MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 47 TAHUN 2022
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG KEAHLIAN DIGITAL FORENSIK SUBBIDANG PENANGANAN PERTAMA BUKTI ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KETENAGAKERJAAN REPUBLIK INDONESIA,

Menimbang :

a. bahwa untuk melaksanakan ketentuan Pasal 31 Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia, perlu menetapkan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keahlian Digital Forensik Subbidang Penanganan Pertama Bukti Elektronik;

b. bahwa Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keahlian Digital Forensik Subbidang Penanganan Pertama Bukti Elektronik telah disepakati melalui Konvensi Nasional pada 29 November 2021 di Jakarta;

c. bahwa sesuai surat Kepala Pusat Pengembangan Profesi dan Sertifikasi Nomor B-1246/KOMINFO/BLSDM.4/LT.02.02/12/2021 tanggal 13 Desember 2021 perihal permohonan Penetapan Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keahlian Digital Forensik Subbidang Penanganan Pertama Bukti Elektronik;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Keputusan Menteri Ketenagakerjaan tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keahlian Digital Forensik Subbidang Penanganan Pertama Bukti Elektronik;

Mengingat : 1. Undang-Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 39, Tambahan Lembaran Negara Republik Indonesia Nomor 4279);

2. Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);

3. Peraturan Pemerintah Nomor 31 Tahun 2006 tentang Sistem Pelatihan Kerja Nasional (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 67, Tambahan Lembaran Negara Republik Indonesia Nomor 4637);

4. Peraturan Presiden Nomor 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 24);

5. Peraturan Presiden Nomor 95 Tahun 2020 tentang Kementerian Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 213);

6. Peraturan Menteri Ketenagakerjaan Nomor 21 Tahun 2014 tentang Pedoman Penerapan Kerangka Kualifikasi Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2014 Nomor 1792);
7. Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2016 Nomor 258);
8. Peraturan Menteri Ketenagakerjaan Nomor 1 Tahun 2021 tentang Organisasi dan Tata Kerja Kementerian Ketenagakerjaan (Berita Negara Republik Indonesia Tahun 2021 Nomor 108);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN MENTERI KETENAGAKERJAAN TENTANG PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG KEAHLIAN DIGITAL FORENSIK SUBBIDANG PENANGANAN PERTAMA BUKTI ELEKTRONIK.

KESATU : Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keahlian Digital Forensik Subbidang Penanganan Pertama Bukti Elektronik, sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Menteri ini.

KEDUA : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan dan pelatihan serta sertifikasi kompetensi.

KETIGA : Pemberlakuan Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dan penyusunan jenjang kualifikasi nasional sebagaimana dimaksud dalam Diktum KEDUA ditetapkan oleh Menteri Komunikasi dan Informatika dan/atau kementerian/lembaga teknis terkait sesuai dengan tugas dan fungsinya.

KEEMPAT : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dikaji ulang setiap 5 (lima) tahun atau sesuai dengan kebutuhan.

KELIMA : Keputusan Menteri ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 20 Mei 2022

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH

LAMPIRAN
KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 47 TAHUN 2022
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG KEAHLIAN DIGITAL FORENSIK SUBBIDANG PENANGANAN PERTAMA BUKTI ELEKTRONIK

BAB I
PENDAHULUAN

A. Latar Belakang

Pemanfaatan teknologi informasi sebagai bagian dari otomatisasi di abad ke-21 sudah merupakan sebuah terobosan yang tidak terelakkan lagi. Pesatnya perkembangan komputer serta teknologi informasi dan komunikasi telah mendorong perusahaan di dunia untuk melakukan adaptasi dan perubahan dalam berbisnis diantaranya melalui pemanfaatan *cloud computing*, *artificial intelligence,* maupun *big data* untuk mengolah aset informasi yang meningkat pesat. Akan tetapi disamping banyaknya manfaat yang diperoleh, penggunaan teknologi juga menimbulkan risiko terjadinya kejahatan atau serangan. Serangan tersebut dapat menyebabkan kebocoran dan kerugian data yang dapat menimbulkan masalah hukum dan kerugian finansial, serta merusak reputasi dan kepercayaan publik. Pemanfaatan teknologi informasi secara digital forensik perlu dilakukan untuk mengidentifikasi, memeriksa dan menganalisa bukti-bukti elektronik yang terkait untuk mengungkap kejahatan atau serangan tersebut secara ilmiah.

Kompetensi bidang digital forensik meliputi mengidentifikasi, mengoleksi, mengakuisisi dan mempreservasi bukti elektronik, serta memeriksa, menganalisa dan menginterpretasinya secara mendalam, sehingga dapat dipertanggungjawabkan secara ilmiah dan hukum.

Perkembangan dan pemanfaatan bidang digital forensik memerlukan personil dengan kompetensi yang mumpuni. Kemampuan personil yang ada di bidang digital forensik sangat bervariasi sejalan dengan munculnya berbagai institusi pendidikan formal maupun informal di bidang tersebut. Standar kompetensi yang sesuai diperlukan untuk memberi kepastian bagi berbagai pihak yang berkepentingan dengan ketersediaan tenaga kerja di bidang ini. Karenanya, dikembangkan Standar Kompetensi Kerja Nasional Indonesia (SKKNI) di Bidang Digital Forensik Subbidang Penanganan Pertama Bukti Elektronik.

Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pada Pasal 5 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menyebutkan bahwa “informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah”. Pengertian informasi elektronik dan dokumen elektronik disebutkan pada Pasal 1, yaitu "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", sedangkan "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".

ISO/IEC 27037:2012 tentang *Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, menjadi referensi utama untuk penanganan pertama bukti elektronik, yang melalui SK Penetapan Badan Standardisasi Nasional (BSN) No. 37/KEP/BSN/3/2014 diadopsi menjadi SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital, dan kemudian dikuatkan melalui Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 04 Tahun 2019 tentang Panduan Identifikasi, Koleksi, Akuisisi dan Preservasi Bukti Digital.

Dalam rangka mengimplementasikan kompetensi kerja digital forensik yang dapat diukur pengetahuan (*knowledge*), keterampilan (*skill*) dan sikap tingkah laku (*attitude*), perlu disusun suatu Standar Kompetensi Kerja Nasional Indonesia (SKKNI). Penyusunan standar kompetensi ini mengacu pada Peraturan Menteri Ketenagakerjaan Republik Indonesia Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia, yang menggambarkan kompetensi personel dalam aspek pengetahuan, keterampilan dan sikap kerja yang relevan untuk melaksanakan tugas atau jabatan tertentu sebagaimana yang dipersyaratkan oleh organisasi atau pengguna sehingga diharapkan sertifikasi kompetensi yang dihasilkan setara dengan kompetensi kerja yang ditetapkan oleh pemerintah.

B. Pengertian

1. Digital Forensik (DF)/*Forensic Digital* (FD) adalah penerapan ilmu pengetahuan dan teknologi informasi untuk kepentingan pro-justisia dan penegakan hukum, dalam keseluruhan proses mengidentifkasi, mengumpulkan, mengakuisisi, memulihkan, menyimpan, memeriksa, menganalisa dan mengintrepretasi informasi elektronik dan/atau dokumen elektronik yang terdapat dalam sistem elektronik atau media penyimpanan elektronik berdasarkan metode dan dengan alat yang dapat

dipertanggungjawabkan secara ilmiah serta oleh personel yang berkompeten.

2. Bukti Elektronik (BE) atau *Digital Evidence* (DE) adalah sistem, perangkat, dan/atau media penyimpanan elektronik yang berpotensi terdapat informasi elektronik dan/atau dokumen elektronik yang dapat diandalkan sebagai alat bukti.
3. Alat bukti elektronik adalah informasi elektronik dan/atau dokumen elektronik yang digunakan sebagai alat bukti sebagaimana diatur dalam peraturan perundangan.
4. *Associate Digital Evidence First Responder* (ADEFR) atau Asisten Penangan Pertama Bukti Elektronik (APPBE) adalah personel yang berwenang, berkompeten dan berkualifikasi sesuai dengan Kerangka Kualifikasi Nasional Indonesia (KKNI) Level 5, serta bertanggungjawab untuk membantu DEFR/PPBE dalam melakukan penanganan pertama terhadap bukti elektronik di tempat kejadian, meliputi: identifikasi, pengumpulan, dan preservasi bukti elektronik.
5. *Digital Evidence First Responder* (DEFR) atau Penangan Pertama Bukti Elektronik (PPBE) adalah personel yang berwenang, berkompeten dan berkualifikasi sesuai dengan KKNI Level 6, serta bertanggungjawab untuk melakukan penanganan pertama terhadap bukti elektronik di tempat kejadian meliputi identifikasi, pengumpulan, akuisisi, dan preservasi bukti elektronik.
6. *Digital Evidence Specialist* (DES) atau Spesialis Bukti Elektronik (SBE) adalah personel yang dapat melaksanakan tugas-tugas DEFR/PPBE yang berwenang, berkompeten dan berkualifikasi sesuai dengan KKNI Level 7 dan memiliki pengetahuan, keterampilan, sikap kerja dan kemampuan khusus untuk menangani berbagai permasalahan teknis yang kompleks dalam penanganan pertama bukti elektronik.
7. *Identification*/identifikasi adalah proses yang meliputi pencarian, pengenalan/rekognisi dan pendokumentasian bukti elektronik.
8. *Collection*/koleksi adalah proses pengumpulan bukti elektronik.

9. *Acquisition*/akuisisi adalah proses penyalinan terhadap data elektronik dalam sebuah rangkaian yang telah ditetapkan, baik salinan fisik *bit-per-bit* maupun salinan logik *non bit-per-bit* yang diverifikasi melalui fungsi *hash* atau fungsi lain yang setara.
10. *Preservation*/preservasi adalah proses mempertahankan dan melindungi integritas/keutuhan dan/atau kondisi orisinal dari bukti elektronik.
11. *Hash* adalah fungsi matematika satu arah yang digunakan untuk verifikasi yang berisikan sederet kode unik melalui algoritma tertentu.
12. *Imaging* adalah proses membuat salinan fisik *bit-per-bit* terhadap media penyimpanan elektronik yang menghasilkan *image file* yang identik dan diverifikasi melalui fungsi *hash* atau fungsi lain yang setara.
13. *Chain of custody* atau rantai pengawasan/catatan penelusuran/ketelusuran barang bukti adalah dokumen atau serangkaian dokumen yang secara kronologis mencatat seluruh aktivitas penanganan dan pergerakan bukti elektronik.
14. *Volatile* adalah data elektronik yang mudah sekali rusak/hilang pada kondisi tertentu, antara lain memori RAM, kontainer/volume enkripsi yang sudah dalam keadaan terdekripsi (*mounted*), proses yang sedang berjalan, koneksi jaringan dan *setting* tanggal/waktu serta informasi berharga lainnya.
15. Prosedur adalah serangkaian tindakan untuk penanganan pertama bukti elektronik yang sudah ditetapkan, meliputi identifikasi, koleksi, akuisisi dan preservasi bukti elektronik.

C. Penggunaan SKKNI

Standar Kompetensi dibutuhkan oleh beberapa lembaga/institusi yang berkaitan dengan pengembangan sumber daya manusia, sesuai dengan kebutuhan masing- masing:

1. Untuk institusi pendidikan dan pelatihan
   a. Memberikan informasi untuk pengembangan program dan kurikulum.

b. Sebagai acuan dalam penyelenggaraan pelatihan, penilaian, dan sertifikasi.

2. Untuk dunia usaha/industri dan penggunaan tenaga kerja
   a. Membantu dalam rekrutmen.
   b. Membantu penilaian unjuk kerja.
   c. Membantu dalam menyusun uraian jabatan.
   d. Membantu dalam mengembangkan program pelatihan yang spesifik berdasar kebutuhan dunia usaha/industri.
3. Untuk institusi penyelenggara pengujian dan sertifikasi
   a. Sebagai acuan dalam merumuskan paket-paket program sertifikasi sesuai dengan kualifikasi dan levelnya.
   b. Sebagai acuan dalam penyelenggaraan pelatihan penilaian dan sertifikasi.

D. Komite Standar Kompetensi

Susunan komite standar kompetensi pada Standar Kompetensi Kerja Nasional Indonesia (SKKNI) di Bidang Digital Forensik Subbidang *Digital Evidence* melalui keputusan melalui Keputusan Sekretaris Badan Litbang SDM Kominfo Nomor 37C tanggal 1 Maret 2021 tentang Tim Komite Standar Kompetensi Kerja Nasional Indonesia Bidang Digital Forensik Subbidang Penanganan Pertama Bukti Elektronik dapat dilihat pada Tabel 1.

Tabel 1. Susunan Komite Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Bidang Komunikasi dan Informatika

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Kepala Badan Litbang SDM	Kementerian Komunikasi dan Informatika	Pengarah
2.	Kepala Pusbang Profesi dan Sertifikasi	Kementerian Komunikasi dan Informatika	Ketua
3.	Sekretaris Badan Litbang SDM	Kementerian Komunikasi dan Informatika	Sekretaris
4.	Kepala Biro Perencanaan	Kementerian Komunikasi dan Informatika	Anggota
5.	Sekretaris Ditjen Aplikasi dan Informatika	Kementerian Komunikasi dan Informatika	Anggota
6.	Sekretaris Ditjen Sumber Daya Perangkat Pos dan Informatika	Kementerian Komunikasi dan Informatika	Anggota
7.	Sekretaris Ditjen Penyelenggaraan Pos dan Informatika	Kementerian Komunikasi dan Informatika	Anggota
8.	Kepala Puslabfor Bareskrim Polri	Markas Besar Kepolisian Negara Republik Indonesia (Mabes Polri)	Anggota
9.	Direktur Teknologi Informasi dan Produksi Intelijen	Jaksa Agung Muda Bidang Intelijen	Anggota
10.	Direktur Kebijakan Sumber Daya Manusia	Badan Siber dan Sandi Negara (BSSN)	Anggota
11.	Direktur Deteksi dan Analisis Korupsi	Komisi Pemberantasan Korupsi (KPK)	Anggota
12.	Direktur Penegakan Hukum	Direktorat Jenderal Pajak (DJP)	Anggota
13.	Ketua Asosiasi Forensik Digital Indonesia	Asosiasi Forensik Digital Indonesia (AFDI)	Anggota
14.	Ketua Umum Ikatan Ahli Informatika Indonesia	Ikatan Ahli Informatika Indonesia (IAII)	Anggota
15.	Ketua Umum Ikatan Profesi Komputer dan Informatika Indonesia	Ikatan Profesi Komputer dan Informatika Indonesia (IPKIN)	Anggota

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
16.	Ketua Umum Indonesia Artificial Intelligence Society	Indonesia Artificial Intelligence Society (IAIS)	Anggota
17.	Ketua Umum Asosiasi Big Data dan AI	Asosiasi Big Data dan AI (ABDI)	Anggota
18.	Ketua Umum Asosiasi Game Indonesia	Asosiasi Game Indonesia (AGI)	Anggota
19.	Ketua Umum Perhimpunan Hubungan Masyarakat Indonesia	Perhimpunan Hubungan Masyarakat Indonesia (PERHUMAS)	Anggota
20.	Ketua Badan Koordinasi Kehumasan Pemerintah	Badan Koordinasi Kehumasan Pemerintah	Anggota

Tabel 2. Susunan Tim Perumus SKKNI Bidang Digital Forensik Subbidang Penanganan Pertama Bukti Elektronik

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Muhammad Nuh Al-Azhar	Pusat Laboratorium Forensik Bareskrim Polri	Ketua
2.	Siswanto	Universitas Budi Luhur/IAII	Sekretaris
3.	Satriyo Wibowo	Indonesia Cyber Security Forum	Anggota
4.	Eko K. Budiardjo	Universitas	Anggota
5.	I Made Wiryana	Universitas Gunadarma/IKPIN	Anggota
6.	Izazi Mubarok	Asosiasi Forensik Digital Indonesia	Anggota
7.	Sari Wardhani	Kemitraan/Program BBE Komisi Pemberantasan Korupsi	Anggota
8.	Hafni Ferdian	Komisi Pemberantasan Korupsi	Anggota
9.	Teguh Arifiadi	Direktorat Pengendalian Aplikasi Informatika	Anggota
10.	Pinuji Prasetyaningtyas	Badan Siber dan Sandi Negara	Anggota

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
11.	Arhemi Dutimarshelly	KPMG Siddharta Advisory	Anggota

Tabel 3. Susunan Tim Verifikasi SKKNI Bidang Digital Forensik Subbidang Penanganan Pertama Bukti Elektronik

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Eyla Alivia Maranny	Kementerian Komunikasi dan Informatika	Ketua
2.	Diah Arum Maharani	Kementerian Komunikasi dan Informatika	Anggota
3.	Yane Erina Marentek	Kementerian Komunikasi dan Informatika	Anggota
4.	Fajar Rulhudana	Kementerian Komunikasi dan Informatika	Anggota
5.	Carmin	Kementerian Komunikasi dan Informatika	Anggota
6.	Maharlesa Putri	Kementerian Komunikasi dan Informatika	Anggota

BAB II
STANDAR KOMPETENSI KERJA NASIONAL INDONESIA

A. Pemetaan Standar Kompetensi

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
Menerapkan identifikasi, koleksi, akuisisi dan preservasi bukti elektronik	Melaksanakan identifikasi dan koleksi bukti elektronik	Mengidentifikasi bukti elektronik	Mempersiapkan penanganan pertama bukti elektronik
			Mencari bukti elektronik fisik mandiri (*standalone devices*)
			Mencari bukti elektronik fisik yang terkoneksi ke jaringan (*networked devices*)
			Mengumpulkan informasi non-elektronik
			Memilih opsi untuk koleksi atau akuisisi
		Mengoleksi bukti elektronik	Mengumpulkan bukti elektronik dalam kondisi masih hidup/*on*
			Mengumpulkan bukti elektronik dalam kondisi sudah mati/*off*
			Mengumpulkan bukti elektronik yang terkoneksi ke jaringan (*networked devices*)
			Mengumpulkan bukti elektronik dari sistem *Closed Circuit Television* (CCTV)
	Melaksanakan akuisisi dan preservasi bukti elektronik	Mengakuisisi bukti elektronik	Menyalin data elektronik dari bukti elektronik dalam kondisi masih hidup/*on*

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
			Menyalin data elektronik dari bukti elektronik dalam kondisi sudah mati/*off*
			Menyalin data elektronik dari bukti elektronik yang terkoneksi ke jaringan (*networked devices*)
			Menyalin data elektronik dari sistem *Closed Circuit Television* (CCTV)
			Menyalin data elektronik dengan kondisi khusus
			Memberi dukungan teknis lanjutan
		Mempreservasi bukti elektronik	Menyegel data elektronik yang telah diakuisisi dengan menggunakan fungsi verifikasi
			Mengamankan bukti elektronik dengan menerapkan prinsip kerahasiaan, integritas, dan ketersediaan
			Mengemas bukti elektronik

B. Daftar Unit Kompetensi

NO.	KODE UNIT	JUDUL UNIT KOMPETENSI
1	*2*	*3*
1.	J.62FDG00.001.1	Mempersiapkan Penanganan Pertama Bukti Elektronik
2.	J.62FDG00.002.1	Mencari Bukti Elektronik Fisik Mandiri (*Standalone Devices*)
3.	J.62FDG00.003.1	Mencari Bukti Elektronik Fisik yang Terkoneksi ke Jaringan (*Networked Devices*)
4.	J.62FDG00.004.1	Mengumpulkan Informasi Non-Elektronik
5.	J.62FDG00.005.1	Memilih Opsi Untuk Koleksi atau Akuisisi
6.	J.62FDG00.006.1	Mengumpulkan Bukti Elektronik dalam Kondisi Masih Hidup/*On*
7.	J.62FDG00.007.1	Mengumpulkan Bukti Elektronik dalam Kondisi Sudah Mati/*Off*
8.	J.62FDG00.008.1	Mengumpulkan Bukti Elektronik yang Terkoneksi ke Jaringan (*Networked Devices*)
9.	J.62FDG00.009.1	Mengumpulkan Bukti Elektronik dari Sistem *Closed Circuit Television* (CCTV)
10.	J.62FDG00.010.1	Menyalin Data Elektronik dari Bukti Elektronik Dalam Kondisi Masih Hidup/*On*
11.	J.62FDG00.011.1	Menyalin Data Elektronik dari Bukti Elektronik Dalam Kondisi Sudah Mati/*Off*
12.	J.62FDG00.012.1	Menyalin Data Elektronik dari Bukti Elektronik yang Terkoneksi ke Jaringan (*Networked Devices*)
13.	J.62FDG00.013.1	Menyalin Data Elektronik dari Sistem *Closed Circuit Television* (CCTV)
14.	J.62FDG00.014.1	Menyalin Data Elektronik dengan Kondisi Khusus
15.	J.62FDG00.015.1	Memberi Dukungan Teknis Lanjutan
16.	J.62FDG00.016.1	Menyegel Data Elektronik yang telah Diakuisisi dengan Menggunakan Fungsi Verifikasi
17.	J.62FDG00.017.1	Mengamankan Bukti Elektronik dengan Menerapkan Prinsip Kerahasiaan, Integritas, dan Ketersediaan
18.	J.62FDG00.018.1	Mengemas Bukti Elektronik

C. Uraian Unit Kompetensi

KODE UNIT : **J.62FGD00.001.1**

JUDUL UNIT : **Mempersiapkan Penanganan Pertama Bukti Elektronik**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengumpulkan informasi insiden dan alat bantu, mempersiapkan penanganan insiden secara seketika, dan mempersiapkan pelaksanaan tugas dan tanggung jawab sebagai anggota tim sesuai kompetensi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengumpulkan informasi insiden dan alat bantu	1.1 **Informasi awal** terjadinya insiden dicari sesuai prosedur. 1.2 **Detail instruksi rencana penanganan pertama bukti elektronik** dilaksanakan sesuai kebutuhan. 1.3 **Alat bantu** disiapkan sesuai kebutuhan.
2. Mempersiapkan penanganan insiden secara seketika	2.1 Strategi dan taktik awal penanganan pertama bukti elektronik dilaksanakan sesuai pembagian tugas **anggota tim** dan kondisi yang ada. 2.2 **Informasi berkembangnya insiden** dikomunikasikan secara efektif sesuai kebutuhan.
3. Mempersiapkan pelaksanaan tugas dan tanggung jawab sebagai anggota tim sesuai kompetensi	3.1 Tugas, peran dan tanggung jawab dari setiap anggota tim diidentifikasi sesuai prosedur. 3.2 Bantuan teknis diidentifikasi sesuai kompetensi dan kewenangan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk personel dalam mempersiapkan penanganan pertama bukti elektronik sesuai prosedur investigasi dari suatu insiden.

1.2 Informasi awal antara lain jenis insiden, tempat, tanggal dan waktu terjadinya insiden.

1.3 Detail instruksi rencana penanganan pertama bukti elektronik mencakup antara lain pencarian, pengumpulan, dan akuisisi bukti elektronik, serta aktivitas jaringan dan data yang mudah hilang/rusak/*volatile.*

1.4 Alat bantu berupa *tools*, perlengkapan dan manual serta dokumentasi penting untuk penanganan pertama bukti elektronik.

1.5 Dokumentasi penting termasuk dengan aspek legalitas dan faktor lainnya yang mungkin melarang pengumpulan bukti elektronik potensial.

1.6 Anggota tim yang diarahkan dan diizinkan untuk mengembangkan strategi dan taktik baru dalam menanggapi kondisi yang ada.

1.7 Informasi insiden, seiring dengan perkembangannya dibagikan kepada anggota tim secepat mungkin untuk memastikan keputusan tentang tindakan yang akan diambil.

1.8 Kompetensi teknis dan legal, antara lain mencakup pada Lampiran A ISO/IEC 27037:2012 serta kualifikasi yang relevan dengan yurisdiksi, proses dan metode yang cocok untuk menangani bukti elektronik potensial dalam konteks penanganan pertama bukti elektronik dipahami dan dilatih dengan benar, dan tanggungjawab untuk pemeliharaan pelatihan, skill dan kompetensi dipegang oleh setiap individu dan institusi.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 *Tools* yang digunakan untuk akuisisi bukti elektronik

2.1.3 *Tools* yang digunakan untuk verifikasi fungsi *hash* atau fungsi lain yang setara

2.1.4 *Tools* yang digunakan untuk *write-protect* guna menjaga keutuhan data elektronik dari perubahan data

2.1.5 *Tools* yang digunakan untuk ekstraksi perangkat seluler pada berbagai *platform* seluler

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat

kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan persiapan penanganan pertama bukti elektronik dari suatu insiden.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Bukti elektronik

3.1.2 Prosedur penanganan pertama bukti elektronik

3.1.3 Informasi awal terjadinya insiden

3.1.4 Aspek legalitas penanganan pertama bukti elektronik

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

3.2.3 Mengolah grafik presentasi

3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai informasi awal insiden dan penyusunan dokumentasi penting terkait aspek legalitas

4. Sikap kerja yang diperlukan

4.1 Teliti dalam penyiapan alat bantu dan dokumentasi penting terkait aspek legalitas

4.2 Berwawasan luas dalam melaksanakan detail instruksi rencana investigasi sesuai kebutuhan

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab dalam mengidentifikasi dari setiap anggota tim sesuai prosedur

5. Aspek kritis

5.1 Ketepatan dalam mencari informasi awal terjadinya insiden sesuai prosedur

KODE UNIT : **J.62FDG00.002.1**

JUDUL UNIT : **Mencari Bukti Elektronik Fisik Mandiri (*Standalone Devices*)**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengenali, menjaga keamanan (*safety*), dan mendokumentasi bukti elektronik fisik mandiri (*standalone devices*) di lokasi insiden.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengenali bukti elektronik fisik mandiri di **lokasi insiden**	1.1 **Bukti elektronik mandiri (*standalone digital device*)** yang tidak terkoneksi ke jaringan beserta **peralatan pendukungnya (*peripheral devices*)** diidentifikasi berdasarkan prosedur. 1.2 **Media penyimpanan elektronik** diidentifikasi dengan teliti. 1.3 **Perangkat deteksi** digunakan untuk mengidentifikasi bukti elektronik yang tersembunyi.
2. Menjaga keamanan (*safety*) bukti elektronik fisik mandiri di lokasi insiden	2.1 Lokasi dari bukti elektronik diklarifikasi kepada penanggung jawab lokasi tersebut. 2.2 **Informasi yang berkaitan dengan insiden** didokumentasikan sesuai **prosedur dokumentasi**. 2.3 Penanganan perangkat dilaksanakan sesuai **prosedur umum penanganan pertama bukti elektronik.** 2.4 Risiko selama proses pencarian dinilai sesuai prosedur untuk melindungi keamanan personel dan keutuhan bukti elektronik.
3. Mendokumentasi bukti elektronik fisik mandiri di lokasi insiden	3.1 **Tanda identifikasi** dari bukti elektronik didokumentasikan sesuai prosedur dokumentasi. 3.2 **Kondisi bukti elektronik** didokumentasikan sesuai prosedur dokumentasi.

BATASAN VARIABEL

1. Konteks variabel

1.1 Lokasi insiden merupakan lokasi tempat insiden keamanan informasi berlangsung atau Tempat Kejadian Perkara (TKP).

1.2 Bukti elektronik mandiri (*standalone digital device*) adalah perangkat elektronik seperti komputer yang jika tidak terkoneksi ke jaringan, namun mungkin terkoneksi dengan perangkat periferal (*peripheral devices*) seperti *printer, scanner, webcam,* pemutar *motion picture experts group audio layer-3* (mp3), *Global Positioning System* (GPS), *Radio Frequency Identification* (RFID) dan lain-lain.

1.3 Peralatan pendukungnya, seperti *battery charger* untuk men-*charge batere* komputer hidup/*on* yang mungkin akan habis, dengan pertimbangan kebutuhan informasi *volatile.*

1.4 Media penyimpanan elektronik, antara lain *harddisk/solid state disk* eksternal, *flashdisk*, CD/DVD, *bluray disk, floppy disk*, *magnetic tapes* dan *memory card* dicari dengan teliti.

1.5 Perangkat deteksi, seperti: *wireless signal detector* digunakan untuk mendeteksi dan mengidentifikasi sinyal *wireless* yang tersembunyi.

1.6 Informasi yang berkaitan dengan insiden, antara lain personel yang punya akses, Tempat Kejadian Perkara (TKP) berikut seluruh komponen perangkat dan kabelnya, pelabelan *ports* dari perangkat/kabelnya, catatan tempel, diari, kertas catatan, manual *hardware/software* dan detail *passwords*/PIN.

1.7 Prosedur dokumentasi, antara lain: pendokumentasian dengan penggunaan fotografi, sketsa dan catatan.

1.8 Prosedur umum penanganan pertama bukti elektronik adalah perangkat yang sudah mati/*off* jangan dihidupkan, dan sebaliknya perangkat yang masih hidup/*on*, jangan dimatikan.

1.9 Tanda identifikasi, antara lain: jenis, *merk* dan model serta nomor seri/lisensi atau tanda identifikasi lainnya.

1.10 Kondisi bukti elektronik, antara lain komputer dalam keadaan sudah mati/*off* atau masih hidup/*on* berikut tampilan layarnya.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 *Tools* yang digunakan sebagai perangkat deteksi
   2.2 Perlengkapan
      2.2.1 Kamera
      2.2.2 Alat tulis

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan

peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi-tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan pencarian bukti elektronik fisik mandiri (*standalone devices*) di lokasi insiden.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Bukti elektronik

3.1.2 Prosedur dokumentasi bukti elektronik

3.1.3 Informasi awal terjadinya insiden

3.1.4 Aspek legalitas penanganan pertama bukti elektronik

3.2 Keterampilan

3.2.1 Menggunakan *tools* perangkat deteksi

3.2.2 Menggunakan aplikasi pengolah kata

3.2.3 Mengolah data angka pada aplikasi *spreadsheet*

3.2.4 Mengolah grafik presentasi

3.2.5 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai pendokumentasian bukti elektronik fisik di Tempat Kejadian Perkara (TKP)

4. Sikap kerja yang diperlukan

4.1 Teliti dalam mengidentifikasi media penyimpanan elektronik

4.2 Berwawasan luas dalam melaksanakan prosedur umum penanganan pertama bukti elektronik

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertangggung jawab dalam menilai risiko selama proses pencarian sesuai prosedur untuk melindungi keamanan personel dan keutuhan bukti elektronik

5. Aspek kritis

5.1 Ketepatan dalam mengidentifikasi bukti elektronik mandiri (*standalone digital device*) yang tidak terkoneksi ke jaringan beserta peralatan pendukungnya (*peripheral devices*) berdasarkan prosedur

KODE UNIT : **J.62FDG00.003.1**

JUDUL UNIT : **Mencari Bukti Elektronik Fisik yang Terkoneksi ke Jaringan (*Networked Devices*)**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan pencarian dan mendokumentasikan bukti elektronik fisik yang terkoneksi ke jaringan (*networked devices*) di lokasi insiden.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melaksanakan pencarian bukti elektronik fisik yang terkoneksi ke jaringan (*networked devices*) di **lokasi insiden**	1.1 Seluruh **perangkat seluler** diidentifikasi nomor serinya. 1.2 Seluruh **bukti elektronik terkoneksi ke jaringan beserta pendukungnya** diidentifikasi berdasarkan prosedur. 1.3 Perangkat elektronik lain yang terkoneksi dengan jaringan diidentifikasi melalui **perangkat deteksi**.
2. Mendokumentasi bukti elektronik fisik yang terkoneksi ke jaringan (*networked devices*) di lokasi insiden	2.1 **Informasi pendukung** berkaitan dengan insiden didokumentasikan sesuai prosedur dokumentasi. 2.2 Bukti elektronik terkoneksi ke jaringan beserta pendukungnya didokumentasikan sesuai prosedur.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk melaksanakan pencarian dan pendokumentasian bukti elektronik fisik terkoneksi ke jaringan (*networked devices*).
   1.2 Lokasi insiden merupakan lokasi tempat insiden keamanan informasi berlangsung atau Tempat Kejadian Perkara (TKP), di mana bukti elektronik terkait insiden berada.

1.3 Perangkat seluler, yaitu *handphone/smartphone,* berikut *memory card, simcard* dan *charger* serta kotak paketnya dicari dengan teliti.

1.4 Bukti elektronik yang terkoneksi ke jaringan beserta pendukungnya antara lain seperti perangkat seluler, komputer yang terhubung ke jaringan, layanan seluler, layanan internet lain, dan sistem *Closed Circuit Television* (CCTV) yang terhubung ke jaringan beserta jumlah kamera yang terkoneksi.

1.5 Perangkat deteksi adalah *network scanner* yang digunakan untuk mendeteksi dan mengidentifikasi bukti elektronik yang tersembunyi.

1.6 Informasi pendukung adalah informasi lain yang berkaitan dengan insiden pada lokasi di mana bukti elektronik secara fisik yang terkoneksi ke jaringan dicari seperti catatan tempel, diari, jenis, merk, model dan nomor seri dari perangkat elektronik termasuk *setting* konfigurasi dari sistem *Closed Circuit Television* (CCTV).

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 *Tools* yang digunakan sebagai perangkat deteksi

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi-tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan pencarian bukti elektronik fisik yang terkoneksi ke jaringan (*networked devices*) di lokasi insiden.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Bukti elektronik

3.1.2 Prosedur dokumentasi bukti elektronik

3.1.3 Informasi awal terjadinya insiden

3.1.4 Aspek legalitas penanganan pertama bukti elektronik

3.2 Keterampilan

3.2.1 Menggunakan *tools* perangkat deteksi

3.2.2 Menggunakan aplikasi pengolah kata

3.2.3 Mengolah data angka pada aplikasi *spreadsheet*

3.2.4 Mengolah grafik presentasi

3.2.5 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai pendokumentasian bukti elektronik fisik yang terkoneksi ke jaringan (*networked devices*) di lokasi insiden

4. Sikap kerja yang diperlukan

4.1 Teliti dalam mengenali bukti elektronik fisik yang terkoneksi ke jaringan (*networked devices*)

4.2 Berwawasan luas

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertangggung jawab

5. Aspek kritis

5.1 Ketepatan dalam mengidentifikasi seluruh bukti elektronik terkoneksi ke jaringan beserta pendukungnya berdasarkan prosedur

KODE UNIT : **J.62FDG00.004.1**

JUDUL UNIT : **Mengumpulkan Informasi Non-Elektronik**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengenali pihak-pihak yang relevan dengan insiden dan mengumpulkan barang bukti *non*-elektronik.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengenali pihak-pihak yang relevan dengan insiden	1.1 **Pihak yang bertanggung jawab** diidentifikasi untuk kebutuhan penanganan pertama bukti elektronik. 1.2 **Pihak-pihak terkait** didokumentasikan untuk kebutuhan penanganan pertama bukti elektronik.
2. Mengumpulkan barang bukti *non*-elektronik	2.1 Kemungkinan risiko **barang bukti *non*-elektronik** diidentifikasi sesuai kebutuhan penanganan pertama bukti elektronik. 2.2 **Informasi tambahan** didokumentasikan sesuai kebutuhan penanganan pertama bukti elektronik.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk personel dalam mempertimbangkan pengumpulan barang bukti yang bersifat *non-elektronik*.
   1.2 Pihak yang bertanggungjawab, meliputi nama, sebutan dan jabatan serta akses terhadap bukti elektronik di lokasi insiden/Tempat Kejadian Perkara (TKP).
   1.3 Pihak-pihak terkait, meliputi administrator sistem, pemilik dan pengguna komputer, perangkat periferal, s*martphone* dan lain-lain dengan informasi relevan untuk pengumpulan bukti elektronik diidentifikasi untuk diwawancarai.
   1.4 Barang bukti *non*-elektronik antara lain berupa informasi mengenai *password* pengguna/administrator dari bukti

elektronik hingga detil penggunaannya mencakup kapan, di mana dan bagaimana serta siapa saja yang menggunakannya dicari dan digali.

1.5 Informasi tambahan, antara lain konfigurasi sistem dan penggunaan/instalasi aplikasi dicari/dimintakan.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan

konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi-tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan pengumpulan informasi *non*-elektronik.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Bukti *non*-elektronik

3.1.2 Prosedur dokumentasi bukti *non*-elektronik

3.1.3 Informasi awal terjadinya insiden

3.1.4 Aspek legalitas penanganan pertama bukti elektronik

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

3.2.3 Mengolah grafik presentasi

3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai mengenai pendokumentasian barang bukti *non*-elektronik di tempat kejadian perkara

4. Sikap kerja yang diperlukan

4.1 Teliti dalam mengumpulkan barang bukti *non*-elektronik

4.2 Berwawasan luas

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam mengidentifikasi pihak yang bertanggung jawab untuk kebutuhan penanganan pertama bukti elektronik

KODE UNIT : **J.62FDG00.005.1**

JUDUL UNIT : **Memilih Opsi Untuk Koleksi atau Akuisisi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mempertimbangkan volatilitas dan persyaratan lainnya yang relevan, mengidentifikasi pengumpulan atau akuisisi, dan mendokumentasikan rantai ketertelusuran (*chain of custody*).

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mempertimbangkan volatilitas dan persyaratan lainnya yang relevan	1.1 Volatilitas dan nilai pembuktian terkait dari bukti elektronik potensial diidentifikasi sesuai kebutuhan penanganan pertama bukti elektronik untuk mendapatkan bukti terbaik dan mencegah hilangnya/rusaknya data. 1.2 **Kondisi bukti elektronik** diidentifikasi sesuai kebutuhan penanganan pertama bukti elektronik. 1.3 **Persyaratan lain** diidentifikasi dalam memutuskan pengumpulan/koleksi atau akuisisi.
2. Mengidentifikasi pengumpulan atau akuisisi	2.1 **Bukti elektronik fisik atau logik** diidentifikasi sesuai kebutuhan penanganan pertama bukti elektronik. 2.2 Keberadaan **bukti elektronik yang tersembunyi** diidentifikasi sesuai kebutuhan penanganan pertama bukti elektronik. 2.3 Bukti elektronik diklasifikasikan dalam bentuk **data elektronik *volatile*** sampai *non-volatile* (tidak mudah hilang/rusak) sesuai prosedur. 2.4 **Bukti elektronik** diidentifikasi untuk pengumpulan/koleksi sesuai **prosedur pengamanan bukti fisik.**
3. Mendokumentasikan rantai ketertelusuran (*chain of custody*)	3.1 Perolehan dan pengidentifikasian data dan perangkat elektronik didokumentasikan di dalam **rantai ketertelusuran (*chain of custody*)** sesuai prosedur**.**

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
	3.2 **Rekaman rantai ketertelusuran (*chain of custody recorder*)**, dijaga keutuhannya secara berkesinambungan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk personel dalam melaksanakan proses pemilihan opsi untuk melakukan koleksi atau akuisisi.
   1.2 Kondisi bukti elektronik dalam hal ini adalah kondisi enkripsi *full disk* atau volume dalam keadaan terbuka (*mounted*) dan *passphrase* tersimpan di *Random Access Memory* (RAM).
   1.3 Persyaratan lain, seperti: legalitas dan sumber daya media penyimpanan serta ketersediaan personel.
   1.4 Bukti elektronik fisik, misalnya media penyimpanan elektronik dan perangkat pemrosesannya, seperti: komputer dan *smartphone*, sedangkan bukti elektronik logik misalnya berupa data elektronik.
   1.5 Bukti elektronik yang tersembunyi, antara lain: media penyimpanan elektronik berupa *cloud computing*, *Network Attached Storage* (NAS) dan *Storage Area Network* (SAN), termasuk yang berukuran kecil sehingga tidak terlihat/terabaikan.
   1.6 Data elektronik *volatile,* berupa data elektronik yang mudah sekali rusak/hilang pada kondisi tertentu, antara lain memori RAM, kontainer/volume enkripsi yang sudah dalam keadaan terdekripsi (*mounted*), proses yang sedang berjalan, koneksi jaringan dan *setting* tanggal/waktu serta informasi berharga lainnya, yang diprioritaskan terlebih dahulu.
   1.7 Bukti elektronik, seperti: media penyimpanan elektronik dan sistem *Closed Circuit Television* (CCTV).
   1.8 Prosedur pengamanan bukti fisik termasuk pengumpulan/koleksi perangkat elektronik yang mungkin

terdapat bukti fisik, seperti: sidik jari dan *Deoxyribonucleic Acid* (DNA) yang harus diperlakukan dengan hati-hati untuk mencegah rusaknya bukti fisik tersebut.

1.9 Rantai ketertelusuran (*chain of custody*) mencakup antara lain: identifikasi unik bukti elektronik fisik/logik, siapa yang mengaksesnya dilengkapi periode waktunya, dan mengapa/apa yang dilakukan terhadap bukti tersebut.

1.10 Rekaman rantai ketertelusuran (*chain of custody*), baik dalam bentuk data elektronik maupun catatan kertas untuk identifikasi dan kronologi pergerakan dan penanganan pertama bukti elektronik dari proses identifikasi, pengumpulan/koleksi dan akuisisi serta preservasi hingga status terkininya.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 *Tools* untuk melaksanakan proses pemilihan opsi untuk koleksi dan akuisisi

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan pemilihan opsi untuk koleksi atau akuisisi.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Bukti elektronik dalam bentuk fisik

3.1.2 Bukti elektronik yang tersembunyi

3.1.3 Data elektronik *volatile*

3.1.4 Prosedur pengamanan bukti fisik

3.1.5 Rantai ketertelusuran (*chain of custody*)

3.1.6 Proses pemilihan opsi untuk pengumpulan dan akuisisi sesuai Gambar 1 dari SNI ISO/IEC 27037:2014

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

3.2.3 Mengolah grafik presentasi

3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai proses pemilihan opsi untuk pengumpulan dan akuisisi

4. Sikap kerja yang diperlukan

4.1 Teliti dalam mengidentifikasi data elektronik volatile

4.2 Berwawasan luas

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam mengidentifikasi keberadaan bukti elektronik yang tersembunyi sesuai kebutuhan penanganan pertama bukti elektronik

KODE UNIT : **J.62FDG00.006.1**

JUDUL UNIT : **Mengumpulkan Bukti Elektronik dalam Kondisi Masih Hidup/*On***

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengumpulkan bukti elektronik dengan prosedur *baseline* untuk seluruh kondisi dan mengumpulkan bukti elektronik *additional* untuk kondisi tertentu dalam kondisi masih hidup/*on.*

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengumpulkan **bukti elektronik** dengan prosedur *baseline* untuk seluruh kondisi	1.1 Pengumpulan bukti elektronik dalam kondisi hidup/*on* dilaksanakan dengan pertimbangan ***baseline***. 1.2 Pertimbangan untuk akuisisi **data *volatile*** dilaksanakan sesuai prosedur. 1.3 Bukti elektronik dimatikan sesuai **prosedur.** 1.4 **Pelabelan** bukti elektronik dilaksanakan sesuai dengan prosedur.
2. Mengumpulkan bukti elektronik *additional* untuk kondisi tertentu	2.1 Pengumpulan bukti elektronik dalam kondisi hidup/*on* dilaksanakan dengan pertimbangan ***additional***. 2.2 Bukti elektronik *laptop* dimatikan setelah akuisisi data *volatile* sesuai prosedur. 2.3 ***Slot*** **media penyimpanan eksternal** disegel sesuai prosedur untuk mencegah penggunaannya.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Bukti elektronik adalah sistem, perangkat, dan/atau media penyimpanan elektronik yang berpotensi terdapat informasi elektronik dan/atau dokumen elektronik yang dapat diandalkan sebagai alat bukti.
   1.2 *Baseline*, berlaku untuk seluruh kasus/insiden.

1.3 *Additional*/tambahan, hanya berlaku pada kasus/insiden tertentu yang relevan.

1.4 Data *volatile* adalah data elektronik yang mudah sekali rusak/hilang pada kondisi tertentu, antara lain memori *Random Access Memory* (RAM), kontainer/volume enkripsi yang sudah dalam keadaan terdekripsi (*mounted*), proses yang sedang berjalan, koneksi jaringan dan setting tanggal/waktu serta informasi berharga lainnya.

1.5 Pelabelan termasuk *port*, diskoneksi dan pengamanan seluruh kabel dari bukti elektronik baik untuk memudahkan rekonstruksi.

1.6 *Slot* media penyimpanan eksternal*, meliputi: slot floppy disk*, *slot* CD/DVD dan/atau *slot* lain yang memiliki potensi sama dalam penggunaannya.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 *Tools* untuk melaksanakan pengumpulan bukti elektronik dalam kondisi masih hidup/*on*

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan, meliputi kombinasi metode tes lisan, tes tertulis, observasi-tempat kerja/ demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan pengumpulan bukti elektronik dalam kondisi masih hidup/*on*.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Bukti elektronik

3.1.2 Prosedur penanganan pertama bukti elektronik

3.1.3 Informasi awal terjadinya insiden

3.1.4 Aspek legalitas penanganan pertama bukti elektronik

3.1.5 Pemahaman dan pelaksanaan Gambar 2 dari ISO/IEC 27037:2012 tentang panduan koleksi bukti elektronik dalam kondisi masih hidup/*on*

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

3.2.3 Mengolah grafik presentasi

3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai pengumpulan bukti elektronik dalam kondisi masih hidup/*on*

4. Sikap kerja yang diperlukan

4.1 Teliti dalam mempertimbangkan untuk akuisisi data *volatile*

4.2 Berwawasan luas

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam melaksanakan pengumpulan bukti elektronik dalam kondisi masih hidup/*on* dengan pertimbangan *baseline*

KODE UNIT : **J.62FDG00.007.1**

JUDUL UNIT : **Mengumpulkan Bukti Elektronik dalam Kondisi Sudah Mati/*Off***

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengumpulkan bukti elektronik dengan prosedur *baseline* untuk seluruh kondisi dan mengumpulkan bukti elektronik *additional* untuk kondisi tertentu dalam kondisi sudah mati/*off*.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengumpulkan bukti elektronik dengan prosedur *baseline* untuk seluruh kondisi	1.1 Pengumpulan **bukti elektronik** dalam kondisi mati/*off* dilakukan dengan pertimbangan ***baseline*** sesuai prosedur. 1.2 Pertimbangan untuk akuisisi **data *non-volatile*** dilaksanakan sesuai prosedur. 1.3 **Pelabelan** bukti elektronik dilaksanakan sesuai dengan prosedur.
2. Mengumpulkan bukti elektronik *additional* untuk kondisi tertentu	2.1 Pengumpulan **bukti elektronik** dalam kondisi mati/*off* dilakukan dengan pertimbangan ***additional*** sesuai prosedur. 2.2 Validasi bukti elektronik *laptop* dalam keadaan mati/*off* dilaksanakan sesuai prosedur. 2.3 Pertimbangan efek listrik statik dalam pelepasan bukti elektronik *harddisk* dilaksanakan sesuai prosedur.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Bukti elektronik adalah sistem, perangkat, dan/atau media penyimpanan elektronik yang berpotensi terdapat informasi elektronik dan/atau dokumen elektronik yang dapat diandalkan sebagai alat bukti.
   1.2 *Baseline*, berlaku untuk seluruh kasus/insiden.

1.3 *Additional*/tambahan, hanya berlaku pada kasus/insiden tertentu yang relevan.

1.4 Data *non-volatile* adalah data elektronik yang tidak mudah rusak/hilang meskipun komputer atau perangkat elektronik sudah dimatikan, antara lain data *intact* (yang masih ada dan terlihat), *deleted* (yang sudah dihapus) dan *lost* (yang sudah hilang dan tidak tercatat di dalam *file system*, meskipun masih ada di sektor fisik penyimpanannya).

1.5 Pelabelan termasuk *port*, diskoneksi dan pengamanan seluruh kabel dari bukti elektronik baik untuk memudahkan rekonstruksi.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 *Tools* yang digunakan untuk melaksanakan pengumpulan bukti elektronik dalam kondisi sudah mati/*off*

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi-tempat kerja/ demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.
   1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan pengumpulan bukti elektronik dalam kondisi sudah mati/*off*.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Bukti elektronik
      3.1.2 Prosedur penanganan pertama bukti elektronik
      3.1.3 Informasi awal terjadinya insiden
      3.1.4 Aspek legalitas penanganan pertama bukti elektronik
      3.1.5 Pemahaman dan pelaksanaan Gambar 3 dari ISO/IEC 27037:2012 untuk pengumpulan/koleksi bukti elektronik dalam kondisi sudah mati/*off*
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah kata
      3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

3.2.3 Mengolah grafik presentasi

3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai pengumpulan buktis elektronik dalam kondisi sudah mati/*off*

4. Sikap kerja yang diperlukan

4.1 Teliti dalam mengidentifikasi data *non-volatile*

4.2 Berwawasan luas

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab

5. Aspek kritis

5.1 Ketepatan dalam melakukan pengumpulan bukti elektronik dalam kondisi mati/*off* dengan pertimbangan *baseline* sesuai prosedur

KODE UNIT : **J.62FDG00.008.1**

JUDUL UNIT : **Mengumpulkan Bukti Elektronik yang Terkoneksi ke Jaringan (*Networked Devices*)**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam memutuskan diskoneksi dan pelacakan koneksi, dan menangani perangkat seluler.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memutuskan diskoneksi bukti elektronik yang terkoneksi ke jaringan (*networked devices)*	1.1 Tindakan diskoneksi **bukti elektronik** terkoneksi ke jaringan (*networked devices)* dilaksanakan sesuai prosedur. 1.2 Pengisolasian koneksi bukti elektronik terkoneksi ke jaringan (*networked devices*) dilaksanakan sesuai prosedur untuk mencegah terjadinya malfungsi. 1.3 Pelacakan koneksi bukti elektronik terkoneksi ke jaringan (*networked devices)* dilaksanakan sesuai prosedur. 1.4 Pelabelan *ports* dilaksanakan sesuai prosedur.
2. Menangani perangkat seluler	2.1 ***Data volatile*** diidentifikasi sesuai prosedur dalam pelepasan sumber daya listrik. 2.2 Tindakan perlindungan bukti elektronik **perangkat seluler** dilaksanakan sesuai prosedur. 2.3 Tindakan mematikan perangkat seluler dilaksanakan sesuai prosedur.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Bukti elektronik adalah sistem, perangkat, dan/atau media penyimpanan elektronik yang berpotensi terdapat informasi elektronik dan/atau dokumen elektronik yang dapat diandalkan sebagai alat bukti.

1.2 Data *volatile* adalah data elektronik yang mudah sekali rusak/hilang pada kondisi tertentu, antara lain memori *Random Access Memory* (RAM), kontainer/volume enkripsi yang sudah dalam keadaan terdekripsi (*mounted*), proses yang sedang berjalan, koneksi jaringan dan setting tanggal/waktu serta informasi berharga lainnya.

1.3 Perangkat seluler yaitu *handphone/smartphone,* berikut *memory card, simcard* dan *charger* serta kotak paketnya dicari dengan teliti.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 *Tools* untuk membungkus, menyegel dan melabeli perangkat seluler, misalnya kantong *Faraday* atau kotak yang terlindungi

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/ demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.
   1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan pengumpulan bukti elektronik yang terkoneksi ke jaringan (*networked devices*).

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Pengumpulan bukti elektronik yang terkoneksi ke jaringan (*networked devices*)
      3.1.2 Bukti elektronik
      3.1.3 Prosedur penanganan pertama bukti elektronik
      3.1.4 Informasi awal terjadinya insiden
      3.1.5 Aspek legalitas penanganan pertama bukti elektronik
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah kata
      3.2.2 Mengolah data angka pada aplikasi *spreadsheet*
      3.2.3 Mengolah grafik presentasi

3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai pengumpulan bukti digital yang terkoneksi ke jaringan (*networked devices*)

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam memutuskan diskoneksi bukti elektronik yang terkoneksi ke jaringan (*networked devices)*
   4.2 Berwawasan luas
   4.3 Cara berpikir sistematis dan *teamwork*
   4.4 Bertanggung jawab

5. Aspek Kritis
   5.1 Kesesuaian dalam melaksanakan pengisolasian koneksi bukti elektronik yang terkoneksi ke jaringan (*networked devices*) dilaksanakan sesuai prosedur untuk mencegah terjadinya malfungsi

KODE UNIT : **J.62FDG00.009.1**

JUDUL UNIT : **Mengumpulkan Bukti Elektronik dari Sistem *Closed Circuit Television* (CCTV)**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menggali informasi sistem CCTV, dan menentukan pemenuhan prasyarat pengumpulan sistem CCTV.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menggali informasi sistem CCTV	1.1 Penentuan proses ekstraksi data elektronik rekaman video **sistem *Digital Video Recorder* (DVR) CCTV** dilaksanakan sesuai prosedur. 1.2 Koreksi waktu lokal sesungguhnya dilaksanakan untuk penentuan jangka waktu rekaman video sesuai prosedur. 1.3 Seluruh **kamera CCTV** yang hidup (aktif merekam) dan yang mati (tidak merekam) diidentifikasi sesuai prosedur. 1.4 **Informasi** dan waktu yang relevan dengan kejadian atau insiden diidentifikasi untuk penentuan bukti elektronik (kamera CCTV yang memuat rekaman kejadian) sesuai prosedur. 1.5 Dokumentasi merk, model, instalasi dan penggunaan sistem CCTV dilaksanakan secara menyeluruh sesuai prosedur.
2. Menentukan pemenuhan prasyarat pengumpulan sistem CCTV	2.1 Pengumpulan dan pendokumentasian **media penyimpanan elektronik** dilaksanakan sesuai prosedur. 2.2 Pemenuhan aspek **legalitas sistem CCTV** dalam pelepasannya dari lokasi dilaksanakan sesuai prosedur. 2.3 **Kompleksitas sistem CCTV** dalam pelepasannya dari lokasi diidentifikasi sesuai prosedur.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk personel yang melaksanakan pengumpulan bukti elektronik dari sistem CCTV.
   1.2 Sistem DVR CCTV yang berbasis komputer atau tertanam (*embedded*) dipahami dengan mempertimbangkan perbedaan ekstraksi data elektronik dari komputer secara konvensional.
   1.3 Kamera CCTV yang memuat rekaman kejadian dilaksanakan dengan mempertimbangkan informasi dan waktu yang relevan dengan kejadian atau insiden tersebut.
   1.4 Informasi tentang ukuran besarnya media penyimpanan dan berapa lama rekaman video bertahan di dalam sistem sebelum tertimpa/hilang.
   1.5 Media penyimpanan elektronik, yaitu: *harddisk* dilaksanakan dengan mempertimbangkan kompatibilitas *harddisk* tersebut dengan sistem CCTV lain.
   1.6 Legalitas dan kompleksitas sistem CCTV untuk kondisi tertentu, pengumpulan dan pendokumentasian seluruh sistem CCTV yang dilepas dari lokasinya dilaksanakan dengan mempertimbangkan kompleksitas sistem dan pemeriksaan lanjutan di Laboratorium Forensik serta pertimbangan aspek legalitas.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Media penyimpanan elektronik
      2.1.3 Tools untuk melakukan pengumpulan bukti elektronik dari sistem CCTV
   2.2 Perlengkapan
      2.2.1 Kamera
      2.2.2 Alat tulis

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

   4.1 Norma

   (Tidak Ada.)

   4.2 Standar

   4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

   1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan pengumpulan bukti elektronik dari sistem CCTV.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
    3.1 Pengetahuan
        3.1.1 Pengumpulan bukti elektronik dari sistem CCTV
        3.1.2 Bukti elektronik
        3.1.3 Prosedur penanganan pertama bukti elektronik
        3.1.4 Informasi awal terjadinya insiden
        3.1.5 Aspek legalitas penanganan pertama bukti elektronik
    3.2 Keterampilan
        3.2.1 Menggunakan aplikasi pengolah kata
        3.2.2 Mengolah data angka pada aplikasi *spreadsheet*
        3.2.3 Mengolah grafik presentasi
        3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai pengumpulan bukti elektronik dari sistem CCTV

4. Sikap kerja yang diperlukan
    4.1 Teliti dalam proses ekstraksi data elektronik rekaman video sistem DVR CCTV
    4.2 Wawasan luas
    4.3 Cara berpikir sistematis dan terstruktur
    4.4 Bertanggung jawab

5. Aspek Kritis
    5.1 Ketepatan dalam mengidentifikasi seluruh kamera CCTV yang hidup (aktif merekam) dan yang mati (tidak merekam) diidentifikasi sesuai prosedur

KODE UNIT : **J.62FGD00.010.1**

JUDUL UNIT : **Menyalin Data Elektronik dari Bukti Elektronik Dalam Kondisi Masih Hidup/*On***

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan akuisisi secara *baseline* untuk seluruh kondisi, dan melakukan akuisisi secara *additional*/tambahan untuk kondisi tertentu.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melaksanakan akuisisi secara *baseline* untuk seluruh kondisi	1.1 Akuisisi terhadap data elektronik disalin secara fisik *bit-per-bit*, maupun logik *non-bit-per-bit*. 1.2 ***Image file*** hasil akuisisi fisik diverifikasi dengan fungsi *hash* atau fungsi lain yang setara. 1.3 Tindakan lanjutan pada mode *screen saver* atau *autolock diidentifikasi* sesuai prosedur. 1.4 *Image file* hasil akuisisi terhadap ***volatile data*** dan ***non-volatile data*** diperoleh sesuai prosedur. 1.5 Penggunaan *tools*/aplikasi akuisisi dipilih sesuai dengan **pertimbangan perubahan data**. 1.6 Kontainer *file* logik hasil akuisisi *data volatile*, maupun *non-volatile* diverifikasi dengan fungsi *hash*. 1.7 Media penyimpanan *image file*, maupun kontainer *file* logik **disiapkan khusus**.
2. Melakukan akuisisi secara *additional*/tambahan untuk kondisi tertentu	2.1 *Image file* hasil akuisisi dari data *volatile* di memori *Random Access Memory* (RAM) dihasilkan sesuai prosedur. 2.2 Pemilihan opsi pelaksanaan akuisisi ditentukan sesuai dengan **kondisi**. 2.3 Dokumentasi untuk pemilihan opsi akuisisi dibuat sesuai prosedur.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Salinan data elektronik atau *image file* secara ideal yang menghasilkan 2 *copy*, yaitu: *master* dan *working*/pemeriksaan, dipahami sebagai pilihan.
   1.2 *Volatile data* dipertimbangkan terlebih dahulu untuk proses akuisisi, setelah itu *non-volatile* data.
   1.3 Pelabelan adalah pemberian nomor urut bukti elektronik yang dilengkapi dengan skala ukur dan dokumentasi identitasnya.
   1.4 Proses akuisisi secara *live*/langsung melalui *console*/perangkat khusus atau *remote* melalui jaringan dilaksanakan dengan pertimbangan data, efektifitas dan efisiensi waktu.
   1.5 Aplikasi *static-binaries* bersifat independen yang penggunaannya terpisah dari sistem bukti elektronik.
   1.6 Akibat yang mungkin ditimbulkan terhadap bukti elektronik dari penggunaan aplikasi akuisisi didokumentasikan secara menyeluruh.
   1.7 Disiapkan khusus artinya media penyimpanan elektronik yang baru atau sudah tersanitasi dengan baik.
   1.8 Kondisi maksudnya adalah sumber daya personel, peralatan dan waktu yang ada, serta kompleksitas insiden dan kuantitas bukti elektronik yang sedang ditangani.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Media penyimpanan elektronik
      2.1.3 *Tools* yang digunakan untuk akuisisi bukti elektronik dalam kondisi masih hidup/*on*
      2.1.4 *Tools* yang digunakan untuk verifikasi fungsi *hash* atau fungsi lain yang setara

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan akuisisi bukti elektronik dalam kondisi masih hidup/*on*.

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Informasi awal terjadinya insiden
      3.1.2 Bukti elektronik
      3.1.3 Prosedur penanganan pertama bukti elektronik
      3.1.4 Aspek legalitas penanganan pertama bukti elektronik
      3.1.5 Akuisisi bukti elektronik dalam kondisi masih hidup/*on*
      3.1.6 *Forensic imaging*
      3.1.7 *Image file*
      3.1.8 Kontainer *file* logik
      3.1.9 *Hash*
      3.1.10 *Chain of custody*
      3.1.11 *Volatile*
      3.1.12 Pemahaman dan pelaksanaan Gambar 4 dari ISO/IEC 27037:2012 tentang akuisisi bukti elektronik dalam keadaan masih hidup/*on*
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi untuk akuisisi bukti elektronik dalam keadaan masih hidup/*on*
      3.2.2 Menggunakan aplikasi untuk verifikasi fungsi *hash*
      3.2.3 Mencari data/informasi dari bukti elektronik dan mendokumentasikan proses akuisisinya dalam *chain of custody*
      3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai proses akuisisi bukti elektronik dalam kondisi masih hidup/*on*

4. Sikap kerja yang diperlukan
    4.1 Teliti dalam proses akuisisi terhadap data elektronik secara fisik *bit-per-bit*, maupun logik non-*bit-per-bit*
    4.2 Berwawasan luas dalam memilih penggunaan tools/aplikasi akuisisi sesuai dengan pertimbangan perubahan data
    4.3 Cara berpikir sistematis dan *teamwork*
    4.4 Bertanggung jawab dalam membuat dokumentasi untuk pemilihan opsi akuisisi sesuai prosedur

5. Aspek Kritis
    5.1 Ketepatan dalam memverifikasi *image file* hasil akuisisi fisik dengan fungsi *hash* atau fungsi lain yang setara

KODE UNIT : **J.62FDG00.011.1**

JUDUL UNIT : **Menyalin Data Elektronik dari Bukti Elektronik Dalam Kondisi Sudah Mati/*Off***

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mempersiapkan akuisisi, dan melaksanakan proses akuisisi terhadap bukti elektronik dalam kondisi sudah mati/*off*.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mempersiapkan akuisisi terhadap bukti elektronik dalam kondisi sudah mati/*off*	1.1 Penyalinan data elektronik dari bukti elektronik dalam kondisi sudah mati/*off* dilaksanakan tanpa mempertimbangkan keberadaan data *volatile*. 1.2 Pengecekan kepastian kondisi bukti elektronik dalam kondisi sudah mati/off dilaksanakan sesuai prosedur. 1.3 Pelepasan media penyimpanan dari bukti elektronik dan pendokumentasian **identitasnya** dilaksanakan sesuai prosedur. 1.4 Untuk kasus media penyimpanan yang tidak dapat dilepas dari **bukti elektronik**, proses *imaging* dilaksanakan sesuai prosedur. 1.5 Pemasangan ***write-protect*** dilaksanakan sesuai prosedur.
2. Melaksanakan proses akuisisi terhadap bukti elektronik dalam kondisi sudah mati/*off*	2.1 Proses ***imaging*** pada komputer/ perangkat khusus dengan *tools*/aplikasi yang tervalidasi, dilaksanakan sesuai prosedur. 2.2 Pengecekan salinan data elektronik atau *image file* yang dihasilkan dari proses akuisisi dilaksanakan dengan fungsi verifikasi *hash* atau fungsi lain yang setara. 2.3 Penyimpanan salinan data elektronik atau *image file* dilaksanakan secara aman dan sesuai prosedur. 2.4 Pembuatan **salinan data elektronik atau *image file*** dilaksanakan sesuai kebutuhan investigasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Identitasnya, antara lain: merk, model, nomor seri dan besarnya ukuran, serta pihak yang memilikinya.
   1.2 Bukti elektronik, misalnya komputer/*laptop* dengan *chipset* terkini dapat dijalankan sebagai *removable* media untuk proses *imaging*.
   1.3 *Write-protect* dalam bentuk perangkat keras (*hardware*) maupun perangkat lunak (*software*) dipasang terlebih dahulu pada komputer/perangkat akuisisi, sebelum dilakukannya proses akuisisi, untuk mencegah terjadinya perubahan data elektronik.
   1.4 *Imaging* dilaksanakan secara fisik *bit-per-bit* terhadap media penyimpanan dari bukti elektronik dan menghasilkan *image file* yang identik melalui verifikasi fungsi *hash* atau fungsi lain yang setara.
   1.5 Salinan data elektronik atau *image file* secara ideal yang menghasilkan 2 *copy*, yaitu: *master* dan *working*/pemeriksaan dipahami sebagai pilihan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Media penyimpanan elektronik
      2.1.3 *Tools* yang digunakan untuk akuisisi bukti elektronik dalam kondisi sudah mati/*off*
      2.1.4 *Tools* yang digunakan untuk verifikasi fungsi *hash* atau fungsi lain yang setara
      2.1.5 *Tools* yang digunakan untuk *write-protect* guna menjaga keutuhan data elektronik dari perubahan data
   2.2 Perlengkapan
      2.2.1 Kamera
      2.2.2 Alat tulis

3. Peraturan yang diperlukan

   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

   4.1 Norma

   (Tidak Ada.)

   4.2 Standar

   4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

   1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan akuisisi bukti elektronik dalam kondisi sudah mati/*off*.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Informasi awal terjadinya insiden

3.1.2 Bukti elektronik

3.1.3 Prosedur penanganan pertama bukti elektronik

3.1.4 Aspek legalitas penanganan pertama bukti elektronik

3.1.5 Akuisisi bukti elektronik dalam kondisi sudah mati/*off*

3.1.6 *Forensic imaging*

3.1.7 *Image file*

3.1.8 *Write Protect*

3.1.9 *Hash*

3.1.10 *Chain of custody*

3.1.11 *Volatile*

3.1.12 Pemahaman dan pelaksanaan Gambar 5 dari ISO/IEC 27037:2012 tentang akuisisi bukti elektronik dalam keadaan sudah mati/*off*

3.2 Keterampilan

3.2.1 Menggunakan aplikasi untuk akuisisi bukti elektronik dalam keadaan sudah mati/*off*

3.2.2 Menggunakan aplikasi untuk verifikasi fungsi *hash*

3.2.3 Menggunakan perangkat keras (*hardware*) atau perangkat lunak (*software*) untuk *write-protect*

3.2.4 Mencari data/informasi tentang identitas bukti elektronik dan mendokumentasikan proses akuisisi-nya dalam *chain of custody*

3.2.5 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai proses akuisisi bukti elektronik dalam kondisi sudah mati/*off*

4. Sikap kerja yang diperlukan

4.1 Teliti dalam pengecekan salinan data elektronik atau *image file* yang dihasilkan dari proses akuisisi dilaksanakan dengan fungsi verifikasi *hash* atau fungsi lain yang setara

4.2 Berwawasan luas

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab

5. Aspek Kritis

5.1 Ketepatan dalam melaksanakan pemasangan *write-protect* sesuai prosedur

KODE UNIT : **J.62FDG00.012.1**

JUDUL UNIT : **Menyalin Data Elektronik dari Bukti Elektronik yang Terkoneksi ke Jaringan (*Networked Devices*)**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mempersiapkan akuisisi, dan melaksanakan proses akuisisi dari bukti elektronik yang terkoneksi ke jaringan (*networked devices*).

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mempersiapkan akuisisi terhadap bukti elektronik yang terkoneksi ke jaringan (*networked devices*)	1.1 Pemutusan koneksi bukti elektronik dari jaringan dilaksanakan sesuai prosedur dengan mempertimbangkan kemungkinan **lebih dari satu koneksi**. 1.2 Pelaksanaan akuisisi logik terhadap data koneksi jaringan dilakukan sesuai prosedur dengan memperhatikan **konfigurasi jaringan**. 1.3 Perlindungan terhadap bukti elektronik yang terkoneksi ke jaringan (*networked devices*) dilaksanakan dengan mencegahnya berinteraksi dengan jaringan radio nirkabel (jaringan seluler). 1.4 Metode isolasi jaringan dilaksanakan sesuai prosedur dengan mempertimbangkan penggunaan perangkat ***jamming***, ***shielding*** dan ***mimic simcard***.
2. Melaksanakan proses akuisisi terhadap bukti elektronik yang terkoneksi ke jaringan (*networked devices*)	2.1 Akuisisi secara *live*/langsung terhadap perangkat seluler dilaksanakan sesuai prosedur dengan pertimbangan **data *volatile seluler***. 2.2 Akuisisi perangkat seluler dilaksanakan sesuai **prosedur ekstraksi**. 2.3 *Simcard* yang diproteksi *Personal Identification Number* (PIN) atau *Personal Unblocking Key* (PUK) diakuisisi bersamaan dengan perangkat selulernya dengan pertimbangan efisiensi waktu.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
	2.4 Pelaksanaan akuisisi perangkat yang terkoneksi ke jaringan (*networked devices*) dilakukan dengan memperhatikan regulasi dan peraturan hukum yang berlaku.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Lebih dari satu koneksi, antara lain: melalui *Virtual Private Network* (VPN) dan *virtual machine.*
   1.2 Konfigurasi jaringan, antara lain: alamat *Internet Protokol* (IP) lokal dan publik, kartu antarmuka jaringan (*Network Interface Card/*NIC) dan *routing tables.*
   1.3 Perangkat *jamming* adalah untuk mengacak/memblok frekuensi radio.
   1.4 *Shielding*, misalnya kantong *faraday*.
   1.5 *Mimic simcard* adalah *simcard* khusus tanpa akses jaringan seluler.
   1.6 Data *volatile* seluler, yaitu pada perangkat seluler sebelum pelepasan *batere* dipertimbangkan dalam proses akuisisi untuk mencegah hilangnya informasi penting potensial yang tersimpan di dalam memori *Random Access Memory* (RAM).
   1.7 Prosedur ekstraksi, maksudnya ekstraksi data elektronik dari perangkat seluler, yang didasarkan pada 3 jenis ekstraksi, yaitu ekstraksi logik (*logical*), ekstraksi *file system* dan ekstraksi fisik (*physical*), yang mana pemilihan jenis ekstraksi tersebut disesuaikan dengan kondisi, waktu dan sumber daya.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 Media penyimpanan elektronik

2.2.3 *Tools* yang digunakan untuk akuisisi bukti elektronik yang terkoneksi ke jaringan (*networked devices*)

2.1.3 *Tools* yang digunakan untuk verifikasi fungsi *hash* atau fungsi lain yang setara

2.1.4 *Tools* yang digunakan untuk *write-protect* guna menjaga keutuhan data elektronik dari perubahan data

2.1.5 *Tools* yang digunakan untuk ekstraksi data elektronik dari perangkat seluler

2.1.6 Kantong *faraday*

2.1.7 Perangkat *jamming*

2.1.8 *Mimic simcard*

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan akuisisi bukti elektronik yang terkoneksi ke jaringan (*networked devices*).

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Informasi awal terjadinya insiden

3.1.2 Bukti elektronik

3.1.3 Prosedur penanganan pertama bukti elektronik

3.1.4 Aspek legalitas penanganan pertama bukti elektronik

3.1.5 Akuisisi bukti elektronik yang terkoneksi ke jaringan (*networked devices*)

3.1.6 *Imaging*

3.1.7 Ekstraksi perangkat seluler

3.1.8 *Image file*

3.1.9 *Hash*

3.1.10 *Chain of custody*

3.1.11 *Volatile*

3.2 Keterampilan

3.2.1 Menggunakan aplikasi untuk akuisisi bukti elektronik yang terkoneksi ke jaringan (*networked devices*)

3.2.2 Menggunakan aplikasi untuk ekstraksi perangkat seluler

3.2.3 Menggunakan aplikasi untuk verifikasi fungsi *hash*

3.2.4 Menggunakan perangkat keras (*hardware*) atau perangkat lunak (*software*) untuk *write-protect*

3.2.5 Mencari data/informasi dari bukti elektronik dan mendokumentasikan proses akuisisi-nya dalam *chain of custody*

3.2.6 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai proses akuisisi bukti elektronik yang terkoneksi ke jaringan (*networked devices*)

4. Sikap kerja yang diperlukan

4.1 Teliti dalam pemutusan koneksi bukti elektronik dari jaringan

4.2 Berwawasan luas

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab

5. Aspek Kritis

5.1 Ketepatan dalam melaksanakan akuisisi perangkat seluler sesuai prosedur ekstraksi

KODE UNIT : **J.62FDG00.013.1**

JUDUL UNIT : **Menyalin Data Elektronik dari Sistem *Closed Circuit Television* (CCTV)**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan akuisisi dan melakukan akuisisi alternatif terhadap bukti elektronik sistem CCTV.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan akuisisi terhadap bukti elektronik sistem CCTV	1.1 Akuisisi terhadap bukti elektronik sistem CCTV dilaksanakan dengan mempertimbangkan penggunaan *write protect* untuk mencegah berubahnya data rekaman. 1.2 Akuisisi data elektronik rekaman video dari sistem CCTV dilaksanakan dengan menuliskannya (*writing*) ke keping CD/DVD/*Bluray* atau ke media penyimpanan elektronik eksternal. 1.3 Akuisisi data elektronik rekaman video dari sistem CCTV dilaksanakan melalui koneksi jaringan dengan pertimbangan sistem CCTV tersebut dilengkapi dengan *port* jaringan. 1.4 Penggunaan **media penyimpanan elektronik** dilaksanakan dengan mempertimbangkannya sebagai *master copy*. 1.5 Akuisisi data elektronik rekaman video dari sistem CCTV dilaksanakan dengan memprioritaskan **format original** yang tidak terkompresi sebagai pilihan utama. 1.6 Penggunaan **format kompresi** dilaksanakan dengan pertimbangan sebagai langkah terakhir.
2. Melakukan akuisisi alternatif terhadap bukti elektronik sistem CCTV	2.1 Pada **kondisi tertentu**, akuisisi dilaksanakan secara analog melalui *port* output-nya di perangkat sistem CCTV. 2.2 Pada **kondisi tertentu** alternatif lain akuisisi dilaksanakan terhadap media

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
	penyimpanan elektronik (yaitu *harddisk*) dari sistem CCTV sesuai **prosedur khusus**. 2.3 Pada **kondisi tertentu** alternatif lain akuisisi dilaksanakan dengan menjalankan rekaman yang diinginkan (sesuai kebutuhan investigasi) sambil **direkam khusus**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Media penyimpanan elektronik, seperti perangkat USB *disk* atau *memory card* yang sudah tersanitasi dengan baik atau dalam kondisi baru, untuk menyimpan file rekaman video hasil proses akuisisi.
   1.2 Format original, adalah format khusus yang hanya bisa dijalankan oleh *player*/aplikasi tertentu/bawaannya, dan belum tentu *compatible*/sesuai dengan *player*/aplikasi lain.
   1.3 Format kompresi dalam bentuk *Motion Picture Expert Group* (MPEG) atau *Audio Video Interleave* (AVI) melalui fitur ekspor di sistem CCTV mengurangi detail tertentu.
   1.4 Kondisi tertentu yaitu yang tidak memungkinkan untuk akuisisi file rekaman melalui fitur ekspor/ekstrak di sistem CCTV.
   1.5 Prosedur khusus, dengan bantuan aplikasi khusus yang dapat membaca rekaman video dan statusnya (masih ada atau sudah terhapus) dari seluruh kamera/*channel* dalam rentang waktu tertentu dan penggunaan *write-protect* untuk mencegah perubahan data rekaman.
   1.6 Direkam khusus artinya menggunakan aplikasi tertentu untuk merekam rekaman video yang sedang diputar secara *live*/langsung.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 Media penyimpanan elektronik

2.1.3 *Tools* yang digunakan untuk akuisisi data elektronik dari sistem CCTV

2.1.4 *Tools* yang digunakan untuk verifikasi fungsi *hash* atau fungsi lain yang setara

2.1.5 *Tools* yang digunakan untuk *write-protect* guna menjaga keutuhan data elektronik dari perubahan data

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan akuisisi data elektronik dari sistem CCTV.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Informasi awal terjadinya insiden

3.1.2 Bukti elektronik

3.1.3 Prosedur penanganan pertama bukti elektronik

3.1.4 Aspek legalitas penanganan pertama bukti elektronik

3.1.5 Akuisisi data elektronik dari sistem CCTV

3.1.6 *Forensic imaging*

3.1.7 Ekstraksi logik (*logical*)

3.1.8 *Image file*

3.1.9 *Hash*

3.1.10 *Chain of custody*

3.1.11 *Volatile*

3.1.12 Format dan retensi rekaman

3.2 Keterampilan

3.2.1 Menggunakan aplikasi untuk akuisisi data elektronik dari sistem CCTV

3.2.2 Menggunakan aplikasi untuk verifikasi fungsi *hash*

3.2.3 Menggunakan perangkat keras (*hardware*) atau perangkat lunak (*software*) untuk *write-protect*

3.2.4 Mencari data/informasi dari bukti elektronik dan mendokumentasikan proses akuisisinya dalam *chain of custody*

3.2.5 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai proses akuisisi data elektronik dari sistem CCTV

4. Sikap kerja yang diperlukan

4.1 Teliti dalam penyiapan media penyimpanan elektronik

4.2 Berwawasan luas

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab

5. Aspek Kritis

5.1 Ketepatan dalam melaksanakan akuisisi data elektronik rekaman video dari sistem CCTV dengan memprioritaskan format original yang tidak terkompresi sebagai pilihan utama, atau format kompresi sebagai pilihan alternatif

KODE UNIT : **J.62FDG00.014.1**

JUDUL UNIT : **Menyalin Data Elektronik dengan Kondisi Khusus**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan akuisisi perangkat komputer dan melakukan akuisisi tambahan dengan kondisi khusus/tertentu.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan akuisisi perangkat komputer dengan kondisi khusus/tertentu	1.1 Akuisisi melalui jaringan dilaksanakan sesuai prosedur pada berbagai ***platform***. 1.2 Akuisisi memori *Random Access Memory* (RAM) dilaksanakan sesuai prosedur pada berbagai *platform*. 1.3 Identifikasi dan akuisisi **volume/kontainer enkripsi** dalam keadaan terdekripsi (*mounted*) dilaksanakan sesuai prosedur pada berbagai *platform*.
2. Melakukan akuisisi tambahan dengan kondisi khusus/tertentu	2.1 Identifikasi dan akuisisi *log files* dilaksanakan sesuai prosedur pada berbagai *platform*. 2.2 Identifikasi dan akuisisi *registry files* dilaksanakan sesuai prosedur pada berbagai *platform*. 2.3 Akuisisi perangkat seluler dilaksanakan sesuai prosedur pada berbagai **jenis ekstraksi**. 2.4 Akuisisi penyimpanan *cloud* dilaksanakan sesuai prosedur pada berbagai **platform penyimpanan**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 *Triage* forensik, yaitu: pengaplikasian digital forensik untuk penanganan pertama bukti elektronik di lapangan, khususnya

akuisisi terhadap perangkat komputer atau *server* dalam keadaan masih hidup/*on* dalam kondisi tertentu.

1.2 *Platform*, yaitu: sistem operasi Windows, Linux dan Mac.

1.3 Volume/kontainer enkripsi hanya bisa diakses isinya ketika sudah dalam keadaan terdekripsi (*mounted*) dan diprioritaskan untuk dilakukan proses akuisisi terhadapnya.

1.4 Jenis ekstraksi data elektronik pada perangkat seluler, yaitu: ekstraksi logik (*logical*), *file system* dan fisik (*physical*).

1.5 *Platform* penyimpanan, untuk komputasi *cloud* (*cloud as a storage*).

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 Media penyimpanan elektronik

2.1.3 *Tools* yang digunakan untuk akuisisi bukti elektronik melalui jaringan pada berbagai *platform*

2.1.4 *Tools* yang digunakan untuk akuisisi memori *Random Access Memory* (RAM) pada berbagai *platform*

2.1.5 *Tools* yang digunakan untuk identifikasi dan akuisisi volume/kontainer enkripsi pada berbagai *platform*

2.1.6 *Tools* yang digunakan untuk akuisisi logik (*logical*) data elektronik pada berbagai *platform*

2.1.7 *Tools* yang digunakan untuk ekstraksi data elektronik dari perangkat seluler pada berbagai *platform* seluler

2.1.8 *Tools* yang digunakan untuk akuisisi data elektronik dari *cloud* pada berbagai *platform* penyimpanan

2.1.9 *Tools* yang digunakan untuk verifikasi fungsi *hash* atau fungsi lain yang setara

2.1.10 *Tools* yang digunakan untuk *write-protect* guna menjaga keutuhan data elektronik dari perubahan data

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan penyalinan data elektronik dengan kondisi khusus.

2. Persyaratan kompetensi

2.1 *Digital Evidence First Responder* (DEFR)/Penangan Pertama Bukti Elektronik (PPBE)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Informasi awal terjadinya insiden

3.1.2 Bukti elektronik

3.1.3 Prosedur penanganan pertama bukti elektronik

3.1.4 Aspek legalitas penanganan pertama bukti elektronik

3.1.5 *Forensic imaging*

3.1.6 *Image file*

3.1.7 *Hash*

3.1.8 *Chain of custody*

3.1.9 *Volatile*

3.1.10 *Triage* forensik

3.1.11 Sistem operasi Windows, Linux dan Mac

3.1.12 Memori *Random Access Memory* (RAM)

3.1.13 Enkripsi dan dekripsi

3.1.14 Ekstraksi data elektronik dari perangkat seluler

3.1.15 Komputasi *cloud*

3.2 Keterampilan

3.2.1 Menggunakan aplikasi untuk akuisisi bukti elektronik melalui jaringan pada berbagai *platform*

3.2.2 Menggunakan aplikasi untuk akuisisi memori *Random Access Memory* (RAM) pada berbagai *platform*

3.2.3 Menggunakan aplikasi untuk akuisisi identifikasi dan akuisisi volume/kontainer enkripsi pada berbagai *platform*

3.2.4 Menggunakan aplikasi untuk akuisisi logik (*logical*) data elektronik pada berbagai *platform*

3.2.5 Menggunakan aplikasi untuk ekstraksi data elektronik dari perangkat seluler pada berbagai *platform* seluler

3.2.6 Menggunakan aplikasi untuk akuisisi data elektronik dari *cloud* pada berbagai *platform* penyimpanan

3.2.7 Menggunakan aplikasi untuk verifikasi fungsi *hash*

3.2.8 Menggunakan perangkat keras (*hardware*) atau perangkat lunak (*software*) untuk *write-protect*

3.2.9 Mencari data/informasi dari bukti elektronik dan mendokumentasikan proses akuisisi-nya dalam *chain of custody*

3.2.10 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai penyalinan data elektronik dengan kondisi khusus

4. Sikap kerja yang diperlukan

4.1 Teliti dalam akuisisi memori *Random Access Memory* (RAM) dan volume/kontainer enkripsi dalam keadaan terdekripsi (*mounted*)

4.2 Berwawasan luas

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab

5. Aspek Kritis

5.1 Ketepatan dalam melaksanakan identifikasi dan akuisisi volume/kontainer enkripsi dalam keadaan terdekripsi (*mounted*) sesuai prosedur pada berbagai *platform*

KODE UNIT : **J.62FDG00.015.1**

JUDUL UNIT : **Memberi Dukungan Teknis Lanjutan**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyediakan dukungan teknis dasar dan dukungan teknis lanjutan digital forensik.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyediakan dukungan teknis dasar digital forensik	1.1 Pemberian dukungan teknis tentang sistem operasi dan *file system* dari berbagai ***platform*** dilaksanakan sesuai prosedur. 1.2 Pemberian dukungan teknis tentang ***write-protect*** dari berbagai *platform* dilaksanakan sesuai prosedur. 1.3 Pemberian dukungan teknis tentang ***hashing*** dari berbagai *platform* dilaksanakan sesuai prosedur. 1.4 Pemberian dukungan teknis tentang identifikasi ***time-stamp*** dari berbagai *platform* dilaksanakan sesuai prosedur.
2. Menyediakan dukungan teknis lanjutan digital forensik	2.1 Pemberian dukungan teknis tentang jaringan komputer dan siber pada berbagai *platform* dilaksanakan sesuai prosedur. 2.2 Pemberian dukungan teknis tentang ***cloud computing*** dari berbagai platform, dilaksanakan sesuai prosedur. 2.3 Pemberian dukungan teknis tentang ***Open Source Intelligence*** **(OSINT)** dari berbagai *platform* dilaksanakan sesuai prosedur. 2.4 Pemberian dukungan teknis tentang enkripsi dan **steganografi** dari berbagai *platform*/aplikasi dilaksanakan sesuai prosedur. 2.5 Pemberian dukungan teknis tentang ***file signature*** dari berbagai jenis format file, dilaksanakan sesuai prosedur. 2.6 Pemberian dukungan teknis tentang ***data recovery*** dan ***secure deletion*** (penghapusan secara aman) dari

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
	berbagai pl*atform*/aplikasi dilaksanakan sesuai prosedur. 2.7 Pemberian dukungan teknis tentang identifikasi ***malware*** dari berbagai *platform* dilaksanakan sesuai prosedur. 2.8 Pemberian dukungan teknis tentang identifikasi ***multimedia*** dari berbagai *platform* dilaksanakan sesuai prosedur.

BATASAN VARIABEL

1. Konteks variabel
   1.1 *Platform*, yaitu: sistem operasi Windows, Linux dan Mac.
   1.2 *Write-protect*, dalam bentuk *hardware* (perangkat keras) dan *software* (perangkat lunak) dari berbagai platform.
   1.3 *Hashing*, yaitu: kalkulasi nilai *hash* melalui berbagai jenis algoritma tertentu terhadap satu bukti elektronik atau *file* secara menyeluruh (mulai dari *header*, isi hingga *footer* dari file tersebut) sehingga menghasilkan nilai *hash* yang unik dan diasosiasikan khusus untuk bukti elektronik atau *file* tersebut.
   1.4 *Time-stamp*, yaitu: *date/time* (tanggal/waktu) dari satu *file*, khususnya *created* dan *modified* yang dapat digunakan untuk menganalisa apakah *file* tersebut dibuat untuk pertama kali, atau sudah di-*copy-paste*, atau sudah di-*edit* isinya.
   1.5 *Cloud computing*, yaitu: *cloud as a platform* (komputasi *cloud* sebagai sebuah sistem operasi), *cloud as an application* (komputasi *cloud* sebagai sebuah aplikasi) dan *cloud as a storage* (komputasi *cloud* sebagai media penyimpanan *online*).
   1.6 *Open Source Intelligence* (OSINT), yaitu: teknik-teknik khusus untuk mencari/mengidentifikasi data dan informasi tertentu yang tersedia pada jaringan *internet* yang bersifat *open-source*, untuk kemudian menganalisanya sesuai kebutuhan *data analytics*, *profiling*, prediksi, keamanan, pelacakan aset dan lain-lain.

1.7 Steganografi merupakan teknik enkripsi lanjutan yang ditambah dengan algoritma penyisipan (*insertion*) guna menyisipkan satu pesan rahasia untuk ditanamkan (*embedded*) ke satu *carrier file* sehingga pesan tersebut tersamarkan dan tidak terdeteksi, sedangkan *file* tersebut tidak mengalami perubahan yang signifikan.

1.8 *File signature*, adalah beberapa *bytes* pertama pada *header* dari suatu *file* yang sifatnya unik dan menunjukkan format *file* tersebut yang sesungguhnya.

1.9 *Data recovery*, bersifat fisik berdasarkan *bit-per-bit* di sektor maupun logik berdasarkan *file system*, yang mencakup antara lain data yang masih ada (*intact*), data yang sudah terhapus (*deleted*) dan data yang sudah hilang dan tidak tercatat di *file system* (*lost*).

1.10 *Secure deletion*, merupakan penghapusan secara sempurna terhadap sekelompok data elektronik dengan menggunakan algoritma tertentu untuk menimpanya (*overwriting*).

1.11 *Malware*, merupakan singkatan dari *malicious software* yang antara lain jenisnya berupa: virus, *worm*, *trojan* dan *rootkit*.

1.12 *Multimedia*, mencakup rekaman *audio*, *video* dan gambar digital, termasuk proses peningkatan kualitas (*enhancement*) terhadapnya.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 Media penyimpanan elektronik

2.1.3 *Tools* yang digunakan untuk verifikasi fungsi *hash* atau fungsi lain yang setara

2.1.4 *Tools* yang digunakan untuk *write-protect* guna menjaga keutuhan data elektronik dari perubahan data

2.1.5 *Tools* yang digunakan untuk *cloud computing* sebagai *platform*, aplikasi dan media penyimpanan

2.1.6 *Tools* yang digunakan untuk *Open Source Intelligence* (OSINT)

2.1.7 *Tools* yang digunakan untuk kriptografi dan steganografi

2.1.8 *Tools* yang digunakan untuk *file signature* dan *data recovery*

2.1.9 *Tools* yang digunakan untuk *secure deletion*

2.1.10 *Tools* yang digunakan untuk pembuatan dan identifikasi *malware*

2.1.11 *Tools* yang digunakan untuk proses peningkatan kualitas (*enhancement*) multimedia

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.

1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil memberikan dukungan teknis lanjutan.

2. Persyaratan kompetensi

2.1 *Digital Evidence First Responder* (DEFR)/Penangan Pertama Bukti Elektronik (PPBE)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Informasi awal terjadinya insiden

3.1.2 Bukti elektronik

3.1.3 Prosedur penanganan pertama bukti elektronik

3.1.4 Aspek legalitas penanganan pertama bukti elektronik

3.1.5 *Forensic imaging*

3.1.6 *Image file*

3.1.7 *Hash*

3.1.8 *Chain of custody*

3.1.9 *Volatile*

3.1.10 Komputasi *cloud*

3.1.11 *Open Source Intelligence* (OSINT)

3.1.12 Kriptografi dan steganografi

3.1.13 *File signature* dan *data recovery*

3.1.14 *Secure deletion*

3.1.15 *Malware*

3.1.16 *Multimedia enhancement*

3.1.17 *Database*/basis data

3.1.18 *Drone*

3.2 Keterampilan

3.2.1 Menggunakan aplikasi untuk verifikasi fungsi *hash*

3.2.2 Menggunakan perangkat keras (*hardware*) atau perangkat lunak (*software*) untuk *write-protect*

3.2.3 Menggunakan aplikasi untuk *cloud computing*

3.2.4 Menggunakan aplikasi untuk *Open Source Intelligence* (OSINT)

3.2.5 Menggunakan aplikasi untuk kriptografi dan steganografi

3.2.6 Menggunakan aplikasi untuk *file signature* dan *data recovery*

3.2.7 Menggunakan aplikasi untuk *secure deletion*

3.2.8 Menggunakan aplikasi untuk *malware*

3.2.9 Menggunakan aplikasi untuk multimedia *enhancement*

3.2.10 Mencari data/informasi dari bukti elektronik dan mendokumentasikan proses akuisisi-nya dalam *chain of custody*

3.2.11 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai pemberian dukungan teknis lanjutan

4. Sikap kerja yang diperlukan

4.1 Teliti dalam pemberian dukungan teknis tentang identifikasi *time-stamp* dan *malware*

4.2 Berwawasan luas

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab dalam melaksanakan Pemberian dukungan teknis tentang *data recovery* dan *secure deletion* (penghapusan secara aman) dari berbagai pl*atform*/aplikasi sesuai prosedur

5. Aspek Kritis

5.1 Ketepatan dalam melaksanakan pemberian dukungan teknis tentang *cloud computing* dari berbagai *platform* dilaksanakan sesuai prosedur

KODE UNIT : **J.62FDG00.016.1**

JUDUL UNIT : **Menyegel Data Elektronik yang telah Diakuisisi dengan Menggunakan Fungsi Verifikasi**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyegel data elektronik yang telah diakuisisi dengan menggunakan fungsi verifikasi dan tanda tangan elektronik.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyediakan penyegelan dengan menggunakan fungsi verifikasi	1.1 Penyegelan terhadap data dari proses akuisisi dilaksanakan dengan ketat sesuai prosedur investigasi. 1.2 Penggunaan fungsi verifikasi terhadap data hasil akuisisi dilaksanakan melalui implementasi algoritma ***hash*** tertentu. 1.3 Perbandingan atau komparasi nilai *hash* dari ***image file*** dilaksanakan terhadap media penyimpanan barang bukti. 1.4 Hasil dari verifikasi **didokumentasikan secara lengkap**.
2. Menyediakan penyegelan dengan menggunakan tanda tangan elektronik	2.1 Tanda tangan elektronik dibubuhkan pada data elektronik hasil akuisisi sesuai dengan prosedur dan sistem tanda tangan digital yang digunakan. 2.2 Pembubuhan **tanda tangan elektronik** didokumentasikan dengan jelas. 2.3 Pengecekan sertifikat tanda tangan elektronik dilaksanakan untuk memverifikasi integritas/keutuhan dari *image file* yang dihasilkan dari proses akuisisi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 *Hash* adalah fungsi matematika satu arah yang digunakan untuk verifikasi yang berisikan sederet kode unik melalui algoritma tertentu.

1.2 Didokumentasikan secara lengkap merupakan dokumentasi secara rinci terhadap proses verifikasi.

1.3 *Image file* dihasilkan dari proses akuisisi secara fisik *bit-per-bit* terhadap media penyimpanan dari bukti elektronik dan ke-identikannya diverifikasi melalui fungsi *hash* atau fungsi lain yang setara.

1.4 Tanda tangan elektronik dilaksanakan melalui algoritma *key pairs* yang kuat dan dilengkapi dengan sertifikatnya.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Komputer dan/atau perangkat pengolahan data

2.1.2 *Tools* untuk melaksanakan penyegelan data melalui fungsi verifikasi *hash*

2.1.3 *Tools* untuk melaksanakan penyegelan data melalui tanda tangan elektronik

2.2 Perlengkapan

2.2.1 Kamera

2.2.2 Alat tulis

3. Peraturan yang diperlukan

3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar

4.1 Norma

(Tidak Ada.)

4.2 Standar

4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.
   1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.
   1.5 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil memberikan melaksanakan penyegelan data yang diakuisisi dengan menggunakan fungsi verifikasi atau tanda tangan elektronik.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan
   3.1 Pengetahuan
      3.1.1 Penyegelan data elektronik yang diakuisisi menggunakan fungsi verifikasi atau tanda tangan elektronik
      3.1.2 Bukti elektronik
      3.1.3 Prosedur penanganan pertama bukti elektronik
      3.1.4 Informasi awal terjadinya insiden
      3.1.5 Aspek legalitas penanganan pertama bukti elektronik
   3.2 Keterampilan
      3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah data angka pada aplikasi spreadsheet

3.2.3 Mengolah grafik presentasi

3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai melaksanakan penyegelan data yang diakuisisi dengan menggunakan fungsi verifikasi atau tanda tangan elektronik

4. Sikap kerja yang diperlukan

4.1 Teliti dalam pendokumentasian proses penyegelan data elektronik

4.2 Berwawasan luas dalam melaksanakan perbandingan atau komparasi nilai *hash* dari *image file* terhadap media penyimpanan barang bukti

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab dalam mendokumentasikan pembubuhan tanda tangan elektronik dengan jelas

5. Aspek Kritis

5.1 Ketepatan dalam melaksanakan penyegelan terhadap data dari proses akuisisi dengan ketat sesuai prosedur investigasi

KODE UNIT : **J.62FDG00.017.1**

JUDUL UNIT : **Mengamankan Bukti Elektronik dengan Menerapkan Prinsip Kerahasiaan, Integritas, dan Ketersediaan**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyediakan kontrol keamanan data elektronik dengan prinsip kerahasiaan, integritas dan ketersediaan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyediakan kontrol keamanan data elektronik dengan prinsip kerahasiaan dan integritas	1.1 Kerahasiaan terhadap data elektronik dilaksanakan dengan ketat sesuai prosedur penanganan pertama bukti elektronik dengan mempertimbangkan **kontrol akses**. 1.2 Integritas terhadap data elektronik dilaksanakan sesuai prosedur penanganan pertama bukti elektronik dengan mempertimbangkan fungsi verifikasi dan/atau tanda tangan elektronik. 1.3 Hasil pelaksanaan kontrol kerahasiaan dan integritas didokumentasikan secara lengkap.
2. Menyediakan kontrol keamanan data elektronik dengan prinsip ketersediaan akses	2.1 Ketersediaan akses terhadap data elektronik yang dihasilkan dari proses akuisisi dilaksanakan sesuai prosedur investigasi. 2.2 Penggunaan ketersediaan akses terhadap data elektronik dilaksanakan sesuai dengan **retensi**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Kontrol akses maksudnya data elektronik dijaga kerahasiaannya dengan mempertimbangkan kontrol akses sesuai prosedur, bisa secara fisik dan *data logic*.

1.2 Retensi adalah durasi waktu penyimpanan bukti elektronik dan/atau data elektronik sesuai dengan aturan berlaku.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 *Tools* untuk melaksanakan pengamanan bukti elektronik dan data elektronik dengan menerapkan prinsip dasar menjaga kerahasiaan, integritas, dan ketersediaan
   2.2 Perlengkapan
      2.2.1 Kamera
      2.2.2 Alat tulis

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar
   4.1 Norma
   (Tidak Ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan

konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan pengamanan bukti elektronik dengan menerapkan prinsip dasar menjaga kerahasiaan, integritas, dan ketersediaan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Pengamanan bukti elektronik dengan menerapkan prinsip dasar menjaga kerahasiaan, integritas, dan ketersediaan

3.1.2 Bukti elektronik

3.1.3 Prosedur penanganan pertama bukti elektronik

3.1.4 Informasi awal terjadinya insiden

3.1.5 Aspek legalitas penanganan pertama bukti elektronik

3.1.6 Keamanan informasi

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

3.2.3 Mengolah grafik presentasi

3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai pengamanan bukti elektronik dengan menerapkan prinsip dasar menjaga kerahasiaan, integritas, dan ketersediaan

4. Sikap kerja yang diperlukan

4.1 Teliti dalam melaksanakan integritas terhadap data elektronik sesuai prosedur penanganan pertama bukti elektronik dengan mempertimbangkan fungsi verifikasi dan/atau tanda tangan elektronik

4.2 Ketat dalam melaksanakan kerahasiaan terhadap data elektronik sesuai prosedur penanganan pertama bukti elektronik dengan mempertimbangkan kontrol akses

4.3 Berwawasan luas dalam melaksanakan penggunaan ketersediaan akses terhadap data sesuai dengan retensi

4.4 Cara berpikir sistematis dan *teamwork*

4.5 Bertanggung jawab dalam mendokumentasikan hasil pelaksanaan kontrol kerahasiaan dan integritas secara lengkap

5. Aspek Kritis

5.1 Ketepatan dalam melaksanakan kerahasiaan terhadap data elektronik dengan ketat sesuai prosedur penanganan pertama bukti elektronik dengan mempertimbangkan kontrol akses

KODE UNIT : **J.62FDG00.018.1**

JUDUL UNIT : **Mengemas Bukti Elektronik**

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan pengemasan/ pembungkusan secara *baseline* untuk seluruh bukti elektronik, dan pengemasan/pembungkusan secara additional/tambahan untuk kondisi tertentu, serta pengiriman bukti elektronik.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melaksanakan pengemasan/ pembungkusan secara *baseline* untuk seluruh bukti elektronik	1.1 **Label** seluruh bukti elektronik diterapkan untuk kepastian dan kejelasan identitas dengan format yang menyesuaikan dengan ketentuan regulasi/yurisdiksi. 1.2 Catu daya yang berkecukupan dipasang sesuai dengan mempertimbangkan penggunaan *charger* untuk kecukupan suplai daya listrik. 1.3 Bukti elektronik dimasukkan ke dalam kontainer sesuai **prosedur.** 1.4 Prosedur pencegahan adanya sidik jari diterapkan dengan ketat sesuai prosedur untuk menjaga keutuhannya.
2. Melakukan pengemasan/ pembungkusan secara *additional*/tambahan untuk kondisi tertentu	2.1 Pengemasan/pembungkusan secara *additional*/tambahan dilaksanakan sesuai kebutuhan penanganan pertama bukti elektronik. 2.2 Pengemasan/pembungkusan dilaksanakan dengan menggunakan **peralatan proteksi**.
3. Melaksanakan pengiriman bukti elektronik	3.1 Dokumentasi *chain of custody* dipelihara sesuai **aturan yang berlaku**. 3.2 Pelaksanaan pengiriman bukti elektronik dilaksanakan sesuai **prosedur pengiriman.**

BATASAN VARIABEL

1. Konteks variabel

   1.1 Label ditempatkan pada posisi sesuai prosedur penanganan pertama bukti elektronik dengan mempertimbangkan penggunaan segel *tamper-evident* (bukti rusak) yang ditandatangani.

   1.2 Prosedur meliputi: kemasan dipasangkan sesuai dengan mempertimbangkan pencegahan kerusakan akibat benturan, getaran, ketinggian, panas dan ekspos frekuensi radio/seluler selama proses pengiriman, serta media penyimpanan magnetik disimpan dalam kemasan yang anti-statik dan bebas partikel.

   1.3 Peralatan proteksi, antara lain: penggunaan sarung tangan atau proteksi bukti elektronik dari pengaruh sumber elektromagnetik, misalnya radio polisi, *speaker*, mesin *X-ray* dengan kondisi lingkungan pengemasan yang bebas dari listrik statik, debu, lemak, dan polutan kimia yang dapat menyebabkan kerusakan oksidatif dan kondensasi kelembaban pada lapisan magnetik, serta bebas dari sinar *Ultra Violet* (UV) yang dapat menyebabkan degradasi *Deoxyribonucleic Acid* (DNA) dan kerusakan pada beberapa media tertentu.

   1.4 Prosedur pengiriman meliputi: selama proses pengiriman dengan pertimbangan untuk mengidentifikasi dan mencegah kemungkinan perubahan atau kerusakan data, penggunaan enkripsi sangat direkomendasikan jika pengiriman bukti elektronik tidak dilakukan oleh *Associate Digital Evidence First Responder* (ADEFR)/*Digital Evidence First Responder* (DEFR)/ *Digital Evidence Specialist* (DES), pelaksanaan pengiriman bukti elektronik dengan mempertimbangkan kemungkinan adanya muatan listrik statis yang dapat menyebabkan kerusakan pada barang bukti, dan kepastian pengemasan/pembungkusan bukti elektronik yang aman dari benturan dan getaran.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Komputer dan/atau perangkat pengolahan data
      2.1.2 *Tools* yang digunakan untuk pengemasan/ pembungkusan bukti elektronik dan pengirimannya
   2.2 Perlengkapan
      2.2.1 Kamera
      2.2.2 Alat tulis

3. Peraturan yang diperlukan
   3.1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018

4. Norma dan standar
   4.1 Norma
   (Tidak Ada.)
   4.2 Standar
      4.2.1 SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja/Tempat Uji Kompetensi (TUK) yang aman.
   1.2 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

1.3 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara serta metode lain yang relevan.

1.4 Hasil unjuk kerja yang berupa kegiatan penuangan dan penyampaian hasil melaksanakan pengemasan/pembungkusan bukti elektronik potensial dan pengirimannya.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang dibutuhkan

3.1 Pengetahuan

3.1.1 Pengemasan/pembungkusan bukti elektronik potensial dan pengirimannya

3.1.2 Bukti elektronik

3.1.3 Prosedur penanganan pertama bukti elektronik

3.1.4 Informasi awal terjadinya insiden

3.1.5 Aspek legalitas penanganan pertama bukti elektronik

3.2 Keterampilan

3.2.1 Menggunakan aplikasi pengolah kata

3.2.2 Mengolah data angka pada aplikasi *spreadsheet*

3.2.3 Mengolah grafik presentasi

3.2.4 Mengolah kata-kata untuk dapat membuat penjelasan yang mudah dipahami mengenai melaksanakan pengemasan/pembungkusan bukti elektronik dan pengirimannya

4. Sikap kerja yang diperlukan

4.1 Teliti dalam pengemasan/pembungkusan dengan mempertimbangkan penggunaan sarung tangan atau peralatan proteksi bukti elektronik

4.2 Berwawasan luas dalam menerapkan prosedur pencegahan adanya sidik jari dengan ketat sesuai prosedur untuk menjaga keutuhannya

4.3 Cara berpikir sistematis dan *teamwork*

4.4 Bertanggung jawab dalam memelihara dokumentasi *chain of custody* dipelihara sesuai aturan yang berlaku

5. Aspek Kritis

5.1 Ketepatan dalam melaksanakan pengemasan/pembungkusan dengan mempertimbangkan penggunaan sarung tangan atau proteksi perangkat elektronik atau lingkungan pengemasan

5.2 Ketepatan dalam memelihara dokumentasi *chain of custody* sesuai aturan yang berlaku

BAB III
PENUTUP

Dengan ditetapkannya Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Keahlian Digital Forensik Subbidang Penanganan Pertama Bukti Elektronik, maka SKKNI ini menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan dan pelatihan serta sertifikasi kompetensi.

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH