem dengan waktu yang sebenarnya dan mencatat setiap perbedaan. PPBE juga harus menentukan kamera yang dibutuhkan dan kemungkinan dapat mengakuisisinya secara terpisah. PPBE harus memperhatikan model dan produsen CCTV. Informasi ini mungkin diperlukan untuk menentukan perangkat lunak yang benar dalam memutar ulang video CCTV.
b. PPBE harus mengakuisisi semua rekaman kamera yang relevan selama waktu yang ditentukan untuk mempreservasi informasi investigasi tambahan yang mungkin dapat dikembangkan. PPBE harus mencatat semua kamera yang terhubung dalam sistem CCTV dan menentukan apakah mereka secara aktif merekam atau tidak merekam.

PPBE harus mengetahui ukuran penyimpanan sistem CCTV, serta kapan sistem dijadwalkan untuk menimpa informasi video. Informasi ini memungkinkan PPBE mengetahui rentang waktu rangkaian video yang akan disimpan pada sistem sebelum hilang. Tindakan pengamanan perlu dilakukan untuk memastikan bukti tidak berubah. Untuk bukti video digital, perlindungan penulisan (*write protection*) harus diberlakukan.

c. Terdapat beberapa pilihan yang dapat PPBE pilih untuk mengakuisisi Bukti Elektronik potensial dari sistem CCTV:
    1) Akuisisi *file* video dengan menuliskannya ke dalam CD/DVD/*Blu-ray disk* namun cara ini mungkin tidak praktis jika *file* video terlalu besar.
    2) Akuisisi *file* video dengan menulisnya ke media penyimpanan eksternal.
    3) Akuisisi *file* video melalui koneksi jaringan. Hal ini mungkin tersedia jika sistem CCTV dilengkapi dengan port jaringan
    4) Menggunakan fitur ekspor dari sistem CCTV ke format *file* lain (biasanya MPEG atau AVI) yang merupakan versi kompresi rekaman video. Cara ini hanya dapat digunakan sebagai upaya terakhir karena

kompresi ulang mengubah data asli dan selalu menghilangkan rincian gambar. Tidak dianjurkan untuk mengandalkan data yang dikompresi ulang untuk pemeriksaan jika data asli ada dan tersedia untuk analisis.

CATATAN 1 Kualitas rekaman video yang diekspor mungkin tidak sebagus rekaman aslinya.

5) Bila tidak memungkinkan untuk mengakuisisi langsung salinan Bukti Elektronik dari *file* pada perangkat rekaman, PPBE atau SBE harus berusaha untuk mengakuisisi salinan analog dari keluaran analog yang tersedia pada perangkat rekaman asli menggunakan alat perekam analog yang sesuai.

d. Setelah menyelesaikan Akuisisi, *file* hasil Akuisisi harus diperiksa untuk memastikan bahwa *file* yang benar atau bagian *file* yang benar telah diakuisisi. *file* juga harus diperiksa dengan perangkat lunak pemutar (untuk format *file* perangkat digital) untuk memastikan dapat diputar pada sistem lain - sebagian besar sistem CCTV memiliki paten masing-masing dan *file* tidak diharuskan dapat diputar dengan menggunakan perangkat lunak pemutar lain. Perangkat lunak pemutar rekaman yang benar mungkin tersedia untuk diunduh dari sistem CCTV pada saat yang sama ketika mengunduh data.
e. Media penyimpanan digital yang berisi *file* hasil Akuisisi harus diperlakukan sebagai salinan master Bukti Elektronik. Jika *file* telah diunduh ke komputer *notebook* atau kartu memori/ perangkat USB, maka salinan master permanen harus dibuat sesegera mungkin.
f. Selanjutnya, PPBE harus menyalakan ulang sistem CCTV jika sebelumnya dimatikan. Hal ini harus dilakukan di hadapan individu yang berwenang.

Dalam keadaan di mana tidak memungkinkan untuk dilakukan Akuisisi di tempat kejadian, PPBE harus memutuskan untuk mengoleksi media penyimpanan digital. Metode cepat yang dapat dilakukan adalah dengan mengganti *hard drive* sistem CCTV, dengan *hard drive* kosong atau hasil kloning. Namun, PPBE harus menilai beberapa risiko sebelum menggunakan metode ini, seperti kesesuaian *hard drive* baru dengan sistem dan kesesuaian *hard drive* yang dilepas dengan sistem lain untuk pemeriksaan.

CATATAN 2 Beberapa sistem memiliki *hard drive* yang dapat dilepas, tapi *hard drive* ini mungkin memerlukan perangkat keras sistemnya untuk dapat diputar kembali.

Jika tidak ada metode di atas yang memungkinkan, maka seluruh sistem CCTV harus dipindahkan dari tempat kejadian dan proses Akuisisi harus dilakukan di laboratorium forensik. Ini merupakan upaya terakhir PPBE dengan asumsi hal tersebut memungkinkan secara fisik untuk dilakukan karena beberapa sistem CCTV sangat besar dan kompleks. Sekali lagi, PPBE harus menilai risiko terhadap implikasi hukum dan asuransi sebelum pemindahan.

Karena sifat perangkat digital dan Bukti Elektronik potensial, pedoman Preservasi sistem CCTV serupa dengan Preservasi komputer, perangkat periferal dan media penyimpanan digital. Lihat klausul 7.1.4 untuk panduan tentang sistem Preservasi CCTV.

Lampiran A

(Informatif)

Deskripsi Kemampuan Dan Kompetensi Inti PPBE

Tabel A.1 – Deskripsi Kompetensi

No	Keahlian Inti	Deskripsi Keahlian Inti	Deskripsi Kompetensi		
			Mengetahui (1)	Memahami (2)	Menerapkan (3)
1	Identifikasi Bukti Elektronik	Memahami karakteristik perangkat digital, komponen-komponen, informasi yang dapat membantu investigasi dan hukum terkait penanganan Bukti Elektronik potensial dan kejahatan yang berhubungan dengan komputer. Dapat mengindentifikasi peralatan yang diperlukan untuk Koleksi, Akuisisi data dan perangkat serta dapat melakukan penilaian risiko.	Penggunaan TI secara umum dan pengadministrasian 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 yang berkaitan dengan forensik	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 non-volatil.	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; pengidentifika

			jaringan.		sian keterkaitan antara alamat IP dan alamat MAC untuk konfirmasi perangkat
2	Koleksi perangkat digital	Mengetahui peralatan yang dibutuhkan dan cara mengimplementasikan pembungkusan Bukti Elektronik, mampu melindungi Bukti Elektronik dari ancaman lingkungan, serta menjamin keutuhan informasi.	Keseluruhan data dikoleksi secara aman; prinsip dan perancangan peralatan dasar; penentuan metode terbaik dalam pengumpulan untuk mempreservasi informasi semaksimal mungkin yang berkaitan dengan perkara.	Perumusan dan pelaksanaan proses Koleksi; pengumpulan bukti; penulisan dokumen bukti; rantai pengawasan bukti; pengendalian kualitas dari proses Koleksi bukti; cara wawancara tersangka.	Optimasi proses Koleksi; pendokumentasian bukti yang tidak dapat diakuisisi karena berbagai kendala; pengumpulan kata kunci, kunci, *dongle*, dan informasi lain yang dibutuhkan untuk melakukan analisis di laboratorium.
3	Akuisisi Bukti Elektronik	Menerapkan persyaratan Akuisisi Bukti Elektronik potensial secara logis, memastikan proses dapat	Memahami informasi yang tersedia dalam perangkat digital, *database*, dokumen	Mengetahui bagaimana menentukan kebutuhan media penyimpanan; pelaksanaan	Mampu untuk melakukan Akuisisi pada media penyimpanan digital termasuk sistem RAID,

		diulang, dapat diaudit, dapat diproduksi kembali, dan dapat dipertahankan. Lingkup area meliputi Akuisisi pada sistem dalam keadaan menyala, Akuisisi sistem dalam keadaan mati, dan forensik jaringan.	yang dihasilkan sistem, data yang dihasilkan pengguna, dan data volatil; struktur file sistem UNIX dan *Windows* serta perangkatnya; dampak dari data volatil.	prosedur Akuisisi penyalinan *per bit* (*imaging*) (seperti Akuisisi media penyimpanan utuh dan parsial); prosedur Akuisisi pada sistem dalam keadaan menyala; prosedur Akuisisi pada sistem dalam keadaan mati; pembuatan nilai *hash*.	*database*, perangkat, dan perangkat miniatur; memahami keterkaitan dan dampak dari metode Akuisisi yang berbeda-beda.
4	Preservasi Bukti Elektronik	Menerapkan dan menilai persyaratan untuk Preservasi Bukti Elektronik potensial, memahami faktor-faktor dan parameter yang mempengaruhi akurasinya.	Persyaratan dan prosedur pengelolaan rantai pengawasan sebagai persyaratan hukum; dampak lingkungan seperti	Cara pembuatan dokumen audit bukti; penentuan parameter dokumen audit bukti; jaminan keamanan informasi,	Tindakan pengamanan Bukti Elektronik, dalam pengubahan perangkat besar menjadi perangkat miniatur genggam;

		Lingkup area meliputi metodologi, pengelolaan rantai pengawasan, penanganan perangkat komputer dan penanganan media penyimpanan digital.	kelembapan, temperatur dan guncangan atas perangkat digital; pilihan pembungkusan, transportasi, dan persyaratan penyimpanan.	ancaman, kerapuhan dan pengendalian untuk Bukti Elektronik.	prosedur untuk mendokumentasikan rincian bukti.

Lampiran B

(Informatif)

Persyaratan Dokumentasi Minimal Untuk Perpindahan Bukti

PPBE harus selalu bertanggungjawab atas data dan perangkat digital yang diakuisisi yang ada dalam kewenangannya. Untuk mempertahankan pengendalian tersebut, PPBE harus memiliki kewenangan, terlatih, dan memiliki kualifikasi sesuai dengan ketentuan peraturan perundang-undangan.

Dokumentasi minimal yang harus disampaikan dalam pertukaran Bukti Elektronik Potensial lintas wilayah adalah:

a. Nama dan alamat pemberi tugas;
b. Surat tugas, keterangan pelatihan dan kualifikasi PPBE;
c. Tujuan pemeriksaan;
d. Tindakan apa saja yang dilakukan;
e. Siapa melakukan apa dan kapan;
f. Dokumentasi rantai pengawasan berkaitan dengan pemeriksaan yang spesifik;
g. Daftar penjelasan dari Bukti Elektronik potensial dan media penyimpanan digital yang dikoleksi dan diakuisisi; dan
h. Informasi terkait pemeriksaan, pengujian dan analisis yang digunakan untuk menghasilkan salinan bukti.

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA,

DRAFTDRAFTDRAFT

JOHNNY G. PLATE

LAMPIRAN II
PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA
NOMOR TAHUN 2021
TENTANG DAFTAR PERLENGKAPAN MINIMUM UNTUK KEPERLUAN PENANGANAN PERTAMA BUKTI ELEKTRONIK

DAFTAR PERLENGKAPAN MINIMUM UNTUK KEPERLUAN PENANGANAN PERTAMA BUKTI ELEKTRONIK

A. Perlengkapan umum termasuk tetapi tidak terbatas pada:
   1. *Flow chart* untuk penanganan kasus yang berbeda-beda
   2. Kamera (Foto dan video)
   3. Jam digital
   4. Kantong bukti
   5. Alat tulis
   6. Sarung tangan
   7. Catatan inventori, stiker, label
   8. *Power bank*
   9. Kantong antistatis dan *non-magnetic toolkit*
   10. Daftar nama dan kontak konsultan hukum

B. Perlengkapan khusus ini dipersiapkan jika PPBE perlu melakukan akusisi Bukti Elektronik potensial di tempat kejadian perkara:
   1. Laptop forensik
      a. Prosesor – Prosesor dengan jumlah inti 8
      b. RAM – 8 *Gigabyte*
      c. Media penyimpanan berkapasitas besar dan cepat
   2. Perangkat *write protection*
   3. Media penyimpanan yang sudah dilakukan proses *wipe* dan/atau *format*
   4. Eksternal HDD (USB *interface*)
   5. DVD RW *drive* (USB *interface*)
   6. CD-R/DVD-R kosong

DRAFTDRAF

C. Perangkat lunak PPBE:

1. Perangkat lunak untuk Akuisisi data volatil;
2. Perangkat lunak untuk Akuisisi media penyimpanan;
3. Perangkat lunak untuk Akuisisi *smartphone;*
4. Perangkat lunak untuk Akuisisi dan analisa komputasi awan
5. *Bootable disc*/*disk* untuk proses Akuisisi.

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA,

DRAFT DRAFT DRAFT

JOHNNY G. PLATE