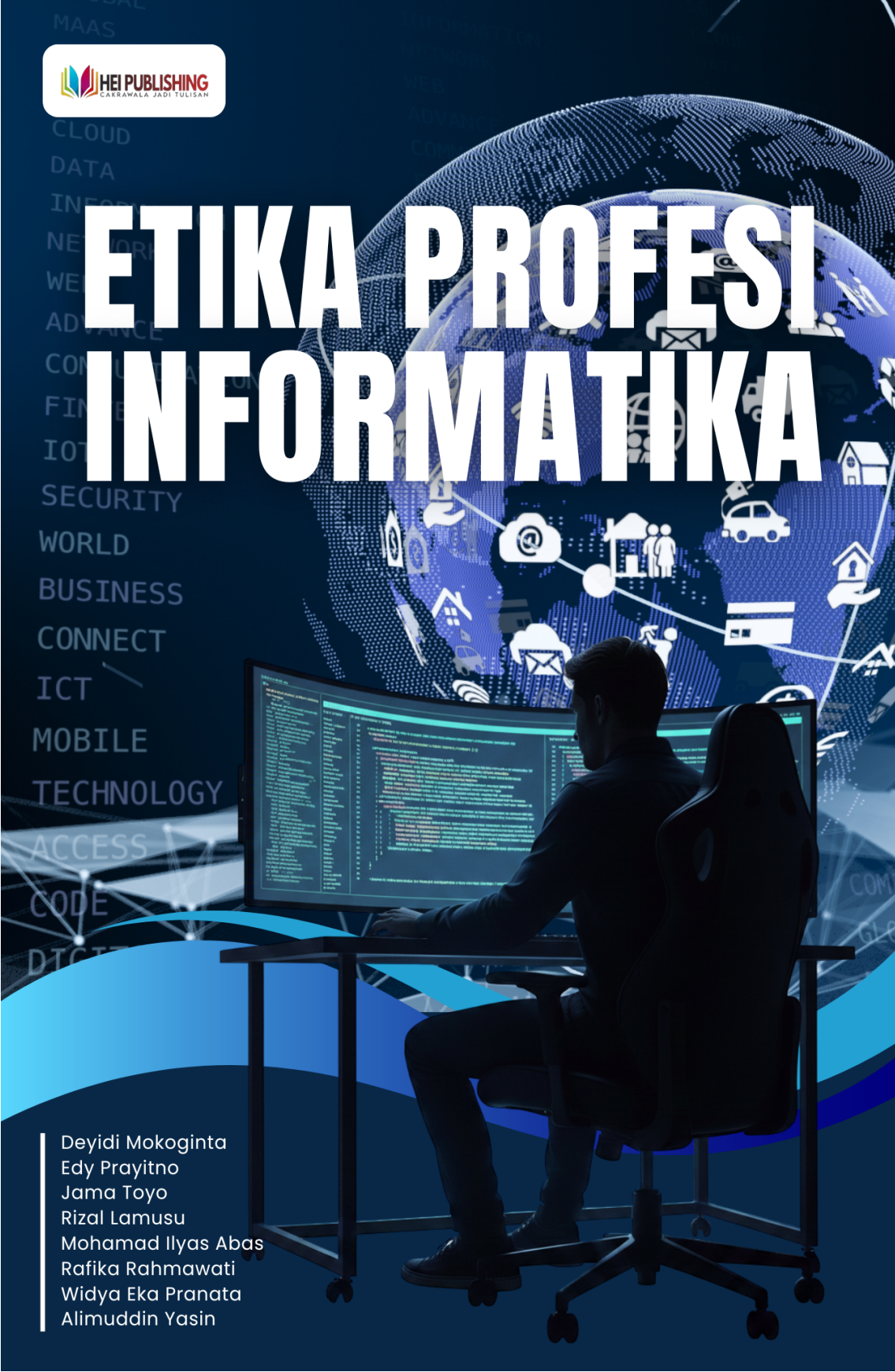
HEI PUBLISHING
CAKRAWALA JADI TULISAN

ETIKA PROFESI INFORMATIKA



Deyidi Mokoginta
Edy Prayitno
Jama Toyo
Rizal Lamusu
Mohamad Ilyas Abas
Rafika Rahmawati
Widya Eka Pranata
Alimuddin Yasin

ETIKA PROFESI INFORMATIKA

Deyidi Mokoginta
Edy Prayitno
Jama Toyo
Rizal Lamusu
Mohamad Ilyas Abas
Rafika Rahmawati
Widya Eka Pranata
Alimuddin Yasin

CV HEI PUBLISHING INDONESIA

ETIKA PROFESI INFORMATIKA

Penulis :
Deyidi Mokoginta
Edy Prayitno
Jama Toyo
Rizal Lamusu
Mohamad Ilyas Abas
Rafika Rahmawati
Widya Eka Pranata
Alimuddin Yasin

ISBN : 978-634-7526-56-4

Editor : Ade Wisandra, S.Kom, M.Kom
Penyunting : Akhirul Desman, ST
Desain Sampul dan Tata Letak : Namira Ummi Khalsum. YB, S.Psi

Penerbit : CV HEI PUBLISHING INDONESIA
Anggota IKAPI No. 034/SBA/2023

Redaksi :
Jl. Air Paku No.29 RSUD Rasidin, Kel. Sungai Sapih, Kec Kuranji
Kota Padang Sumatera Barat
Website : www.heipublishing.com
Email : heipublishing.id@gmail.com

Cetakan pertama, Januari 2026

KATA PENGANTAR

Dengan mengucapkan puji syukur kehadirat Allah SWT, atas limpahan rahmat dan hidayahNya, maka Penulisan Buku dengan judul Etika Profesi Informatika dapat diselesaikan. Buku refernsi ini membahas tentang Pengertian Etika, Pengertian Profesi, Ciri Khas Profesi, Pengertian Profesionalisme, Ciri-ciri Profesionalisme, Kode Etik Profesional, Jenis-jenis Ancaman (*threats*) Melalui IT, Kasus *Computer Crime/cyber Crime*, IT Audit Trail, Real Time Audit, IT Forensics, UU Tentang Hak Cipta, Prosedur Pendirian Bisnis, Kontrak Kerja, Dan Pengadaan, Kontak Bisnis, Pakta Integritas, Jenis-jenis Profesi Di Bidang IT, Deskripsi Kerja Profesi IT Stándar Profesi ACM Dan IEEE Stándar Profesi Di Indonesia Dan RegionaAL.

Buku ini masih banyak kekurangan dalam penyusunannya. Kami mengucapkan terima kasih kepada berbagai pihak yang telah membantu dalam proses penyelesaian Buku ini. Semoga Buku ini dapat menjadi sumber referensi dan literatur yang mudah dipahami.

Padang, Januari 2026

Penulis

DAFTAR ISI

DAFTAR TABEL

BAB 1
PENGERTIAN ETIKA, PENGERTIAN PROFESI, CIRI KHAS PROFESI

1.1 Pendahuluan

Dalam kehidupan bermasyarakat yang kompleks dan dinamis, etika dan profesi menjadi dua elemen fundamental yang saling terkait dan berkontribusi dalam membentuk karakter individu serta integritas suatu komunitas. Etika, yang berasal dari kata Yunani "ethos," merujuk pada sistem nilai dan prinsip moral yang mengatur perilaku dan interaksi manusia. Etika membantu kita membedakan antara tindakan yang baik dan buruk, serta memberikan panduan dalam pengambilan keputusan di berbagai aspek kehidupan, termasuk di tempat kerja.

Sementara itu, profesi dapat diartikan sebagai suatu kegiatan atau pekerjaan yang memerlukan keahlian, pengetahuan, dan pelatihan khusus. Profesi tidak hanya sekadar mengandalkan keterampilan teknis, tetapi juga membutuhkan pemahaman mendalam tentang tanggung jawab moral yang melekat pada posisi tersebut. Dalam banyak profesi, terdapat kode etik yang harus dipatuhi, yang mengatur bagaimana para profesional harus berperilaku dalam menjalankan tugas mereka.

Ciri khas dari sebuah profesi mencakup beberapa aspek penting. Pertama, adanya standar pendidikan dan pelatihan yang tinggi, yang memastikan bahwa individu memiliki kompetensi yang memadai untuk menjalankan tugasnya dengan baik. Kedua, profesi biasanya melibatkan komitmen

terhadap pengembangan diri dan pembelajaran berkelanjutan, di mana para profesional diharapkan untuk selalu memperbarui pengetahuan dan keterampilan mereka. Ketiga, profesi diakui melalui kode etik yang jelas, yang menetapkan prinsip-prinsip moral dan tanggung jawab sosial, serta menjamin kepercayaan masyarakat terhadap profesional tersebut.

Dengan memahami etika dan profesi secara mendalam, kita dapat menciptakan lingkungan kerja yang tidak hanya produktif tetapi juga bermoral. Hal ini penting dalam membangun hubungan yang saling menghormati antara profesional dengan klien, kolega, dan masyarakat luas. Selain itu, dengan menegakkan etika dalam profesi, individu dapat berkontribusi pada terciptanya masyarakat yang lebih adil dan beradab. Dalam era yang penuh tantangan ini, kesadaran akan pentingnya etika dalam profesi menjadi semakin mendesak untuk menjamin keberlanjutan dan kesejahteraan bersama.

1.2 Pengertian Etika

Etika berasal dari bahasa Yunani "ethos" yang berarti karakter atau kebiasaan. Dalam konteks filsafat, etika merujuk pada studi tentang moralitas, nilai, dan prinsip yang mengatur perilaku individu dan masyarakat. Etika berfungsi sebagai panduan untuk menentukan apa yang benar dan salah, baik dan buruk dalam berbagai konteks kehidupan.

Etika adalah cabang filsafat yang mempelajari tentang apa yang baik dan buruk, serta tentang kewajiban dan moralitas. Secara umum, etika berusaha menjawab pertanyaan-pertanyaan mendasar tentang nilai-nilai dan prinsip-prinsip yang memandu perilaku manusia. Etika juga sering disebut sebagai ilmu tentang moral, yang mencakup norma-norma dan nilai-nilai yang mengatur tindakan individu dan kelompok. (Rachels, James, & Rachels, Stuart. 2019).

1.2.1 Definisi Etika

Etika dapat didefinisikan sebagai disiplin yang mengeksplorasi dan menganalisis prinsip-prinsip moral yang memengaruhi perilaku manusia (Singer, 2011). Etika mencakup berbagai aspek, termasuk norma, nilai, dan kepercayaan yang mendasari tindakan kita. Terdapat beberapa cabang utama dalam etika :

1. Etika Normatif: Meneliti standar-standar moral yang harus diikuti. Ini mencakup prinsip-prinsip yang menentukan perilaku yang benar atau salah.
2. Etika Deskriptif: Menggambarkan dan menganalisis praktik moral yang ada dalam masyarakat, tanpa menghakimi apakah praktik tersebut baik atau buruk.
3. Etika Terapan: Menerapkan prinsip-prinsip etika dalam situasi nyata, seperti etika bisnis, etika medis, dan etika lingkungan.

1.2.2 Teori-teori Etika

Berbagai teori etika telah dikembangkan oleh para filsuf sepanjang sejarah (Velasquez, 2017). Berikut adalah beberapa teori utama:

1. Utilitarianisme: Teori ini menekankan bahwa tindakan yang benar adalah yang menghasilkan kebahagiaan atau manfaat terbesar bagi jumlah orang terbanyak. Utilitarianisme sering diasosiasikan dengan filsuf Jeremy Bentham dan John Stuart Mill.
2. Deontologi: Dikenalkan oleh Immanuel Kant, teori ini berfokus pada kewajiban dan hak. Menurut deontologi, tindakan dianggap benar jika dilakukan berdasarkan prinsip moral yang universal, terlepas dari konsekuensinya.
3. Etika Kebajikan: Berakar pada ajaran Aristoteles, etika kebajikan menekankan pengembangan karakter dan

kebajikan individu sebagai dasar untuk tindakan moral yang baik.

4. Etika Konsekuensialis: Pendekatan ini menilai tindakan berdasarkan hasil atau konsekuensi yang dihasilkan, serupa dengan utilitarianisme tetapi lebih luas dalam ruang lingkupnya.

1.2.3 Peran Etika dalam Kehidupan Sehari-hari

Etika memainkan peranan penting dalam berbagai aspek kehidupan, termasuk :

1. Etika Pribadi: Mengatur perilaku individu dalam menjalani kehidupan sehari-hari, termasuk pengambilan keputusan yang melibatkan integritas dan tanggung jawab.
2. Etika Sosial: Menyentuh bagaimana individu berinteraksi dalam masyarakat. Ini mencakup isu-isu seperti keadilan, kesetaraan, dan hak asasi manusia.
3. Etika Profesional: Banyak profesi memiliki kode etik yang mengatur perilaku anggotanya, seperti kedokteran, hukum, dan bisnis. Kode etik ini bertujuan untuk menjaga standar profesionalisme dan melindungi kepentingan klien serta masyarakat. (Beauchamp, & Childress, 2019)

1.3 Pengertian Profesi

1.3.1 Defenisi Profesi

Profesi adalah suatu pekerjaan yang memerlukan pendidikan, pelatihan, dan keahlian khusus dalam suatu bidang tertentu. Pekerjaan ini biasanya melibatkan tanggung jawab yang tinggi dan memerlukan pengetahuan yang mendalam. Menurut Alvin Toffler dalam bukunya "Future Shock," profesi adalah sebuah kategori kerja yang ditandai oleh tingkat keahlian yang spesifik dan diakui oleh masyarakat (Toffler, 1970). Profesi berperan penting dalam memenuhi kebutuhan

sosial dan ekonomi, memberikan kontribusi yang signifikan terhadap kemajuan masyarakat.

Secara harfiah profesi berasal dari kata profession (ingris) yang berasal dari bahasa latin profesus ang berarti "mampu atau ahli dalam suatu bentuk pekerjaan". Dalam webster‟s new worl dictionary di temukan bahwa profesi merupakan suatu pekerjaan yang menuntut pendidikan tinggi.1 Kata profesi dapat di ketahui dari tiga sumber makna yaitu makna Secara etimologi profesi berasal dari bahasa ingris profession atau bahasa latin profecus yang artinya mengakui, pengakuan, menyatakan mampu atau ahli dalam melakukan pekerjaan tertentu.

Secara terminologi profesi dapat di artikan sebagai suatu pekerjaan yang mempersyaratkan pekerjaan tinggi bagi pelakunya yang di tekankan pada pekerjaan mental. Sementara secara sosiologi profesi merupakan jenis model pekerjaan yang ideal, karena dalam realitanya bukanlah hal yang mudah untuk mewujudkannya dan hanya bisa dilakukan oleh orang-orang yang sudah profesional dalam bidangnya.

1.3.2 Karakteristik Profesi

1. Pendidikan dan Pelatihan Khusus

   Salah satu karakteristik utama dari sebuah profesi adalah adanya pendidikan dan pelatihan khusus yang diperlukan untuk memasuki bidang tersebut. Profesi seperti kedokteran, hukum, dan teknik memerlukan gelar akademis serta pelatihan praktis yang ketat sebelum individu dapat berpraktik. Menurut Abbot (1988) dalam The System of Professions, pendidikan formal berfungsi untuk memastikan bahwa para profesional memiliki pengetahuan yang mendalam serta keterampilan teknis yang diperlukan untuk melaksanakan tugas mereka secara

efektif. Hal ini membedakan profesi dari pekerjaan lainnya yang mungkin tidak memerlukan kualifikasi formal yang sama.

2. Standar Etika dan Kode Etik

   Profesi biasanya memiliki standar etika yang jelas, yang diatur dalam bentuk kode etik. Kode etik ini berfungsi sebagai pedoman moral bagi para profesional dalam menjalankan tugas mereka, mengarahkan mereka untuk bertindak dengan integritas dan tanggung jawab. Menurut Richard T. DeGeorge dalam Business Ethics, kode etik sangat penting untuk menjaga kepercayaan masyarakat terhadap profesi, serta memastikan bahwa tindakan profesional sesuai dengan norma-norma moral yang diharapkan (DeGeorge, 1999). Kode etik ini juga berfungsi untuk menangani konflik kepentingan dan situasi etis yang kompleks dalam praktik sehari-hari.

3. Komitmen terhadap Pengembangan Diri

   Karakteristik lain dari profesi adalah komitmen terhadap pengembangan diri dan pembelajaran berkelanjutan. Para profesional diharapkan untuk terus memperbarui pengetahuan dan keterampilan mereka seiring dengan kemajuan dalam bidang masing-masing. Donald Schön dalam The Reflective Practitioner menekankan pentingnya refleksi dalam praktik profesional, di mana individu diharapkan untuk mengevaluasi dan meningkatkan pendekatan mereka terhadap pekerjaan seiring dengan perkembangan ilmu pengetahuan dan teknologi (Schön, 1983). Hal ini menunjukkan bahwa profesi memerlukan individu yang tidak hanya terampil, tetapi juga memiliki rasa ingin tahu dan kemauan untuk belajar.

4. Pengakuan oleh Masyarakat

   Profesi juga dicirikan oleh pengakuan dari masyarakat. Status profesi sering kali didasarkan pada keahlian dan kontribusi yang diberikan kepada masyarakat. Menurut Freidson (2001) dalam Professionalism: The Third Logic, profesi berfungsi sebagai jembatan antara pengetahuan dan tindakan, dan mereka memiliki tanggung jawab untuk menyediakan layanan berkualitas tinggi yang bermanfaat bagi masyarakat (Freidson, 2001). Pengakuan ini juga mencakup kepercayaan dari masyarakat terhadap kemampuan profesional dalam menjalankan tugas mereka.

5. Tanggung Jawab Sosial

   Setiap profesi memiliki tanggung jawab sosial yang melekat, di mana para profesional diharapkan untuk berkontribusi terhadap kesejahteraan masyarakat. Profesi tidak hanya berfokus pada keuntungan pribadi, tetapi juga pada dampak yang ditimbulkan oleh tindakan mereka terhadap masyarakat luas. Menurut Etzioni (1993) dalam *The Spirit of Community*, profesionalisme melibatkan komitmen terhadap nilai-nilai sosial dan etika yang lebih besar, yang menciptakan kepercayaan dan kolaborasi dalam masyarakat (Etzioni, 1993). Tanggung jawab sosial ini menciptakan hubungan yang saling menguntungkan antara profesional dan masyarakat yang mereka layani.

1.3.3 Komitmen dalam Pengembangan Diri

Pengertian Komitmen terhadap Pengembangan Diri

Komitmen terhadap pengembangan diri adalah sikap dan upaya individu untuk terus meningkatkan pengetahuan, keterampilan, dan kemampuan mereka sepanjang hayat. Dalam konteks profesional, komitmen ini mencerminkan dedikasi seorang profesional untuk tidak hanya memenuhi persyaratan

dasar pekerjaan, tetapi juga untuk berkembang dan beradaptasi dengan perubahan di bidangnya. Menurut Merriam-Webster, pengembangan diri mencakup semua kegiatan yang membantu seseorang untuk mencapai potensi penuh mereka, termasuk pendidikan formal, pelatihan, dan pengalaman praktis (Merriam-Webster, 2021).

Pentingnya Pengembangan Diri dalam Karier

Pengembangan diri sangat penting dalam konteks karier, terutama di era globalisasi dan kemajuan teknologi yang pesat. Seiring dengan cepatnya perubahan dalam industri, para profesional diharapkan untuk tetap relevan dan kompetitif. Menurut O'Donnell dan Garavan (2001) dalam studi mereka tentang pelatihan dan pengembangan, organisasi yang mendukung pengembangan karyawan cenderung memiliki tingkat produktivitas yang lebih tinggi dan retensi karyawan yang lebih baik. Hal ini menunjukkan bahwa komitmen terhadap pengembangan diri tidak hanya bermanfaat bagi individu, tetapi juga bagi organisasi secara keseluruhan (O'Donnell & Garavan, 2001).

Metode Pengembangan Diri

Ada berbagai metode yang dapat digunakan untuk pengembangan diri, termasuk pendidikan formal, kursus online, seminar, dan mentoring. Penggunaan teknologi informasi, seperti platform pembelajaran daring, semakin memudahkan individu untuk mengakses sumber daya untuk pengembangan diri. Menurut Knowles (1984) dalam bukunya *Andragogy in Action*, penting bagi individu untuk memiliki kendali atas proses pembelajaran mereka sendiri, dan pendekatan ini membantu menciptakan motivasi yang lebih besar untuk belajar (Knowles, 1984). Pendekatan yang

berorientasi pada individu ini sangat relevan dalam konteks pengembangan diri.

Pengembangan Keterampilan Interpersonal

Selain keterampilan teknis, pengembangan keterampilan interpersonal juga merupakan aspek penting dari pengembangan diri. Keterampilan ini meliputi kemampuan berkomunikasi, bekerja dalam tim, dan kepemimpinan. Menurut Goleman (1998) dalam *Emotional Intelligence*, kecerdasan emosional kemampuan untuk memahami dan mengelola emosi sendiri dan orang lain—merupakan faktor kunci dalam kesuksesan profesional (Goleman, 1998). Dengan mengembangkan keterampilan interpersonal, individu dapat meningkatkan kemampuan mereka untuk berkolaborasi dan memimpin dalam lingkungan kerja.

Dampak Positif dari Komitmen terhadap Pengembangan Diri

Komitmen terhadap pengembangan diri memiliki dampak positif yang signifikan baik bagi individu maupun organisasi. Individu yang aktif dalam pengembangan diri cenderung memiliki tingkat kepuasan kerja yang lebih tinggi dan lebih mampu mengatasi stres serta tantangan di tempat kerja. Menurut research oleh Noe (2010) dalam *Employee Training and Development*, investasi dalam pengembangan karyawan tidak hanya meningkatkan keterampilan mereka tetapi juga meningkatkan komitmen mereka terhadap organisasi (Noe, 2010). Hal ini menunjukkan bahwa pengembangan diri yang berkelanjutan dapat menciptakan hubungan yang lebih kuat antara karyawan dan organisasi.

1.3.4 Kode Etik Profesi

Pengertian Kode Etik Profesi

Kode etik profesi adalah seperangkat prinsip dan norma yang mengatur perilaku profesional dalam suatu bidang tertentu. Kode ini berfungsi sebagai pedoman moral yang membantu individu dalam membuat keputusan yang etis dan bertanggung jawab dalam praktik mereka. Menurut Richard T. DeGeorge dalam bukunya *Business Ethics*, kode etik menetapkan standar yang diharapkan dari anggota profesi, sehingga menciptakan kepercayaan antara profesional dan masyarakat (DeGeorge, 1999). Kode etik menjadi fondasi bagi integritas dan kredibilitas suatu profesi.

Fungsi Kode Etik

Kode etik memiliki beberapa fungsi penting dalam profesi. Pertama, kode etik memberikan pedoman bagi perilaku profesional yang diharapkan, membantu anggota profesi dalam menghadapi situasi yang sulit. Menurut Beauchamp dan Childress (2001) dalam *Principles of Biomedical Ethics*, kode etik berfungsi untuk menetapkan standar yang jelas mengenai apa yang dianggap benar dan salah dalam praktik profesional (Beauchamp & Childress, 2001). Kedua, kode etik juga berfungsi untuk melindungi kepentingan publik dengan memastikan bahwa para profesional bertindak dengan integritas dan dalam batasan etika yang telah ditentukan.

Komponen Kode Etik

Kode etik biasanya terdiri dari beberapa komponen utama, termasuk prinsip dasar, nilai-nilai inti, dan pedoman perilaku. Menurut Wilmot (2009) dalam *Ethics in the Workplace*, prinsip dasar seperti kejujuran, keadilan, dan tanggung jawab sosial sering kali menjadi inti dari kode etik profesional (Wilmot,

2009). Selain itu, kode etik juga mencakup pedoman yang lebih spesifik yang mengatur interaksi antara profesional dan klien, kolega, serta masyarakat umum.

Peran Kode Etik dalam Pengambilan Keputusan

Kode etik berperan penting dalam pengambilan keputusan etis di tempat kerja. Dalam situasi yang kompleks, di mana mungkin terdapat konflik kepentingan atau dilema moral, kode etik memberikan kerangka kerja untuk mengevaluasi pilihan dan konsekuensinya. Menurut Hunt dan Vitell (1986) dalam *A General Theory of Marketing Ethics*, kode etik membantu profesional dalam menavigasi tantangan etis dan mempertimbangkan dampak tindakan mereka terhadap semua pemangku kepentingan (Hunt & Vitell, 1986). Dengan demikian, kode etik berfungsi sebagai kompas moral yang membimbing perilaku profesional.

1.3.5 Dampak Profesi terhadap Masyarakat

Profesi memiliki peran penting dalam membentuk struktur sosial dan ekonomi masyarakat. Setiap profesi, mulai dari dokter, guru, hingga insinyur, memberikan kontribusi yang berbeda terhadap perkembangan masyarakat. Secara umum, dampak profesi dapat dilihat dari segi ekonomi, sosial, dan budaya.

Dampak Ekonomi

Profesi-profesi tertentu, seperti pengusaha dan profesional di bidang teknologi, secara langsung mempengaruhi pertumbuhan ekonomi. Pengusaha menciptakan lapangan kerja, sementara profesional teknologi mendorong inovasi yang meningkatkan produktivitas. Menurut laporan World Economic Forum (2021), sektor teknologi informasi dan komunikasi menyumbang lebih dari 10% produk

domestik bruto (PDB) global, menunjukkan betapa signifikan peran profesi ini dalam ekonomi (World Economic Forum, 2021).

Dampak Sosial

Sektor pendidikan, diwakili oleh profesi guru, memiliki dampak sosial yang mendalam. Pendidikan yang berkualitas membantu meningkatkan kesadaran masyarakat akan isu-isu sosial, kesehatan, dan lingkungan. Penelitian oleh UNESCO (2020) menunjukkan bahwa akses pendidikan yang baik mengurangi ketimpangan sosial dan meningkatkan partisipasi masyarakat dalam proses demokrasi (UNESCO, 2020).

Dampak Kesehatan

Profesi di bidang kesehatan, terutama dokter dan perawat, memainkan peran kunci dalam meningkatkan kualitas hidup masyarakat. Mereka tidak hanya merawat penyakit, tetapi juga berkontribusi dalam pencegahan penyakit melalui edukasi kesehatan. Menurut Organisasi Kesehatan Dunia (WHO, 2021), sistem kesehatan yang kuat dan tenaga kesehatan yang terlatih berhubungan langsung dengan penurunan angka kematian dan peningkatan kesehatan masyarakat secara keseluruhan (WHO, 2021).

Dampak Budaya

Profesi di bidang seni dan budaya, seperti seniman, penulis, dan musisi, memberikan dampak yang besar dalam memperkaya warisan budaya masyarakat. Mereka menciptakan karya yang tidak hanya menghibur tetapi juga mengedukasi dan membangkitkan kesadaran akan nilai-nilai budaya. Sebuah studi oleh Arts Council England (2019) menunjukkan bahwa keterlibatan dalam seni dan budaya meningkatkan kohesi sosial

dan mengurangi ketegangan dalam masyarakat (Arts Council England, 2019).

Dampak Lingkungan

Dengan meningkatnya kesadaran akan isu-isu lingkungan, profesi di bidang lingkungan, seperti ahli lingkungan dan insinyur lingkungan, semakin penting. Mereka berkontribusi dalam merancang solusi untuk masalah lingkungan, seperti perubahan iklim dan pencemaran. Menurut laporan dari Intergovernmental Panel on Climate Change (IPCC, 2022), tindakan profesional di bidang ini sangat penting untuk mencapai tujuan keberlanjutan dan mitigasi perubahan iklim (IPCC, 2022).

1.4 Ciri Khas Profesi

Setiap profesi memiliki ciri khas yang membedakannya dari bidang pekerjaan lainnya. Ciri-ciri ini mencakup keahlian, tanggung jawab, etika, pendidikan, dan pengakuan sosial. Memahami ciri khas profesi sangat penting untuk menghargai peran yang dimainkan dalam masyarakat.

1. Keahlian dan Kompetensi

   Salah satu ciri khas utama dari setiap profesi adalah keahlian dan kompetensi yang spesifik. Profesional dalam bidang tertentu memiliki pengetahuan dan keterampilan yang diperlukan untuk menjalankan tugas mereka. Misalnya, seorang dokter harus memahami anatomi manusia dan prosedur medis, sementara seorang insinyur harus memiliki pemahaman mendalam tentang prinsip-prinsip teknik. Menurut Schmidt dan Hunter (1998), keahlian yang tepat dan pelatihan yang mendalam berkontribusi signifikan terhadap kinerja dalam profesi tertentu (Schmidt & Hunter, 1998).

2. Tanggung Jawab Profesional

   Setiap profesi juga memiliki tanggung jawab yang jelas terhadap klien, masyarakat, dan lingkungan. Tanggung jawab ini sering diatur oleh kode etik yang mengharuskan profesional untuk bertindak dengan integritas dan transparansi. Misalnya, jurnalis diharuskan untuk melaporkan informasi dengan akurat dan objektif. Menurut Davis (1996), etika profesi membantu menjaga kepercayaan publik terhadap profesi tersebut dan mendorong standar tinggi dalam praktik profesional (Davis, 1996).

3. Pendidikan dan Pelatihan

   Sebagian besar profesi memerlukan pendidikan formal dan pelatihan yang spesifik. Pendidikan ini tidak hanya mencakup teori, tetapi juga praktik di lapangan. Contohnya, seorang guru harus memiliki gelar pendidikan dan pengalaman mengajar sebelum diakui sebagai profesional. Menurut Baird dan Zacker (2018), pendidikan dan pelatihan yang tepat sangat penting untuk mempersiapkan individu dalam menjalankan tanggung jawab profesional mereka (Baird & Zacker, 2018).

4. Sertifikasi dan Lisensi

   Banyak profesi memerlukan sertifikasi atau lisensi resmi untuk memastikan bahwa individu yang berpraktik memenuhi standar tertentu. Ini berlaku untuk profesi seperti dokter, pengacara, dan akuntan. Proses sertifikasi ini mencakup ujian dan penilaian keterampilan. Menurut National Council of Examiners for Engineering and Surveying (NCEES, 2021), sertifikasi membantu melindungi masyarakat dengan memastikan bahwa hanya individu yang memenuhi syarat yang diizinkan untuk menjalankan tugas profesional tertentu (NCEES, 2021).

5. Pengakuan Sosial

   Profesi tertentu sering kali memiliki tingkat pengakuan sosial yang tinggi, tergantung pada kontribusi mereka terhadap masyarakat. Profesi yang dianggap penting, seperti dokter dan guru, sering kali dihormati dan dianggap sebagai pilar masyarakat. Menurut penelitian oleh the Pew Research Center (2019), masyarakat cenderung menghargai profesi yang berkontribusi langsung pada kesejahteraan dan pendidikan, yang berdampak positif terhadap persepsi publik terhadap profesi tersebut (Pew Research Center, 2019).

6. Komunitas Profesional

   Setiap profesi biasanya memiliki komunitas atau asosiasi profesional yang memberikan dukungan, jaringan, dan kesempatan untuk pengembangan berkelanjutan. Komunitas ini sering menyelenggarakan seminar, lokakarya, dan konferensi untuk berbagi pengetahuan dan pengalaman. Menurut Larsson dan Hällgren (2016), asosiasi profesional memainkan peran penting dalam mengembangkan standar praktik, etika, dan kolaborasi antar anggota (Larsson & Hällgren, 2016).

DAFTAR PUSTAKA

Rachels, James, & Rachels, Stuart. (2019). The Elements of Moral Philosophy. McGraw-Hill Education.

Singer, Peter. (2011). Practical Ethics. Cambridge University Press.

Velasquez, Manuel. (2017). Business Ethics: Concepts and Cases. Pearson.

Beauchamp, Tom L., & Childress, James F. (2019). Principles of Biomedical Ethics. Oxford University Press.

Toffler, A. (1970). Future Shock. Bantam Books.

Abbot, A. (1988). The System of Professions. University of Chicago Press.

Schön, D. A. (1983). The Reflective Practitioner: How Professionals Think in Action. Basic Books.

DeGeorge, R. T. (1999). Business Ethics. Prentice Hall.

Freidson, E. (2001). Professionalism: The Third Logic. University of Chicago Press.

Schmidt, F. L., & Hunter, J. E. (1998). The validity of general cognitive ability in predicting academic performance: A meta-analysis. Psychological Bulletin, 124(2), 262-274. Link

Davis, M. (1996). The Role of Ethics in Professional Life. Professional Ethics: A Multidisciplinary Journal, 4(1), 1-16. Link

Baird, L. L., & Zacker, K. (2018). Education and training in the professions: The role of field experience. Journal of Career Development, 45(2), 149-162. Link

National Council of Examiners for Engineering and Surveying (NCEES). (2021). Licensure. Link

Pew Research Center. (2019). The State of Professions: Public Perceptions and Expectations. Link

Larsson, A., & Hällgren, M. (2016). Professional communities in practice: The role of professional associations in learning and knowledge sharing. Journal of Workplace Learning, 28(1), 33-47

BAB 2
PENGERTIAN PROFESIONALISME, CIRI-CIRI PROFESIONALISME, DAN KODE ETIK PROFESIONAL

Dalam dunia informatika, profesionalisme menjadi landasan penting untuk menjaga standar mutu pekerjaan, melindungi masyarakat, dan menjunjung tinggi integritas profesi. Profesionalisme bukan hanya soal kemampuan teknis, tetapi juga melibatkan nilai-nilai yang membentuk karakter seorang profesional sejati.

Bab ini akan mengupas tiga aspek utama terkait profesionalisme: pengertian profesionalisme, ciri-ciri yang menjadi penanda seorang profesional, serta kode etik profesional yang menjadi panduan dalam menjalankan tugas di bidang informatika.

2.1 Pendahuluan

Di era modern ini, profesionalisme menjadi sangat penting untuk keberhasilan setiap bidang pekerjaan, termasuk informatika. Sebagai pekerjaan yang sangat berubah-ubah, informatika tidak hanya membutuhkan kemampuan teknis. Pelakunya juga harus memiliki integritas, tanggung jawab, dan kemampuan untuk bertindak secara etis saat menghadapi tantangan. Profesionalisme telah menjadi dasar bagi setiap orang yang ingin dianggap kompeten dan kredibel di bidang ini.

Dibandingkan dengan profesi lain, definisi "profesionalisme" jauh lebih rumit dalam informatika. Hal ini disebabkan oleh fakta bahwa pekerjaan di bidang ini sangat berkaitan dengan hal-hal yang sangat penting bagi manusia, seperti privasi data, keamanan siber, dan bagaimana teknologi memengaruhi masyarakat secara keseluruhan (Husna *et al.*, 2021). Akibatnya, profesionalisme tidak hanya mencakup kemampuan teknis, tetapi juga kemampuan untuk bertindak secara moral dan mengutamakan kepentingan publik.

Bab ini akan membahas konsep profesionalisme secara menyeluruh, dari definisi, kemudian ciri-ciri penting seseorang dapat disebut professional, dan juga kode etik professional.

2.2 Pengertian Profesionalisme

Dalam kehidupan sehari-hari, istilah profesionalisme sering kali diartikan sebagai kemampuan seseorang untuk menjalankan pekerjaan atau tanggung jawabnya dengan baik. Namun, profesionalisme bukan hanya tentang keterampilan teknis atau hasil kerja yang sempurna. Profesionalisme mencakup seperangkat nilai, sikap, dan perilaku yang menunjukkan komitmen terhadap standar kualitas, etika, dan tanggung jawab moral dalam pekerjaan (Yusuf and Syarif, 2018).

Secara etimologis, istilah "profesionalisme" berasal dari kata "profesi," yang pada awalnya merujuk pada sumpah atau janji untuk melayani masyarakat dengan pengetahuan dan keahlian khusus. Dalam konteks modern, profesionalisme menjadi sebuah prinsip yang mengatur bagaimana seseorang bertindak dan berpikir dalam menjalankan perannya secara bertanggung jawab, terlepas dari bidang pekerjaannya (Saleng, 2021).

Beberapa ahli telah memberikan definisi yang beragam mengenai profesionalisme. Tabel 2.1 memuat definisi dari berbagai perspektif, sekaligus menyoroti aspek penting yang ditekankan oleh masing-masing ahli.

Tabel 2.1. Definisi Profesionalisme Menurut Para Ahli.

No.	Ahli	Definisi Profesionalisme	Catatan Penting
1	Hoyle (1995)	Profesionalisme adalah sikap yang mengacu pada standar perilaku tertentu yang diharapkan dari seseorang dalam profesinya.	Menekankan pada aspek sikap dan perilaku yang sesuai dengan standar profesi.
2	Evans (2008)	Profesionalisme adalah kombinasi dari komitmen terhadap nilai-nilai kerja, penguasaan keahlian, dan kemampuan untuk menjunjung tanggung jawab sosial.	Menggarisbawahi tiga elemen utama: nilai kerja, keahlian teknis, dan tanggung jawab sosial.
3	Eraut (1994)	Profesionalisme adalah pengembangan standar kerja melalui pelatihan, pengalaman, dan pembelajaran berkelanjutan.	Fokus pada pengembangan diri melalui proses pembelajaran yang berkesinambungan.
4	Saks (2016)	Profesionalisme adalah keterlibatan emosional, etika, dan komitmen individu dalam pekerjaan yang berkualitas tinggi sesuai dengan kebutuhan masyarakat.	Menghubungkan profesionalisme dengan komitmen etis dan kepentingan publik.

Definisi dalam tabel di atas menyoroti bahwa profesionalisme tidak hanya mencakup kompetensi teknis semata, tetapi juga sikap, nilai-nilai moral, serta tanggung

jawab sosial. Hoyle (Eric Hoyle, 1995) menekankan pentingnya sikap dan perilaku sebagai elemen utama profesionalisme, sementara Evans (Linda Evans, 2008) memperluas pandangan dengan memasukkan komitmen terhadap nilai kerja dan tanggung jawab sosial. Eraut (Michael Eraut, 1994) menambahkan aspek penting lain, yaitu pembelajaran berkelanjutan, yang relevan dalam bidang informatika yang terus berkembang. Terakhir, Saks (Mike Saks, 2014) menghubungkan profesionalisme dengan kepentingan masyarakat dan komitmen etis, yang merupakan fondasi dalam pengembangan teknologi yang bertanggung jawab.

Profesionalisme dalam Konteks Informatika

Dalam dunia informatika, profesionalisme memiliki arti yang lebih kompleks. Tidak hanya berkaitan dengan kemampuan teknis, profesionalisme juga berhubungan dengan tanggung jawab untuk memahami dampak teknologi terhadap masyarakat dan ekosistem global. Pekerjaan di bidang ini sering kali melibatkan keputusan yang berdampak luas, seperti keamanan data, privasi, dan etika penggunaan teknologi.

Sebagai contoh, seorang pengembang perangkat lunak yang merancang aplikasi pengelola data pribadi harus mempertimbangkan keamanan dan privasi pengguna sebagai prioritas. Kelalaian melindungi data pengguna dapat menimbulkan pelanggaran privasi yang merugikan banyak orang. Dalam konteks ini, profesionalisme tidak hanya berarti mampu membuat kode yang efisien, tetapi juga memahami dampaknya terhadap masyarakat dan mematuhi standar kode etik yang berlaku (Nurdin, 2017).

Contoh Praktik Profesionalisme dalam Dunia Informatika

Salah satu contoh profesionalisme dalam informatika adalah ketika seorang profesional keamanan siber dihadapkan pada pelanggaran data sensitif. Alih-alih menyembunyikan insiden demi menjaga reputasi perusahaan, profesional yang bertanggung jawab akan melaporkan pelanggaran tersebut kepada otoritas terkait, memberi tahu pihak-pihak terdampak, dan memastikan langkah-langkah pencegahan dilakukan untuk mencegah insiden serupa di masa depan. Sikap seperti ini menunjukkan bahwa profesionalisme dalam informatika tidak hanya berfokus pada keterampilan teknis, tetapi juga komitmen terhadap transparansi dan kepentingan publik.

2.3 Ciri-Ciri Profesionalisme

Profesionalisme bukan hanya sebuah konsep abstrak, tetapi diwujudkan melalui karakteristik dan perilaku nyata yang dimiliki oleh seorang individu dalam profesinya. Dalam bidang informatika, ciri-ciri profesionalisme menjadi panduan utama yang membedakan antara seseorang yang hanya memiliki kemampuan teknis dengan individu yang dianggap sebagai seorang profesional sejati.

Subbab ini membahas lima ciri utama profesionalisme: kompetensi teknis, tanggung jawab, integritas dan kejujuran, keterbukaan terhadap kritik serta pembelajaran berkelanjutan, dan kemampuan berkomunikasi serta bekerja dalam tim.

2.3.1 Kompetensi Teknis

Kompetensi teknis adalah fondasi utama dari profesionalisme. Dalam profesi informatika, kompetensi ini mencakup penguasaan pengetahuan, keterampilan, dan keahlian yang relevan dengan bidang yang digeluti. Seorang profesional informatika diharapkan tidak hanya memahami teori-teori dasar, tetapi juga mampu menerapkannya dalam

situasi nyata untuk menyelesaikan masalah dengan cara yang efisien dan efektif.

Pentingnya kompetensi teknis dalam profesionalisme dapat dilihat pada kebutuhan untuk:

1. Mengikuti perkembangan teknologi: Teknologi informasi terus berubah dengan cepat, sehingga seorang profesional harus selalu memperbarui keterampilannya agar tetap relevan.
2. Mengelola risiko teknologi: Sebagai contoh, seorang insinyur perangkat lunak harus mampu mengidentifikasi dan mengatasi potensi bug atau masalah keamanan dalam aplikasi yang mereka kembangkan.
3. Menghasilkan solusi yang dapat diandalkan: Kompetensi teknis memastikan bahwa sistem yang dibuat memiliki kualitas tinggi, aman, dan dapat diandalkan oleh pengguna.

Kompetensi teknis bukan hanya tentang keahlian teknis, tetapi juga kemampuan untuk beradaptasi dan memanfaatkan teknologi baru demi memenuhi kebutuhan masyarakat dan organisasi.

2.3.2 Tanggung Jawab

Tanggung jawab adalah inti dari profesionalisme. Dalam profesi informatika, tanggung jawab tidak hanya terbatas pada penyelesaian pekerjaan yang diberikan, tetapi juga mencakup kepedulian terhadap dampak yang ditimbulkan oleh teknologi terhadap masyarakat.

Seorang profesional informatika memiliki tanggung jawab di tiga aspek utama:

1. Tanggung jawab terhadap pekerjaan: Seorang profesional harus menyelesaikan tugas dengan penuh dedikasi, sesuai dengan standar kualitas yang telah disepakati.
2. Tanggung jawab terhadap masyarakat: Dalam merancang teknologi, profesional harus mempertimbangkan dampaknya terhadap pengguna dan masyarakat secara keseluruhan. Sebagai contoh, seorang pengembang sistem pembayaran digital harus memastikan bahwa sistemnya aman dan tidak memudahkan penipuan.
3. Tanggung jawab terhadap dampak teknologi: Setiap teknologi yang diciptakan memiliki potensi untuk memberikan dampak positif maupun negatif. Seorang profesional bertanggung jawab untuk meminimalkan risiko negatif, seperti pelanggaran privasi atau kerusakan lingkungan.

Tanggung jawab profesional juga mencakup keberanian untuk mengambil tindakan yang benar, bahkan ketika keputusan tersebut sulit atau berisiko.

2.3.3 Integritas dan Kejujuran

Integritas dan kejujuran adalah nilai utama yang mendasari profesionalisme. Dalam dunia informatika, di mana keputusan teknis dapat memiliki konsekuensi besar, kejujuran dan moralitas menjadi sangat penting.

Integritas dalam profesi informatika tercermin melalui:

1. Kejujuran dalam pelaporan: Seorang profesional harus jujur dalam melaporkan hasil pekerjaannya, baik berhasil maupun gagal. Misalnya, jika Tim Keamanan Jaringan menemukan potensi pelanggaran keamanan, ia harus melaporkannya meskipun dapat merugikan reputasi perusahaan.

2. Konsistensi dengan kode etik: Profesional yang berintegritas akan bertindak sesuai dengan kode etik yang berlaku, bahkan dalam situasi yang penuh tekanan.
3. Menolak penyalahgunaan keahlian: Seorang profesional yang berintegritas tidak akan menggunakan pengetahuannya untuk tujuan yang melanggar hukum atau merugikan orang lain, seperti peretasan atau pencurian data.

Integritas memastikan bahwa seorang profesional tidak hanya menghasilkan pekerjaan yang berkualitas, tetapi juga menjaga kepercayaan masyarakat terhadap profesi mereka.

2.3.4 Keterbukaan terhadap Kritik

Dalam dunia informatika yang terus berkembang, keterbukaan terhadap kritik dan pembelajaran berkelanjutan adalah ciri penting dari seorang profesional. Seorang profesional sejati tidak pernah berhenti belajar, baik dari pengalaman pribadi, masukan orang lain, maupun perkembangan teknologi baru.

Beberapa aspek dari keterbukaan terhadap kritik dan pembelajaran berkelanjutan adalah:

1. Kemauan untuk menerima umpan balik: Kritik yang konstruktif membantu profesional untuk meningkatkan kualitas pekerjaan mereka. Misalnya, dalam pengembangan perangkat lunak, sesi tinjauan kode (*code review*) memungkinkan pengembang untuk memperbaiki kesalahan dan meningkatkan efisiensi kode mereka.
2. Komitmen terhadap pembelajaran seumur hidup: Seorang profesional informatika harus terus mempelajari teknologi baru, seperti kecerdasan buatan, blockchain, atau keamanan siber, agar tetap relevan di dunia kerja.

3. Kemampuan beradaptasi: Keterbukaan terhadap perubahan memungkinkan profesional untuk menghadapi tantangan baru dengan solusi yang inovatif.

Dengan sikap ini, profesional tidak hanya berkembang secara individu, tetapi juga berkontribusi lebih besar bagi organisasi dan masyarakat.

2.3.5 Kemampuan Berkomunikasi dan Bekerja dalam Tim

Kemampuan teknis saja tidak cukup untuk menjadikan seseorang seorang profesional sejati. Dalam banyak kasus, pekerjaan di bidang informatika membutuhkan kolaborasi dengan berbagai pihak, baik itu anggota tim, pemangku kepentingan, maupun pengguna akhir. Oleh karena itu, kemampuan berkomunikasi dan bekerja dalam tim menjadi ciri yang sangat penting.

Kemampuan ini mencakup:

1. Komunikasi yang efektif: Profesional harus mampu menjelaskan konsep teknis yang kompleks dalam bahasa yang mudah dipahami oleh orang-orang dari latar belakang non-teknis (Suryanto, 2019).
2. Kolaborasi lintas disiplin: Dalam proyek pengembangan sistem, seorang profesional informatika mungkin harus bekerja sama dengan desainer produk, analis bisnis, dan bahkan ahli hukum. Kemampuan untuk bekerja dalam tim lintas disiplin adalah kunci keberhasilan.
3. Mengelola konflik: Dalam tim, perbedaan pendapat adalah hal yang biasa. Seorang profesional sejati harus mampu mengelola konflik dengan cara yang konstruktif dan menemukan solusi yang terbaik bagi semua pihak.

Kemampuan komunikasi dan kolaborasi ini memastikan bahwa hasil pekerjaan tidak hanya memuaskan dari segi teknis, tetapi juga relevan dan bermanfaat bagi pengguna.

Ciri-ciri profesionalisme yang telah diuraikan mencerminkan bahwa profesionalisme bukan hanya tentang keterampilan teknis, tetapi juga mencakup tanggung jawab, integritas, keterbukaan terhadap kritik, dan kemampuan bekerja dalam tim. Dalam profesi informatika, ciri-ciri ini menjadi landasan untuk menghasilkan teknologi yang berkualitas tinggi dan bertanggung jawab terhadap masyarakat.

2.4 Kode Etik Profesional

Dalam dunia profesional, keberadaan kode etik menjadi elemen mendasar yang berfungsi sebagai pedoman moral bagi setiap individu dalam menjalankan tugas dan tanggung jawabnya. Di bidang informatika, kode etik tidak hanya berfungsi untuk mengatur perilaku profesional, tetapi juga untuk menjaga keseimbangan antara pengembangan teknologi dengan dampak sosialnya. Subbab ini akan membahas pengertian kode etik profesional, pentingnya kode etik dalam profesi informatika, beberapa contoh kode etik yang digunakan di bidang ini, serta penerapannya dalam praktik nyata.

2.4.1 Pengertian Kode Etik Profesional

Kode etik profesional adalah serangkaian prinsip, nilai, dan aturan tertulis yang dirancang untuk mengatur perilaku individu dalam sebuah profesi. Kode etik bertujuan untuk memastikan bahwa para profesional bertindak secara konsisten dengan standar moral dan nilai-nilai yang telah disepakati

dalam profesi tersebut (Dr. Syarifah Normawati, M.Pd.I, Sudirman Anwar, M.Pd.I, Selpi Indramaya, 2019).

Menurut Sarah Jane Banks, kode etik adalah dokumen formal yang memberikan panduan tentang tindakan yang diharapkan dari seorang profesional dalam konteks tanggung jawab mereka kepada masyarakat, kolega, dan organisasi tempat mereka bekerja (Banks, 2012). Dalam pengertian ini, kode etik menjadi kompas moral yang membantu profesional menghadapi dilema etis yang mungkin muncul dalam pekerjaan mereka.

Fungsi utama kode etik adalah:

1. Mengatur perilaku profesional: Kode etik memberikan pedoman tentang apa yang dianggap benar atau salah dalam suatu profesi.
2. Melindungi kepentingan publik: Dengan adanya kode etik, profesi tertentu dapat memastikan bahwa praktik yang dilakukan tidak merugikan masyarakat.
3. Meningkatkan kepercayaan masyarakat: Kode etik membantu membangun kredibilitas profesi di mata publik.
4. Mencegah penyalahgunaan kekuasaan atau wewenang: Dengan adanya aturan yang jelas, profesional dapat bertanggung jawab atas tindakan mereka.

Kode etik profesional dalam informatika menjadi semakin penting mengingat profesi ini sering melibatkan pengelolaan data sensitif, desain teknologi yang memengaruhi masyarakat luas, dan keputusan yang berpotensi menimbulkan dilema etis (Dr. Muhammad Ridha Albaar, 2021).

2.4.2 Pentingnya Kode Etik dalam Profesi Informatika

Profesi informatika memiliki pengaruh yang signifikan terhadap berbagai aspek kehidupan, mulai dari cara

masyarakat mengakses informasi hingga bagaimana data pribadi dikelola dan digunakan. Dalam konteks ini, kode etik menjadi instrumen penting untuk memastikan bahwa pengembangan teknologi dilakukan secara bertanggung jawab dan berorientasi pada kepentingan publik.

Pentingnya kode etik dalam profesi informatika dapat dirangkum sebagai berikut:

1. Membangun kepercayaan publik: Dalam dunia yang semakin digital, masyarakat perlu merasa yakin bahwa teknologi yang mereka gunakan diciptakan dan dikelola oleh profesional yang memprioritaskan keamanan, kejujuran, dan tanggung jawab.
2. Menjaga profesionalisme: Kode etik membantu memastikan bahwa setiap individu dalam profesi informatika mengikuti standar yang sama, sehingga meningkatkan kualitas dan integritas pekerjaan.
3. Memandu pengambilan keputusan dalam situasi sulit: Di tengah dilema etis, seperti apakah akan melaporkan kebocoran data atau bagaimana menangani algoritma yang bias, kode etik memberikan panduan tentang tindakan yang benar.
4. Mengurangi risiko hukum dan reputasi: Kode etik yang diterapkan dengan baik dapat mencegah tindakan yang melanggar hukum atau merusak reputasi organisasi.

2.4.3 Contoh Kode Etik Profesional di Bidang Informatika

Dalam bidang informatika, terdapat beberapa kode etik yang diakui secara internasional maupun nasional. Beberapa di antaranya adalah sebagai berikut:

1. ACM *Code of Ethics and Professional Conduct Association for Computing Machinery* (ACM) menetapkan kode etik yang menyoroti empat prinsip utama:

menghormati kepentingan publik, menjunjung tinggi kejujuran dan keadilan, memberikan kualitas terbaik, dan memelihara profesionalisme. Contohnya, prinsip pertama menyatakan bahwa seorang profesional informatika harus menghindari menyakiti orang lain melalui pekerjaannya, misalnya dengan memastikan keamanan data (Machinery, 2018).

2. IEEE Code of Ethics
   Institute of Electrical and Electronics Engineers (IEEE) juga memiliki kode etik yang relevan untuk para profesional di bidang informatika. Kode ini menekankan tanggung jawab untuk meningkatkan kesejahteraan masyarakat, menghindari konflik kepentingan, dan memberikan informasi yang jujur dan realistis kepada publik (IEEE, 2020).
3. Kode Etik Nasional
   Di Indonesia, asosiasi seperti Ikatan Ahli Informatika Indonesia (IAII) memiliki kode etik yang mencakup tanggung jawab terhadap masyarakat, kolega, dan profesi itu sendiri. Kode etik ini berfungsi untuk memastikan bahwa para profesional informatika di Indonesia mematuhi nilai-nilai moral dan hukum yang berlaku secara lokal (Ikatan Ahli Informatika Indonesia, no date).

Tabel 2.2. Contoh Kode Etik Profesional di Bidang Informatika.

Kode Etik	Prinsip Utama	Contoh Implementasi
ACM Code of Ethics	Menghormati kepentingan publik	Menjaga privasi data pengguna dalam sistem online.
IEEE Code of Ethics	Meningkatkan kesejahteraan masyarakat	Menghindari penggunaan algoritma yang bias terhadap kelompok tertentu.
IAII (Kode Etik Nasional)	Tanggung jawab terhadap masyarakat dan profesi	Memastikan sistem teknologi sesuai dengan hukum dan budaya lokal.

2.4.4 Implementasi Kode Etik dalam Praktik

Penerapan kode etik dalam pekerjaan informatika menjadi langkah penting untuk memastikan bahwa setiap keputusan dan tindakan yang diambil tidak hanya tepat secara teknis tetapi juga etis. Beberapa contoh implementasi kode etik dalam praktik nyata antara lain:

1. Privasi Data
   Seorang pengembang perangkat lunak yang bekerja di perusahaan media sosial harus memastikan bahwa data pengguna dilindungi sesuai dengan kebijakan privasi. Ketika menghadapi tekanan untuk menjual data pengguna kepada pihak ketiga tanpa persetujuan, kode etik memberikan panduan untuk menolak tindakan tersebut.
2. Pengelolaan AI
   Dalam pengembangan teknologi kecerdasan buatan (AI), profesional informatika harus memastikan bahwa sistem yang dirancang tidak menghasilkan bias yang merugikan kelompok tertentu. Misalnya, sistem rekrutmen berbasis AI

harus diuji untuk memastikan bahwa algoritma tidak diskriminatif terhadap jenis kelamin, ras, atau faktor lainnya.

3. Keamanan Siber
   Ketika menghadapi pelanggaran data, seorang profesional keamanan siber harus melaporkan insiden tersebut kepada pihak terkait, meskipun hal ini dapat berdampak pada reputasi perusahaan. Transparansi dalam menangani insiden seperti ini menjadi contoh nyata penerapan kode etik.

2.5 Ilustrasi Profesionalisme dalam Informatika

Ilustrasi ini bertujuan memberikan gambaran konkret bagaimana prinsip profesionalisme dan kode etik dapat diterapkan dalam praktik, serta dampaknya terhadap masyarakat dan profesi.

Kasus: Pelanggaran Data Pengguna pada Aplikasi E-Commerce

Sebuah platform e-commerce, BelanjaOnline.id, menghadapi insiden kebocoran data pelanggan yang melibatkan informasi pribadi seperti nama, nomor telepon, dan riwayat pembelian. Insiden ini terjadi setelah seorang karyawan IT tidak sengaja meninggalkan celah keamanan dalam pengelolaan server yang menyebabkan pihak ketiga dengan mudah mengakses data pelanggan.

Perusahaan awalnya ragu untuk melaporkan insiden tersebut. Beberapa anggota manajemen khawatir bahwa pengungkapan akan merusak kepercayaan pelanggan dan mengundang denda dari regulator. Namun, kepala divisi IT mendesak perusahaan untuk bertindak secara transparan. Ia berargumen bahwa menyembunyikan insiden ini akan

melanggar prinsip profesionalisme dan kode etik, khususnya terkait tanggung jawab terhadap pelanggan.

Setelah diskusi intens, manajemen memutuskan untuk:

1. Memberitahukan insiden ini kepada pelanggan melalui email resmi.
2. Melaporkan insiden tersebut kepada Kementerian Komunikasi dan Informatika (Kominfo) sesuai dengan regulasi perlindungan data di Indonesia.
3. Memberikan langkah mitigasi berupa saran kepada pelanggan untuk mengganti kata sandi dan menawarkan layanan keamanan tambahan secara gratis selama tiga bulan.

Analisis Kasus

Keputusan ini mencerminkan penerapan prinsip profesionalisme dan kode etik bidang informatika:

1. Tanggung Jawab terhadap Masyarakat
   Kepala Divisi dan tim IT menunjukkan tanggung jawab dengan mendesak perusahaan untuk memberi tahu pelanggan dan regulator, sehingga pelanggan dapat mengambil langkah pencegahan. Hal ini selaras dengan nilai-nilai yang diatur dalam kode etik seperti Ikatan Ahli Informatika Indonesia (IAII).
2. Integritas dan Kejujuran
   Keputusan untuk bersikap transparan menunjukkan komitmen perusahaan terhadap integritas. Meskipun berdampak pada reputasi jangka pendek, langkah ini membantu membangun kepercayaan pelanggan di masa depan.
3. Kepatuhan terhadap Regulasi Lokal
   Di Indonesia, regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) menuntut perusahaan

untuk melaporkan pelanggaran data kepada otoritas terkait. Kepatuhan terhadap aturan ini merupakan cerminan profesionalisme perusahaan.

Dampak positif dari kasus ini adalah pelanggan merasa dihargai karena perusahaan bersikap jujur, dan juga langkah mitigasi meningkatkan perlindungan pelanggan di masa depan. Walaupun perusahaan mengalami kerugian reputasi sementara akibat pemberitaan insiden ini.

Studi kasus ini menegaskan pentingnya profesionalisme dalam menghadapi dilema etika, khususnya di industri teknologi di Indonesia. Profesionalisme tidak hanya melindungi pelanggan tetapi juga memperkuat kepercayaan publik terhadap industri secara keseluruhan.

DAFTAR PUSTAKA

Banks, S. (2012) *Ethics and Values in Social Work*. Palgrave Macmillan.

Dr. Muhammad Ridha Albaar, S. K. M. K. (2021) *ETIKA PROFESI INFORMATIKA*. uwais inspirasi indonesia.

Dr. Syarifah Normawati, M.Pd.I, Sudirman Anwar, M.Pd.I, Selpi Indramaya, M. P. . (2019) *Etika dan Profesi Keguruan*. PT. INDRAGIRI DOT COM.

Eric Hoyle, P. D. J. (1995) *Professional Knowledge and Professional Practice*. Cassell.

Husna, A. N. *et al.* (2021) *Memberdayakan Masyarakat Digital*. Unimma Press.

IEEE (2020) *IEEE Code of Ethics*. Available at: https://www.ieee.org/about/corporate/governance/p7-8.html (Accessed: 24 November 2024).

Ikatan Ahli Informatika Indonesia (no date) *Kode Etik*. Available at: https://www.iaii.or.id/index.php?model=iaii_content&action=showContent&lang=id&id=c20ad4d76fe97759aa27a0c99bff6710&type=0&title=Kode-Etik (Accessed: 24 November 2024).

Linda Evans (2008) 'Professionalism, Professionality and the Development of Education Professionals', *British Journal of Educational Studies*, 56(1), pp. 20–38. doi: 10.1111/j.1467-8527.2007.00392.x.

Machinery, A. for C. (2018) *ACM Code of Ethics and Professional Conduct*. Available at: https://www.acm.org/code-of-ethics (Accessed: 24 November 2024).

Michael Eraut (1994) 'Developing Professional Knowledge and Competence', *Psychology Press*.

Mike Saks (2014) 'Professions and Professionalism', *Wiley*.

Available at: https://doi.org/10.1002/9781118410868.wbehibs099.

Nurdin, I. (2017) *Etika Pemerintahan: Norma, Konsep, dan Praktek bagi Penyelenggara Pemerintahan*. Lintang Rasi Aksara Books.

Saleng, Z. A. (2021) *KECERDASAN EMOSIONAL PROFESIONALISME GURU DAN PRESTASI BELAJAR SISWA: Buku Berbasis Riset Pendidikan*. Media Nusa Creative (MNC Publishing).

Suryanto, D. (2019) *Effective Leadership Communication*. Gramedia Pustaka Utama.

Yusuf, R. M. and Syarif, D. (2018) *Komitmen Organisasi*. Nas Media Pustaka.

BAB 3
JENIS-JENIS ANCAMAN (THREATS) MELALUI IT, KASUS-KASUS COMPUTER CRIME/CYBER CRIME

3.1 Pendahuluan Jenis-jenis Ancaman (*Threats*) Melalui IT

Ancaman Siber (*Cyber Threat*) Ancaman siber sendiri merupakan potensi kejahatan siber yang dapat terjadi. Ancaman siber sendiri secara garis besar tentu saja segala sesuatu ancaman kejahatan yang dapat dilakukan yang berhubungan dengan suatu teknologi informasi seperti komputer baik dalam perangkat keras ataupun perangkat ringannya. Ancaman siber sendiri memiliki tiga jenis menurut Mcdonnel dan Sayers dalam (Abdul Razaq, 2022) diantaranya adalah:

1. Ancaman perangkat keras atau hardware threat, adalah ancaman penyebab utamanya adalah instalasi suatu perangkat tertentu pada hardware yang bertujuan untuk melakukan kegiatan tertentu di dalam sistem komputer, hasil akhir dari pemasangan perangkat tersebut adalah dapat terjadi gangguan pada jaringan software dan hardware pada suatu komputer.
2. Ancaman perangkat lunak atau software threat, adalah suatu ancaman pada sebuah komputer yang penyebabnya dikarenakan adanya adalah software tertentu yang masuk dan bertujuan untuk melakukan hal-hal ilegal seperti

mencuri, merusak dan memanipulasi informasi ada dalam komputer itu.

3. Ancaman pada data/informasi atau data information threat, merupakan salah satu jenis ancaman yang penyebabnya adalah karena adanya penyebaran beberapa data atau informasi untuk suatu tujuan tertentu.

Perkembangan sistem Informasi membuka celah bagi penjahat siber untuk memberi berbagai ancaman yang bisa merusak keamanan penggunanya. Berbagai macam cara dapat dilakukan oleh pelaku untuk merusak keamanan sistem informasi yang ada di tulis oleh Achmad Mukhlis (2023).

1. Ancaman Fisik (*Physical Threats*)

   Adapun macam-macam ancaman fisik Menurut Digky B.P (2016) dibagi menjadi 3 yaitu : ancaman bencana alam, ancaman lingkungan, ancaman teknis, dan ancaman manusia.

   a. Ancaman Bencana Alam

      Ancaman bencana alam merupakan sumber ancaman yang mencakup wilayah yang luas dan merupakan ancaman bagi datacenter, fasilitas pengolah informasi dan karyawan. Sangat mungkin untuk menilai resiko dari bermacam-macam bencana alam dan mengambil langkah-langkah pencegahan sehingga bencana kehilangan akibat bencana alam bisa dicegah. Ancaman lingkungan meliputi keadaan di mana terjadi perubahan kondisi di lingkungan sekitar data center yang dapat merusak atau menganggu pelayanan sistem informasi dan data yang disimpan

   b. Ancaman lingkungan

      Ancaman lingkungan meliputi keadaan di mana terjadi perubahan kondisi di lingkungan sekitar data center

yang dapat merusak atau menganggu pelayanan sistem informasi dan data yang disimpan.

c. Ancaman teknis

Ancaman teknis seperti contohnya kelistrikan, Listrik merupakan bagian penting bagi aktifitas sebuah sistem informasi. Semua peralatan listrik dan elektronik membutuhkan listrik agar dapat beroperasi. Pasokan listrik yang stabil juga diperlukan agar tidak terjadi kerusakan atau hal-hal yang tidak diinginkan seperti pelayanan yang terganggu. Undervoltage dan overvoltage merupakan gangguan listrik yang dapat mengganggu kegiatan operasional

d. Ancaman Disebabkan Manusia

Ancaman yang ditimbulkan oleh manusia lebih sulit dihadapi dibandingkan dengan ancaman bencana alam, lingkungan dan teknis karena ancaman dari manusia lebih sulit untuk diprediksi. Ancaman yang disebakan oleh manusia telah dirancang secara spesifik untuk mencari celah keamanan yang paling mudah untuk diserang. Vacca (936:2012) mengelompokkan ancaman manusia ke dalam beberapa kategori yaitu Unauthorized Physical Access, Theft, Vandalism, dan Misuse.

2. Ancaman Perangkat Lunak (*Software Threats*)

Cyber Crime merupakan suatu jenis kejahatan dengan level transnasional yang sangat berbahaya karena dapat memicu terjadinya sebuah perang siber atau *Cyber Warfare. Cybercrime* memiliki beberapa jenis atau macam-macam di dalamnya, menurut (Subagyo, 2018: 98-99) cybercrime terdiri atas enam jenis, diantaranya adalah sebagai berikut:

a. *Hacking* adalah suatu jenis kejahatan siber dimana terjadi penerobosan pada suatu program komputer yang dilakukan oleh pihak lain. Seseorang yang melakukan kegiatan hacking ini disebut dengan hacker. Hacker sendiri tentu saja orang dengan keahlian komputer tertentu yang peretasan terhadap komputer lain dan dapat mengakses informasi di dalam komputer lain tersebut.
b. *Cracking* adalah salah satu jenis dari hacking namun dengan tujuan yang buruk. Sedikit berbeda dengan hacking, pada cracking tujuan utamanya adalah pada hasil dari tindakan peretasan komputer. Jika hacker biasanya cukup puas pada level menerobos keamanan komputer, cracker atau sebutan untuk orang yang melakukan cracking melakukan ini untuk menikmati hasil dari peretasan tersebut dan biasanya hasil ini secara finansial seperti melakukan hacking pada kartu kredit dan kemudian melakukan pengambilan dan pencurian uang yang ada di dalamnya.
c. *Cyber Sabotage* merupakan jenis cybercrime dengan cara melakukan sabotase atau gangguan termasuk merusak dan juga menghancurkan baik data-data, sistem jaringan maupun program dalam suatu komputer yang mengakses internet.
d. *Cyber Attack* adalah jenis kejahatan siber yang menyerang dan mengganggu informasi yang ada dalam suatu komputer dengan sengaja. Tindakan ini biasanya memiliki tujuan untuk mengganggu baik secara fisik bahkan sistem dan perangkat lunak yang ada dalam suatu komputer.
e. *Carding* adalah kejahatan siber yang kegiatannya adalah dengan melakukan pembelian barang namun

dengan menggunakan identitas dari orang lain. Data-data ini biasanya didapatkan dengan cara mencuri data identitas seseorang dari internet. Kejahatan ini biasa disebut dengan cyber fraud atau penipuan pada dunia maya.

Spyware adalah program perangkat lunak yang menjadi alat bagi oknum untuk dapat mengakses kegiatan siber di komputer orang lain. Spyware dapat melakukan perekaman pada aktivitas siber dari user komputer tersebut seperti cookies dan juga registry. Kemudian informasi yang telah direkam dan diapatkan ini dapat diperjualbelikan kepada pihak ketiga seperti perusahaan yang dapat digunakan untuk tujuan tertentu seperti penyebaran virus atau mendapatkan tertentu.

3.2 Kasus- Kasus *Computer Crime/Cyber Crime*

Kasus-kasus *computer crime* atau kejahatan komputer merujuk pada berbagai tindakan kriminal yang dilakukan dengan menggunakan komputer atau teknologi informasi. Kejahatan ini dapat berupa pelanggaran terhadap perangkat keras, perangkat lunak, data, atau sistem jaringan. Beberapa bentuk kejahatan siber yang dituliskan oleh Babys (2021) adalah hacking yang merupakan penerobosan kedalam program untuk merusak maupun mencuri data, sabotase yang merupakan proses membuat gangguan dan perusakan data, program, maupun sistem jaringan, spionase yang merupakan penggunaan internet untuk memata matai pihak lain dengan penerobosan sistem jaringan korban, cyber attack yang merupakan proses untuk mengganggu kerahasiaan informasi dan integritas informasi dengan mencuri informasi khusus, garding yang merupakan penggunaan identitas orang lain untuk berbelanja, dan vandalism yang merupakan perusakan

halaman web atau penggunaan denial of service yang merusak sumber daya komputer. Ancaman lain yang ditemukan oleh Laksono (2021) saat melakukan threat modelling pada Universitas XYZ adalah spoofing, tempering, dan repudiation :

1. *Hacking* (Peretasan)
   Hacking adalah tindakan membobol sistem komputer atau jaringan tanpa izin untuk mengakses informasi atau merusak sistem. Para peretas (hackers) dapat memasuki jaringan komputer perusahaan untuk mencuri data sensitif atau untuk merusak sistem.
2. *Phishing* (Penipuan)
   Phishing adalah teknik penipuan yang digunakan untuk mendapatkan informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi sensitif lainnya dengan menyamar sebagai entitas yang tepercaya, biasanya melalui email atau situs web palsu.
3. *Ransomware*
   Ransomware adalah jenis malware yang mengenkripsi data pada komputer korban dan meminta tebusan untuk mengembalikan akses ke data tersebut. Serangan ransomware sering kali ditujukan kepada individu, perusahaan, atau bahkan lembaga pemerintah.
4. *Identity Theft* (Pencurian Identitas)
   Pencurian identitas melibatkan pengambilan informasi pribadi seseorang, seperti nomor jaminan sosial, informasi kartu kredit, atau data pribadi lainnya, dengan tujuan untuk melakukan penipuan atau aktivitas kriminal lainnya.
5. *Cyberbullying* (Pelecehan Siber)
   Cyberbullying melibatkan pelecehan atau perundungan yang dilakukan melalui media sosial, pesan teks, email, atau platform online lainnya. Pelaku dapat menggunakan

teknologi untuk mengancam, menghina, atau mengekspos korban secara publik.

6. Data Breach (Kebocoran Data)
   Kebocoran data terjadi ketika informasi sensitif, seperti nama pengguna, kata sandi, nomor kartu kredit, atau data pribadi lainnya, diakses atau dibocorkan tanpa izin dari pihak yang berwenang.
7. *Distributed Denial of Service* (DDoS) Attacks
   Serangan DDoS adalah serangan yang melibatkan penggunaan sejumlah besar perangkat yang terinfeksi (disebut botnet) untuk membanjiri server atau situs web dengan lalu lintas yang sangat besar, sehingga mengakibatkan situs web atau aplikasi tidak dapat diakses.
8. *Cyber Espionage* (Spionase Siber)
   Cyber espionage merujuk pada kegiatan peretasan yang dilakukan untuk mengakses informasi sensitif yang digunakan untuk keuntungan politik atau ekonomi. Biasanya, serangan ini dilakukan oleh negara atau kelompok yang berafiliasi dengan negara.
9. *Cryptojacking*
   Cryptojacking adalah bentuk kejahatan di mana peretas memasang perangkat lunak penambang *cryptocurrency* di komputer korban tanpa izin untuk menggunakan daya pemrosesan komputer tersebut dalam menambang *cryptocurrency*.
10. Insider Threat (Ancaman dari Dalam)
    Kasus: Insider threat terjadi ketika seseorang yang memiliki akses sah ke sistem atau data (seperti karyawan atau kontraktor) menyalahgunakan akses tersebut untuk tujuan pribadi atau merusak organisasi.

Kejahatan komputer atau *cybercrime* terus berkembang seiring dengan kemajuan teknologi. Penting bagi individu, perusahaan, dan negara untuk menjaga keamanan digital dengan memperbarui sistem, melatih pengguna tentang ancaman keamanan, dan menerapkan kebijakan keamanan yang ketat untuk mengurangi potensi ancaman tersebut.

DAFTAR PUSTAKA

Achmad Mukhlis Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review, Jurnal ilmiah Sistem Informasi dan Ilmu Komputer Vol. 3 No. 2 Juli 2023 p-ISSN: 2827-8135 e-ISSN : 2827-7953, Hal 143-152 DOI: https://doi.org/10.55606/juisik.v3i2.496

Digky Bima Priatmoko Endang Siti Astuti Riyadi. 2016. Analisis Penerapan Sistem Keamanan Fisik Pada Data Center Untuk Melindungi Data Organisasi (Studi Kasus Pada Unit Penerimaan Mahasiswa Baru Dan Sistem Informasi (PMBSI) IKIP PGRI MADIUN), Jurnal Administrasi Bisnis (JAB)|Vol. 40 No.1 November 2016| administrasibisnis.studentjournal.ub.ac.id

Babys, S.A.M. (n.d.). 2021. Ancaman Perang Siber Di Era Digital Dan Solusi Keamanan Nasional Indonesia. Jurnal Oratio Directa, 3(1), 425-442

Laksono, A. C., & Prayudi, Y. (2021). Modeling Menggunakan Pendekatan STRIDEdan DREADuntuk Mengetahui Risiko dan Mitigasi Keamananpada Sistem Informasi Akademik p-ISSN : 2502-5724; e-ISSN : 2541-5735 9Threat. Jurnal Sistem dan Teknologi Informasi Indonesia, 6(1), 9-21. http://jurnal.unmuhjember.ac.id/ index.php/JUSTINDO/article/view/3944/3023

BAB 4
IT AUDIT TRAIL DAN REAL-TIME AUDIT

4.1 Pendahuluan

Perkembangan teknologi informasi telah mengubah secara fundamental cara organisasi mengelola data, menjalankan proses bisnis, serta mempertanggungjawabkan setiap aktivitas operasionalnya. Sistem informasi yang sebelumnya berfungsi sebagai alat pendukung administratif kini bertransformasi menjadi tulang punggung pengambilan keputusan dan pengendalian organisasi. Konsekuensinya, risiko yang melekat pada sistem tersebut, baik berupa kesalahan, penyalahgunaan, maupun kecurangan menjadi semakin kompleks dan tidak selalu dapat diidentifikasi melalui pendekatan audit konvensional.

Dalam konteks ini, audit yang bersifat periodik dan retrospektif menunjukkan keterbatasannya. Jarak waktu antara terjadinya transaksi dan proses pemeriksaan sering kali menyebabkan temuan audit bersifat reaktif, yakni baru teridentifikasi setelah dampak negatif muncul. Kondisi tersebut menuntut pendekatan audit yang lebih adaptif, berkelanjutan, dan terintegrasi langsung dengan sistem informasi yang diaudit.

IT Audit Trail dan Real-Time Audit muncul sebagai respons atas kebutuhan tersebut. IT Audit Trail menyediakan rekam jejak digital yang sistematis dan kronologis atas setiap aktivitas dalam sistem, sehingga memungkinkan penelusuran tanggung jawab dan validitas transaksi secara objektif.

Sementara itu, Real-Time Audit memperluas fungsi audit dengan menghadirkan mekanisme pengawasan yang berlangsung seiring dengan proses bisnis berjalan, bukan setelahnya. Kombinasi keduanya tidak hanya memperkuat fungsi pengendalian internal, tetapi juga menggeser paradigma audit dari sekadar alat verifikasi menjadi instrumen pencegahan dan peringatan dini.

Bab ini secara khusus membahas IT Audit Trail dan Real-Time Audit dari sisi konseptual, mekanisme implementasi, hingga implikasinya bagi organisasi dan profesi auditor. Pembahasan disusun secara bertahap, dimulai dari pemahaman dasar mengenai audit trail, dilanjutkan dengan konsep real-time audit, serta diakhiri dengan analisis integrasi keduanya dalam mendukung tata kelola sistem informasi yang transparan, akuntabel, dan berorientasi pada pengendalian risiko. Dengan demikian, bab ini diharapkan dapat memberikan landasan analitis yang kuat untuk memahami peran audit berbasis teknologi dalam lingkungan organisasi modern.

4.2 Konsep Dasar IT Audit Trail

4.2.1 Pengertian IT Audit Trail

IT Audit Trail pada dasarnya merupakan mekanisme pencatatan sistematis terhadap seluruh aktivitas yang terjadi dalam sistem informasi berbasis teknologi. Pencatatan ini dilakukan secara otomatis oleh sistem dan disusun secara kronologis, sehingga setiap transaksi, perubahan data, maupun interaksi pengguna dapat ditelusuri kembali secara utuh dan objektif. Dalam konteks audit, audit trail tidak dipahami semata-mata sebagai log teknis, melainkan sebagai representasi formal dari jejak akuntabilitas digital.

Secara konseptual, IT Audit Trail berfungsi sebagai penghubung antara proses bisnis dan bukti audit elektronik.

Setiap aktivitas yang tercatat di dalamnya merefleksikan hubungan sebab–akibat antara tindakan pengguna, respon sistem, dan output yang dihasilkan. Dengan demikian, audit trail memungkinkan auditor untuk menelusuri alur transaksi dari titik awal hingga akhir, serta mengidentifikasi apakah proses tersebut telah berjalan sesuai dengan kebijakan, prosedur, dan pengendalian yang ditetapkan.

Lebih jauh, IT Audit Trail juga memiliki dimensi preventif dan korektif. Dari sisi preventif, keberadaan audit trail menciptakan efek pengawasan berkelanjutan (*deterrent effect*) yang dapat menekan potensi penyalahgunaan sistem. Sementara itu, dari sisi korektif, audit trail menyediakan bukti yang diperlukan untuk melakukan analisis atas kesalahan, anomali, maupun indikasi kecurangan yang terdeteksi. Dalam konteks ini, audit trail berperan sebagai dasar faktual bagi proses evaluasi dan pengambilan keputusan manajerial.

Dengan demikian, IT Audit Trail dapat disimpulkan sebagai elemen fundamental dalam audit sistem informasi, karena memastikan bahwa setiap aktivitas digital tidak hanya terekam, tetapi juga dapat dipertanggungjawabkan. Keandalan audit trail menjadi prasyarat utama bagi efektivitas audit berbasis teknologi, khususnya ketika organisasi mulai mengadopsi pendekatan audit yang bersifat berkelanjutan dan real-time. Oleh karena itu, pemahaman yang tepat mengenai pengertian IT Audit Trail menjadi landasan penting sebelum membahas fungsi, komponen, dan implementasinya secara lebih mendalam pada subbab berikutnya.

4.2.2 Tujuan dan Fungsi IT Audit Trail

Penerapan IT Audit Trail dalam sistem informasi tidak dapat dilepaskan dari tujuan utama audit itu sendiri, yaitu memastikan bahwa aktivitas organisasi berlangsung secara

andal, terkendali, dan dapat dipertanggungjawabkan. Dalam lingkungan digital yang ditandai oleh kecepatan transaksi dan kompleksitas proses, audit trail berfungsi sebagai instrumen yang menjembatani kebutuhan pengawasan dengan karakteristik sistem berbasis teknologi.

Secara umum, tujuan IT Audit Trail adalah menyediakan bukti audit elektronik yang memadai dan relevan atas seluruh aktivitas yang terjadi dalam sistem informasi. Bukti ini menjadi dasar bagi auditor dan manajemen untuk menilai apakah transaksi dan proses telah berjalan sesuai dengan kebijakan, prosedur, serta pengendalian yang ditetapkan. Tanpa audit trail yang memadai, proses audit berisiko kehilangan keterlacakan (*traceability*) dan objektivitas penilaian.

Dari sisi fungsional, IT Audit Trail menjalankan beberapa peran utama yang saling berkaitan. Pertama, sebagai fungsi pengendalian (*control function*), audit trail memungkinkan organisasi untuk memantau aktivitas sistem secara berkelanjutan dan mendeteksi penyimpangan sejak dini. Setiap aktivitas yang terekam menciptakan mekanisme pengawasan implisit yang dapat menekan potensi kesalahan maupun penyalahgunaan sistem.

Kedua, IT Audit Trail berfungsi sebagai sarana akuntabilitas. Dengan adanya pencatatan yang jelas mengenai siapa melakukan apa dan kapan suatu aktivitas terjadi, tanggung jawab atas setiap tindakan dalam sistem menjadi lebih transparan. Hal ini tidak hanya memperkuat disiplin pengguna sistem, tetapi juga memudahkan proses evaluasi kinerja dan penelusuran tanggung jawab apabila terjadi permasalahan.

Ketiga, audit trail memiliki fungsi kepatuhan (*compliance function*) terhadap standar, kebijakan internal, dan regulasi eksternal yang mengatur pengelolaan sistem informasi.

Keberadaan audit trail mendukung organisasi dalam menunjukkan bahwa proses bisnis dan pengolahan data telah dilaksanakan sesuai dengan ketentuan yang berlaku, sehingga mengurangi risiko ketidakpatuhan dan sanksi yang mungkin timbul.

Keempat, IT Audit Trail berperan sebagai alat investigatif dan forensik. Dalam situasi terjadinya insiden keamanan, kesalahan sistem, atau dugaan kecurangan, audit trail menyediakan rekam jejak kronologis yang dapat dianalisis untuk mengidentifikasi sumber masalah dan pola kejadian. Fungsi ini menjadikan audit trail sebagai elemen penting dalam manajemen risiko dan penanganan insiden berbasis teknologi. Dengan demikian, tujuan dan fungsi IT Audit Trail tidak hanya terbatas pada kebutuhan audit formal, tetapi juga berkontribusi secara strategis terhadap penguatan tata kelola sistem informasi. Audit trail menjadi fondasi bagi pendekatan audit yang lebih maju, termasuk real-time audit dan continuous auditing, yang akan dibahas pada bagian selanjutnya. Oleh karena itu, pemahaman yang komprehensif terhadap tujuan dan fungsi IT Audit Trail merupakan prasyarat penting bagi efektivitas pengawasan dan pengendalian dalam lingkungan organisasi modern.

4.2.3 Komponen Utama IT Audit Trail

Keandalan IT Audit Trail tidak hanya ditentukan oleh keberadaannya, tetapi terutama oleh kelengkapan dan kualitas komponen yang membentuknya. Audit trail yang tidak dirancang dengan komponen yang memadai berpotensi kehilangan nilai audit, karena tidak mampu memberikan informasi yang cukup untuk penelusuran, evaluasi, dan pengambilan keputusan. Oleh karena itu, identifikasi

komponen utama IT Audit Trail menjadi aspek krusial dalam memastikan efektivitasnya sebagai instrumen pengendalian.

Komponen pertama yang bersifat fundamental adalah identitas pengguna (*user identification*). Komponen ini berfungsi untuk memastikan bahwa setiap aktivitas dalam sistem dapat dikaitkan secara jelas dengan individu atau entitas tertentu. Identitas pengguna menjadi dasar akuntabilitas, karena tanpa informasi ini, audit trail tidak mampu menjawab pertanyaan siapa yang bertanggung jawab atas suatu tindakan. Dalam praktiknya, identitas pengguna harus dikelola secara unik dan konsisten untuk menghindari ambiguitas dalam penelusuran audit.

Komponen kedua adalah waktu aktivitas (*timestamp*) yang mencatat secara presisi kapan suatu transaksi atau perubahan data terjadi. Informasi waktu tidak hanya penting untuk menyusun urutan kejadian secara kronologis, tetapi juga berperan dalam analisis pola aktivitas, deteksi anomali, serta evaluasi kepatuhan terhadap batasan waktu tertentu. Ketepatan dan konsistensi timestamp menjadi syarat penting agar audit trail dapat digunakan sebagai bukti yang andal.

Komponen ketiga mencakup deskripsi aktivitas atau jenis transaksi yang dilakukan dalam sistem. Komponen ini menjelaskan apa yang dilakukan oleh pengguna atau sistem, seperti penambahan data, perubahan, penghapusan, atau akses terhadap informasi tertentu. Tanpa deskripsi aktivitas yang jelas, audit trail hanya akan menjadi catatan waktu dan identitas tanpa konteks, sehingga menyulitkan auditor dalam memahami substansi kejadian.

Komponen keempat adalah informasi perubahan data (*before and after state*). Komponen ini memberikan gambaran kondisi data sebelum dan sesudah suatu aktivitas dilakukan. Keberadaan informasi ini sangat penting dalam konteks audit

dan forensik, karena memungkinkan auditor menilai dampak suatu tindakan terhadap integritas data. Perubahan data yang tidak wajar atau tidak sesuai prosedur dapat diidentifikasi melalui perbandingan ini.

Selanjutnya, sumber atau lokasi akses juga merupakan komponen penting dalam IT Audit Trail. Informasi ini mencakup asal akses, seperti alamat jaringan atau perangkat yang digunakan. Komponen ini memperkaya analisis audit dengan dimensi kontekstual, khususnya dalam mendeteksi akses tidak sah atau aktivitas yang berasal dari lokasi yang tidak semestinya.

Komponen terakhir yang tidak kalah penting adalah status hasil aktivitas, yaitu informasi mengenai apakah suatu transaksi berhasil, gagal, atau dibatalkan. Status ini membantu auditor memahami tidak hanya niat atau upaya yang dilakukan, tetapi juga hasil akhir dari aktivitas tersebut. Dalam banyak kasus, percobaan yang gagal justru memberikan indikasi awal terhadap potensi masalah keamanan atau kesalahan sistem.

Secara keseluruhan, komponen-komponen utama IT Audit Trail tersebut membentuk satu kesatuan yang saling melengkapi. Ketidakhadiran atau kelemahan pada salah satu komponen dapat mengurangi nilai audit trail secara signifikan. Oleh karena itu, perancangan audit trail harus dilakukan secara holistik, dengan mempertimbangkan kebutuhan audit, pengendalian internal, serta kesiapan sistem untuk mendukung analisis berkelanjutan, termasuk penerapan *real-time* audit yang akan dibahas pada bagian selanjutnya.

4.3 Implementasi IT Audit Trail dalam Sistem Informasi

4.3.1 Mekanisme Pencatatan Audit Trail

Mekanisme pencatatan IT Audit Trail merupakan inti dari keberfungsian audit berbasis teknologi, karena pada tahap inilah seluruh aktivitas sistem diterjemahkan menjadi bukti audit elektronik. Pencatatan audit trail tidak dapat dipahami sebagai proses tambahan yang bersifat opsional, melainkan sebagai bagian integral dari desain dan operasional sistem informasi itu sendiri. Oleh sebab itu, mekanisme pencatatan harus dirancang secara sistematis, konsisten, dan selaras dengan tujuan pengendalian internal.

Secara prinsip, pencatatan audit trail dilakukan secara otomatis oleh sistem, tanpa bergantung pada intervensi pengguna. Otomatisasi ini penting untuk menjamin objektivitas dan menghindari risiko manipulasi atau kelalaian dalam pencatatan. Setiap aktivitas yang memenuhi kriteria tertentu—seperti akses sistem, pemrosesan transaksi, perubahan data, maupun kegagalan sistem—harus langsung tercatat pada saat kejadian berlangsung. Dengan demikian, audit trail mampu merepresentasikan kondisi sistem secara aktual.

Mekanisme pencatatan audit trail umumnya diterapkan pada beberapa lapisan sistem informasi. Pada tingkat aplikasi, audit trail mencatat interaksi pengguna dengan fitur dan fungsi aplikasi, termasuk transaksi yang dilakukan dan perubahan data yang dihasilkan. Pada tingkat basis data, pencatatan difokuskan pada aktivitas yang memengaruhi struktur dan isi data, seperti operasi insert, update, dan delete. Sementara itu, pada tingkat sistem dan infrastruktur, audit trail mencakup aktivitas sistem operasi dan jaringan, termasuk proses login, konfigurasi, dan akses sumber daya. Integrasi pencatatan lintas

lapisan ini memperkaya konteks audit dan meningkatkan keterlacakan.

Agar mekanisme pencatatan audit trail berjalan efektif, diperlukan pengaturan yang jelas mengenai kriteria aktivitas yang dicatat. Tidak semua aktivitas harus dicatat secara detail yang sama, karena hal tersebut dapat menimbulkan beban penyimpanan dan kompleksitas pengelolaan. Oleh karena itu, organisasi perlu menetapkan kebijakan yang menyeimbangkan antara kebutuhan audit dan efisiensi sistem, dengan memprioritaskan aktivitas yang berdampak signifikan terhadap risiko, integritas data, dan kepatuhan.

Selain itu, mekanisme pencatatan audit trail harus didukung oleh pengamanan terhadap data audit trail itu sendiri. Data yang telah tercatat harus dilindungi dari perubahan, penghapusan, atau akses tidak sah. Pengendalian akses, pemisahan tugas, serta penggunaan mekanisme penguncian atau pencatatan perubahan lanjutan terhadap audit trail menjadi penting untuk menjaga integritas bukti audit. Tanpa perlindungan ini, audit trail berisiko kehilangan kredibilitas sebagai sumber informasi yang andal.

Dengan mekanisme pencatatan yang dirancang secara otomatis, terintegrasi, dan aman, IT Audit Trail dapat berfungsi tidak hanya sebagai catatan historis, tetapi juga sebagai fondasi bagi pengawasan berkelanjutan. Mekanisme inilah yang memungkinkan audit trail dimanfaatkan dalam pendekatan audit yang lebih maju, termasuk real-time audit, di mana data aktivitas sistem dianalisis secara langsung untuk mendeteksi penyimpangan dan risiko secara dini. Oleh karena itu, pemahaman terhadap mekanisme pencatatan audit trail menjadi langkah penting sebelum membahas tantangan dan implikasi implementasinya pada subbab berikutnya.

4.3.2 Tantangan Implementasi IT Audit Trail

Meskipun IT Audit Trail secara konseptual menawarkan manfaat signifikan bagi pengendalian dan akuntabilitas sistem informasi, implementasinya dalam praktik menghadapi berbagai tantangan yang bersifat teknis, organisasional, maupun etis. Tantangan-tantangan ini menjadi semakin kompleks ketika audit trail diterapkan pada sistem berskala besar dan terintegrasi, seperti sistem keuangan, ERP, dan e-government.

Tantangan utama yang sering muncul adalah volume dan kompleksitas data audit trail. Sistem yang memproses transaksi dalam jumlah besar akan menghasilkan data audit trail yang masif dan berkelanjutan. Tanpa perencanaan kapasitas penyimpanan dan mekanisme pengelolaan yang memadai, audit trail berpotensi menjadi beban sistem, baik dari sisi performa maupun biaya. Selain itu, kompleksitas data yang tinggi dapat menyulitkan auditor dalam mengidentifikasi informasi yang relevan, sehingga mengurangi efektivitas audit trail sebagai alat pengendalian.

Tantangan berikutnya berkaitan dengan kualitas dan konsistensi pencatatan. Audit trail yang dihasilkan dari berbagai modul atau subsistem sering kali memiliki format, tingkat detail, dan standar pencatatan yang berbeda. Kondisi ini umum terjadi dalam lingkungan ERP dan e-government yang melibatkan banyak unit kerja dan aplikasi pendukung. Ketidakkonsistenan tersebut dapat menghambat proses penelusuran dan analisis audit, serta berpotensi menimbulkan celah pengendalian internal.

Dari sisi keamanan, perlindungan terhadap data audit trail itu sendiri menjadi tantangan yang tidak dapat diabaikan. Audit trail menyimpan informasi sensitif mengenai aktivitas sistem dan pengguna, sehingga menjadi target potensial bagi pihak

yang berniat menyembunyikan penyimpangan atau kecurangan. Jika akses terhadap audit trail tidak dikendalikan secara ketat, data tersebut dapat dimodifikasi atau dihapus, yang pada akhirnya merusak kredibilitas bukti audit. Oleh karena itu, tantangan keamanan audit trail tidak hanya berkaitan dengan pencatatan aktivitas, tetapi juga dengan integritas dan kerahasiaan data audit.

Selain aspek teknis, tantangan implementasi IT Audit Trail juga muncul pada kesiapan sumber daya manusia. Auditor dan pengelola sistem dituntut memiliki pemahaman yang memadai terhadap mekanisme pencatatan, struktur log, serta teknik analisis audit trail. Tanpa kompetensi tersebut, audit trail berisiko hanya menjadi data pasif yang tidak dimanfaatkan secara optimal dalam proses pengawasan dan pengendalian.

Tantangan lainnya berkaitan dengan isu privasi dan etika, terutama dalam sistem e-government dan sistem yang melibatkan data pribadi. Pencatatan aktivitas pengguna secara rinci harus dilakukan dengan memperhatikan batasan hukum dan etika, agar tidak melanggar hak privasi individu. Ketidakseimbangan antara kebutuhan pengawasan dan perlindungan privasi dapat menimbulkan resistensi pengguna serta risiko hukum bagi organisasi.

Secara keseluruhan, tantangan implementasi IT Audit Trail menunjukkan bahwa keberhasilan penerapannya tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh kebijakan, pengendalian internal, dan kesiapan organisasi secara menyeluruh. Tanpa penanganan yang tepat terhadap tantangan-tantangan tersebut, audit trail berpotensi kehilangan nilai strategisnya. Oleh karena itu, organisasi perlu mengadopsi pendekatan yang terintegrasi dan berkelanjutan agar IT Audit Trail dapat berfungsi secara efektif sebagai

fondasi pengawasan, sekaligus mendukung penerapan real-time audit yang akan dibahas pada bagian selanjutnya.

4.4 Konsep *Real-Time* Audit

4.4.1 Pengertian *Real-Time* Audit

Real-Time Audit merupakan pendekatan audit yang dilakukan secara berkelanjutan dan bersamaan dengan berlangsungnya aktivitas atau transaksi dalam sistem informasi. Berbeda dengan audit tradisional yang dilakukan secara periodik setelah suatu periode berakhir, real-time audit memungkinkan proses pengawasan dilakukan sejak awal hingga akhir kegiatan, sehingga potensi kesalahan atau penyimpangan dapat diketahui lebih cepat.

Dalam praktiknya, real-time audit memanfaatkan teknologi informasi untuk memantau aktivitas sistem secara otomatis berdasarkan data yang dihasilkan oleh IT Audit Trail. Setiap transaksi, akses pengguna, maupun perubahan data yang terjadi dalam sistem akan dianalisis secara langsung sesuai dengan aturan atau kriteria yang telah ditetapkan. Dengan demikian, audit tidak hanya berfungsi sebagai alat pemeriksaan, tetapi juga sebagai bagian dari mekanisme pengendalian yang berjalan secara terus-menerus.

Jika dikaitkan dengan kerangka pengendalian internal SPIP/COSO, *real-time* audit berperan penting pada komponen monitoring *activities.* Monitoring dalam SPIP/COSO bertujuan untuk memastikan bahwa pengendalian internal telah dirancang dan dilaksanakan secara efektif. Real-time audit mendukung tujuan tersebut dengan menyediakan informasi yang aktual dan relevan mengenai pelaksanaan proses dan kepatuhan terhadap prosedur. Melalui pemantauan yang berkelanjutan, kelemahan pengendalian dapat segera diidentifikasi dan ditindaklanjuti.

Dalam konteks ERP swasta, real-time audit membantu manajemen memantau transaksi lintas modul secara langsung, sehingga kesalahan pencatatan atau pelanggaran prosedur dapat segera diketahui. Sementara itu, dalam sistem e-*government, real-time* audit mendukung transparansi dan akuntabilitas dengan memastikan bahwa setiap layanan dan proses administrasi tercatat dan diawasi secara berkesinambungan. Meskipun konteks penerapannya berbeda, prinsip dasar real-time audit tetap sama, yaitu pengawasan yang berkelanjutan berbasis sistem.

Dengan demikian, real-time audit dapat disimpulkan sebagai pendekatan audit berbasis teknologi yang memperkuat fungsi monitoring dalam pengendalian internal. Pendekatan ini memungkinkan organisasi melakukan pengawasan secara lebih efektif, cepat, dan preventif. Pemahaman mengenai real-time audit menjadi penting sebagai dasar untuk membahas perbedaannya dengan audit tradisional serta perannya dalam mendukung efektivitas pengendalian internal pada subbab berikutnya.

4.4.2 Perbedaan Audit Tradisional dan Real-Time Audit

Audit tradisional dan real-time audit memiliki tujuan yang sama, yaitu memastikan kepatuhan dan efektivitas pengendalian internal. Perbedaannya terletak pada waktu pelaksanaan, pendekatan pengawasan, dan peran audit dalam sistem pengendalian.

Audit tradisional dilaksanakan secara periodik dan bersifat retrospektif, karena pemeriksaan dilakukan setelah kegiatan atau periode tertentu berakhir. Dalam konteks sistem e-government, pendekatan ini sering menyebabkan temuan audit baru diketahui setelah layanan publik dijalankan, sehingga tindak lanjut bersifat reaktif.

Sebaliknya, real-time audit dilakukan secara berkelanjutan dan terintegrasi dengan sistem informasi e-government. Melalui pemanfaatan IT Audit Trail, aktivitas layanan dan transaksi administrasi dapat dipantau saat proses berlangsung. Pendekatan ini memungkinkan deteksi dini terhadap kesalahan prosedur atau penyimpangan, sehingga tindakan korektif dapat segera dilakukan.

Dari sisi pengendalian internal, audit tradisional lebih berperan dalam mengevaluasi hasil pengendalian, sedangkan real-time audit memperkuat fungsi monitoring sebagaimana ditekankan dalam kerangka SPIP/COSO. Dengan monitoring yang berkelanjutan, efektivitas pengendalian dapat dijaga secara lebih konsisten.

Perbedaan utama kedua pendekatan tersebut dapat diringkas sebagai berikut.

Aspek	**Audit Tradisional**	**Real-Time Audit**
Waktu	Periodik	Berkelanjutan
Sifat	Retrospektif	Proaktif
Fokus	Pemeriksaan pasca-kegiatan	Pemantauan saat kegiatan
Peran Pengendalian	Evaluasi	Monitoring

Dengan demikian, dalam sistem *e-government, real-time* audit tidak menggantikan audit tradisional, melainkan melengkapinya. Audit tradisional tetap diperlukan untuk penilaian menyeluruh, sementara real-time audit berfungsi memperkuat pengawasan harian dan meningkatkan transparansi serta akuntabilitas layanan publik.

4.5 Integrasi IT Audit Trail dengan Real-Time Audit

4.5.1 Peran Audit Trail dalam Real-Time Audit

Audit trail memiliki peran yang sangat penting dalam penerapan real-time audit karena berfungsi sebagai sumber data utama bagi proses pemantauan yang dilakukan secara berkelanjutan. Tanpa audit trail yang andal, real-time audit tidak dapat berjalan secara efektif, karena tidak memiliki dasar informasi yang memadai untuk menilai aktivitas sistem secara langsung.

Dalam konteks sistem e-government, audit trail mencatat seluruh aktivitas yang terjadi dalam layanan publik digital, seperti akses pengguna, pemrosesan data administrasi, dan penerbitan dokumen elektronik. Data yang tercatat tersebut kemudian dimanfaatkan oleh mekanisme real-time audit untuk memantau kepatuhan terhadap prosedur, mendeteksi penyimpangan, serta mengidentifikasi aktivitas yang tidak sesuai dengan ketentuan yang berlaku.

Peran audit trail dalam real-time audit tidak hanya bersifat pencatatan, tetapi juga mendukung fungsi pengendalian internal, khususnya pada aspek monitoring. Informasi yang dihasilkan dari audit trail memungkinkan pengawasan dilakukan secara terus-menerus, sehingga kelemahan pengendalian dapat segera diketahui dan ditindaklanjuti. Dengan demikian, audit trail membantu menggeser peran audit dari pemeriksaan pasca-kejadian menjadi pengawasan yang bersifat preventif.

Selain itu, audit trail memperkuat akuntabilitas dan transparansi dalam penyelenggaraan e-government. Setiap aktivitas yang terekam dapat ditelusuri kembali, sehingga tanggung jawab atas pelaksanaan layanan publik menjadi lebih

jelas. Hal ini penting untuk menjaga kepercayaan masyarakat terhadap sistem dan proses pemerintahan berbasis digital.

Dengan demikian, audit trail dapat disimpulkan sebagai fondasi utama real-time audit. Keberadaan audit trail yang lengkap, akurat, dan terlindungi memungkinkan real-time audit berfungsi secara optimal dalam mendukung pengendalian internal, meningkatkan transparansi, serta memastikan akuntabilitas dalam sistem e-government.

4.5.2 Model Integrasi Konseptual

Model integrasi konseptual antara IT Audit Trail dan real-time audit menggambarkan bagaimana pencatatan aktivitas sistem dan proses audit berkelanjutan saling terhubung dalam mendukung pengendalian internal. Dalam konteks e-government, integrasi ini bertujuan memastikan bahwa setiap layanan dan proses administrasi digital tidak hanya tercatat, tetapi juga diawasi secara langsung selama berlangsung.

Secara konseptual, integrasi dimulai dari aktivitas sistem *e-government*, seperti akses pengguna, pemrosesan data, dan penyelesaian layanan publik. Setiap aktivitas tersebut secara otomatis direkam dalam IT Audit Trail sebagai jejak digital yang bersifat kronologis. Audit trail kemudian berfungsi sebagai basis data utama yang menyediakan informasi aktual mengenai pelaksanaan proses dan kepatuhan terhadap prosedur.

Data audit trail yang terkumpul selanjutnya dianalisis oleh mekanisme real-time audit melalui pemantauan berkelanjutan. Pada tahap ini, sistem melakukan identifikasi terhadap aktivitas yang menyimpang dari aturan atau parameter yang telah ditetapkan. Jika ditemukan indikasi ketidaksesuaian, sistem dapat memberikan peringatan dini kepada pengelola atau auditor untuk segera dilakukan tindak lanjut.

Dalam perspektif pengendalian internal SPIP/COSO, model integrasi ini memperkuat komponen monitoring, karena pengawasan tidak lagi dilakukan secara periodik, melainkan berlangsung secara terus-menerus. Informasi yang dihasilkan memungkinkan manajemen melakukan tindakan korektif secara cepat, sehingga risiko kesalahan atau penyimpangan dalam layanan e-government dapat diminimalkan.

Dengan demikian, model integrasi konseptual IT Audit Trail dan real-time audit menempatkan audit sebagai bagian dari sistem pengendalian yang berjalan. Integrasi ini tidak hanya meningkatkan efektivitas pengawasan, tetapi juga mendukung transparansi dan akuntabilitas penyelenggaraan e-government. Model konseptual ini menjadi dasar penting untuk memahami manfaat strategis penerapan audit berbasis teknologi yang akan dibahas pada bagian selanjutnya.

4.6 Manfaat Strategis bagi Organisasi

Penerapan IT Audit Trail dan real-time audit dalam lingkungan ERP swasta memberikan berbagai manfaat strategis bagi organisasi, khususnya dalam mendukung efektivitas pengendalian internal dan keandalan proses bisnis. Manfaat tersebut tidak hanya bersifat teknis, tetapi juga berdampak pada aspek manajerial dan pengambilan keputusan.

Manfaat utama yang dirasakan organisasi adalah peningkatan transparansi proses bisnis. Dengan adanya audit trail yang terintegrasi dalam sistem ERP, setiap aktivitas pengguna dan transaksi bisnis dapat ditelusuri secara jelas dan kronologis. Transparansi ini memudahkan manajemen dalam memahami alur proses, sekaligus mengurangi ruang terjadinya penyimpangan yang tidak terdeteksi.

Selain itu, integrasi audit trail dengan real-time audit memberikan manfaat berupa deteksi dini terhadap risiko dan

penyimpangan. Melalui pemantauan yang berkelanjutan, organisasi dapat mengidentifikasi transaksi tidak wajar, pelanggaran prosedur, atau kelemahan pengendalian sejak awal. Kondisi ini memungkinkan tindakan korektif dilakukan lebih cepat, sehingga potensi kerugian dapat diminimalkan.

Manfaat strategis lainnya adalah penguatan pengendalian internal, khususnya pada komponen monitoring. Real-time audit yang memanfaatkan data audit trail membantu manajemen memastikan bahwa pengendalian yang telah dirancang dalam ERP benar-benar dijalankan. Dengan demikian, pengendalian internal tidak hanya dinilai secara periodik, tetapi diawasi secara terus-menerus selama proses bisnis berlangsung.

Penerapan audit trail dan real-time audit juga mendukung efisiensi proses audit dan pengambilan keputusan manajerial. Data yang tersedia secara aktual dan terstruktur memudahkan auditor internal dalam melakukan evaluasi, sekaligus membantu manajemen dalam mengambil keputusan berbasis informasi yang andal. Hal ini menjadikan ERP tidak hanya sebagai sistem operasional, tetapi juga sebagai alat pendukung pengendalian dan strategi organisasi.

Dengan demikian, IT Audit Trail dan real-time audit memberikan manfaat strategis yang signifikan bagi organisasi pengguna ERP swasta. Keduanya berkontribusi pada peningkatan transparansi, pengendalian risiko, dan efektivitas pengendalian internal, sehingga mendukung tercapainya tujuan organisasi secara lebih akuntabel dan berkelanjutan.

4.7 Implikasi terhadap Profesi Auditor

Penerapan IT Audit Trail dan real-time audit dalam ERP swasta membawa implikasi langsung terhadap peran dan cara kerja auditor, baik auditor internal maupun auditor eksternal.

Perkembangan ini menuntut perubahan pendekatan audit yang lebih adaptif terhadap sistem berbasis teknologi.

Bagi auditor internal, audit trail dan real-time audit memperkuat fungsi pengawasan berkelanjutan. Auditor internal tidak lagi hanya berfokus pada pemeriksaan periodik, tetapi juga berperan dalam memantau efektivitas pengendalian internal selama proses bisnis berlangsung. Dengan akses terhadap data audit trail secara real-time, auditor internal dapat mendeteksi penyimpangan lebih dini dan memberikan rekomendasi perbaikan secara cepat.

Sementara itu, bagi auditor eksternal, audit trail dan real-time audit meningkatkan efisiensi dan kualitas proses audit. Data yang tercatat secara sistematis dalam ERP membantu auditor eksternal memahami alur transaksi dan pengendalian yang diterapkan oleh perusahaan. Meskipun auditor eksternal tetap melakukan audit secara periodik, ketersediaan audit trail yang andal mendukung penilaian risiko dan pengujian pengendalian secara lebih efektif.

Implikasi lainnya adalah meningkatnya kebutuhan kompetensi teknologi informasi bagi kedua jenis auditor. Auditor dituntut memahami sistem ERP, struktur audit trail, serta keterkaitannya dengan pengendalian internal. Selain itu, profesionalisme dan etika auditor tetap menjadi aspek penting, mengingat akses terhadap data sistem yang bersifat sensitif.

Dengan demikian, penerapan IT Audit Trail dan real-time audit memperjelas perbedaan peran audit internal dan audit eksternal, sekaligus memperkuat kontribusi keduanya dalam menjaga efektivitas pengendalian internal dan keandalan proses bisnis dalam lingkungan ERP swasta.

4.8 Refleksi Kritis dan Keterbatasan

Penerapan IT Audit Trail dan real-time audit dalam lingkungan ERP swasta memberikan kontribusi yang signifikan terhadap penguatan pengendalian internal dan pengawasan proses bisnis. Namun demikian, penerapan kedua konsep tersebut perlu dilihat secara kritis, karena tidak terlepas dari berbagai keterbatasan yang dapat memengaruhi efektivitasnya.

Salah satu keterbatasan utama adalah ketergantungan yang tinggi pada teknologi dan sistem ERP itu sendiri. Audit trail dan real-time audit hanya akan berjalan efektif apabila sistem dirancang dengan baik, data tercatat secara lengkap, serta pengendalian akses diterapkan secara konsisten. Jika desain sistem lemah atau pengelolaan ERP tidak optimal, audit trail berpotensi tidak mencerminkan kondisi sebenarnya dari proses bisnis.

Keterbatasan berikutnya berkaitan dengan kualitas sumber daya manusia. Meskipun data audit trail tersedia secara lengkap, pemanfaatannya sangat bergantung pada kemampuan auditor dan pengelola sistem dalam memahami dan menganalisis informasi tersebut. Kurangnya kompetensi di bidang sistem informasi dapat menyebabkan audit trail dan real-time audit tidak dimanfaatkan secara maksimal dalam proses pengawasan.

Selain itu, penerapan real-time audit juga berpotensi menimbulkan tantangan operasional, seperti munculnya peringatan berlebihan akibat pengaturan parameter yang kurang tepat. Kondisi ini dapat mengurangi efektivitas monitoring jika tidak diimbangi dengan kebijakan dan prosedur yang jelas dalam menindaklanjuti hasil pemantauan.

Dari sudut pandang manajerial, terdapat pula keterbatasan terkait biaya dan kesiapan organisasi.

Implementasi audit trail yang komprehensif dan real-time audit membutuhkan investasi pada infrastruktur, pengaturan sistem, serta pelatihan personel. Tidak semua organisasi ERP swasta memiliki tingkat kesiapan yang sama untuk mengadopsi pendekatan audit berbasis teknologi secara optimal.

Dengan demikian, meskipun IT Audit Trail dan real-time audit menawarkan manfaat yang besar, penerapannya perlu disesuaikan dengan kondisi dan kemampuan organisasi. Refleksi kritis terhadap keterbatasan ini penting agar penerapan audit berbasis teknologi tidak hanya bersifat formal, tetapi benar-benar mendukung efektivitas pengendalian internal dan pencapaian tujuan organisasi secara berkelanjutan.

4.9 Ringkasan

Bab ini telah membahas secara komprehensif mengenai peran IT Audit Trail dan Real-Time Audit dalam mendukung pengendalian internal pada lingkungan ERP swasta. Pembahasan diawali dengan penjelasan konsep dasar IT Audit Trail, tujuan, fungsi, serta komponen utamanya, yang menunjukkan bahwa audit trail merupakan elemen penting dalam memastikan keterlacakan, akuntabilitas, dan keandalan proses bisnis berbasis sistem informasi.

Selanjutnya, bab ini menguraikan mekanisme pencatatan audit trail, tantangan implementasinya, serta keterkaitannya dengan pengendalian internal. Pembahasan tersebut menegaskan bahwa keberhasilan audit trail tidak hanya bergantung pada teknologi, tetapi juga pada desain sistem, keamanan data, dan kesiapan sumber daya manusia. Tantangan-tantangan tersebut perlu dikelola secara tepat agar audit trail dapat memberikan nilai tambah bagi organisasi.

Bab ini juga membahas konsep real-time audit, perbedaannya dengan audit tradisional, serta model integrasi

konseptual antara audit trail dan real-time audit dalam ERP swasta. Integrasi tersebut memperlihatkan bagaimana audit dapat berfungsi sebagai bagian dari mekanisme monitoring yang berjalan secara berkelanjutan, sehingga mendukung deteksi dini risiko dan peningkatan efektivitas pengendalian internal.

Selain itu, dibahas pula manfaat strategis penerapan audit trail dan real-time audit bagi organisasi, implikasinya terhadap profesi auditor internal dan eksternal, serta refleksi kritis mengenai keterbatasan penerapannya. Keseluruhan pembahasan menunjukkan bahwa audit berbasis teknologi memiliki potensi besar, namun perlu diterapkan secara realistis dan terintegrasi dengan kebijakan serta kemampuan organisasi.

DAFTAR PUSTAKA

Arens, A. A., Elder, R. J., & Beasley, M. S. (2017). *Auditing and assurance services: An integrated approach* (15th ed.). Pearson Education.

Bodnar, G. H., & Hopwood, W. S. (2014). *Accounting information systems* (11th ed.). Pearson Education.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal control – Integrated framework*. COSO.

Hall, J. A. (2016). *Information technology auditing and assurance* (4th ed.). Cengage Learning.

Hall, J. A. (2019). *Accounting information systems* (10th ed.). Cengage Learning.

Hunton, J. E., Bryant, S. M., & Bagranoff, N. A. (2011). *Core concepts of information technology auditing*. Wiley.

Ismail, N. A., & King, M. (2007). Factors influencing the alignment of accounting information systems in small and medium sized Malaysian manufacturing firms. *Journal of Information Systems and Small Business*, 1(1–2), 1–20.

James, K., & Sidhu, B. K. (2012). The impact of continuous auditing on audit quality. *Managerial Auditing Journal*, 27(7), 599–614.

Knechel, W. R., Salterio, S. E., & Ballou, B. (2007). Auditing and assurance services. *McGraw-Hill Education*.

Mansouri, A., Pirayesh, R., & Salehi, M. (2009). Audit automation and audit quality: Case of Iran. *International Journal of Accounting and Information Management*, 17(2), 152–168.

Romney, M. B., & Steinbart, P. J. (2018). *Accounting information systems* (14th ed.). Pearson Education.

Sayana, S. A. (2003). Continuous auditing: The audit of the future. *ISACA Journal*, 5, 21–25.

Spathis, C., & Ananiadis, J. (2005). Assessing the benefits of using an enterprise system in accounting information and management. *Journal of Enterprise Information Management*, 18(2), 195–210.

Susanto, A. (2013). *Sistem informasi akuntansi*. Lingga Jaya.

Weber, R. (2010). *Information systems control and audit*. Pearson Education.

Wilkinson, J. W., Cerullo, M. J., Raval, V., & Wong-On-Wing, B. (2000). *Accounting information systems: Essential concepts and applications*. Wiley.

BAB 5
IT FORENSICS

5.1 Pendahuluan

Perkembangan teknologi informasi yang semakin pesat membawa dampak signifikan terhadap meningkatnya kejahatan berbasis digital (*cybercrime*), termasuk peretasan (*hacking*), pencurian data pribadi, penipuan daring, penyebaran *malware*, hingga sabotase sistem digital. Fenomena ini menunjukkan bagaimana teknologi dapat dimanfaatkan tidak hanya untuk meningkatkan efisiensi dan inovasi, tetapi juga sebagai sarana pelanggaran hukum dan ancaman terhadap kepentingan individu, organisasi, bahkan negara. Dalam konteks tersebut, disiplin *IT Forensics* atau *Digital Forensics* menjadi sangat penting sebagai pendekatan ilmiah dan yuridis untuk menginvestigasi dan mengungkap kejadian kejahatan digital secara sah di depan hukum.

IT Forensics merupakan bagian dari ilmu forensik yang khusus menangani bukti digital yang ditemukan dalam perangkat teknologi informasi seperti komputer, ponsel, jaringan, server, maupun media penyimpanan lainnya. Menurut Raharjo (2013), *digital forensics* mencakup "penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital, yang sering kali berkaitan dengan kejahatan komputer" (Raharjo, 2013). Dengan kata lain, disiplin ini tidak hanya berfokus pada aspek teknis pemulihan data, tetapi juga pada validitas dan penerimaan bukti dalam proses hukum.

Definisi yang lebih luas menyatakan bahwa *digital forensics* adalah cabang dari ilmu forensik yang mencakup

"pemulihan, investigasi, pemeriksaan, dan analisis materi yang ditemukan di perangkat digital," dan diterapkan terutama dalam konteks hukum pidana atau perdata untuk mendukung pengambilan keputusan hukum (Wikipedia, 2025). Proses ini mencakup serangkaian tahapan sistematis — mulai dari identifikasi, akuisisi dan pelestarian bukti digital, hingga pemeriksaan, analisis, dan pelaporan hasil secara sah di pengadilan (Wikipedia, 2025). Pendekatan sistematis ini memastikan bahwa bukti digital tetap utuh, autentik, dan dapat dipertanggungjawabkan tanpa mengubah kondisi aslinya.

Dalam konteks penegakan hukum di Indonesia, digital forensik juga memiliki fungsi penting sebagai alat bukti elektronik yang diakui secara hukum. Mawlidya (2025) menegaskan bahwa *digital forensics* merupakan proses sistematis termasuk identifikasi, pelestarian, pengumpulan, analisis, dan pelaporan bukti digital yang sah di mata hukum, yang sangat dibutuhkan untuk mendukung penyidikan dan penegakan hukum terhadap kejahatan siber (Mawlidya, 2025). Hal ini menandakan bahwa bukti digital tidak hanya menjadi objek teknis investigasi, tetapi juga instrumen hukum yang krusial dalam proses peradilan.

Selanjutnya, bukti digital yang dihasilkan melalui prosedur *IT Forensics* memungkinkan penyidik dan penegak hukum mendapatkan gambaran objektif mengenai kejadian kriminal yang terjadi di ranah digital. Menurut Arfin & Seto Aji (2025), bukti digital memainkan peran penting dalam membuktikan keaslian dan integritas informasi, sehingga diperlukan langkah forensik yang valid dalam penyelidikan modern terhadap kejahatan berbasis teknologi (Arfin & Seto Aji, 2025). Dengan demikian, *IT Forensics* berfungsi tidak hanya untuk mengungkap fakta teknis, tetapi juga untuk menyediakan bukti

yang dapat digunakan secara efektif dalam proses hukum sesuai dengan standar yuridis dan ilmiah yang berlaku.

5.2 Pengertian IT Forensics

IT Forensics, yang juga dikenal sebagai *digital forensic*, merupakan disiplin ilmu yang sistematis dan terstruktur untuk menangani bukti digital yang berasal dari perangkat teknologi informasi. Secara umum, *IT Forensics* melibatkan proses ilmiah yang mencakup identifikasi, pengumpulan, pemeliharaan (*preservation*), analisis, serta penyajian bukti digital yang ditemukan pada perangkat digital seperti komputer, ponsel, server, sistem jaringan, penyimpanan eksternal, hingga perangkat IoT (*Internet of Things*) dengan tujuan mendukung proses hukum dan investigasi (*digital forensics is the process of collecting and analyzing digital evidence while maintaining its integrity and admissibility in court*) (Badman & Forrest, 2024; IBM, 2024).

Dalam konteks penegakan hukum, bukti digital memiliki karakteristik yang lebih kompleks dibandingkan bukti fisik karena sifatnya yang sangat rapuh dan mudah berubah bila tidak ditangani secara tepat. Oleh karena itu, metode *IT Forensics* menekankan pentingnya menjaga **integritas bukti** dan mematuhi prinsip ilmiah serta prosedur yang diakui secara hukum (*Forensic investigators must follow strict forensic procedures to ensure proper handling and protection of digital evidence*) (IBM, 2024).

Tujuan utama *IT Forensics* mencakup beberapa aspek penting yang saling berkaitan:

1. **Menemukan fakta dari data digital**
   Salah satu tujuan utama adalah untuk mengungkap fakta yang tersembunyi dalam bentuk data digital yang berkaitan dengan suatu tindak kejahatan atau insiden

keamanan siber. Proses ini tidak hanya sekadar menemukan file atau rekaman, tetapi juga menafsirkan hubungan temporal antar bukti untuk membantu mengungkap bagaimana peristiwa terjadi (*digital evidence must be analyzed methodically to determine what happened and how it happened*) (Cyberhaven, 2025).

2. **Menjaga integritas dan keaslian bukti**
   Bukti digital yang dikumpulkan harus tetap dalam kondisi aslinya dan dilindungi dari segala bentuk perubahan atau kontaminasi sejak tahap identifikasi hingga pelaporan (*Forensic evidence must be collected and preserved to prevent data loss or corruption*) (IBM, 2024). Hal ini penting untuk memastikan bahwa bukti tersebut dapat diterima di pengadilan dan dianalisis ulang oleh pihak lain jika diperlukan (*maintaining the chain of custody is essential so evidence can be admissible in court and reproduced by other experts*) (Cyberhaven, 2025).
3. **Mendukung proses hukum dan pengambilan keputusan**
   Bukti digital yang telah diperoleh dan dianalisis secara forensik dapat digunakan untuk mendukung proses peradilan dalam menguatkan dakwaan atau pembelaan pihak tertentu. Keabsahan bukti ini sangat bergantung pada prosedur forensik yang benar dan dokumentasi yang lengkap (*digital evidence needs to be retained and documented so it can support legal processes*) (Cyberhaven, 2025).
4. **Mengungkap pola, pelaku, dan metode kejahatan digital**
   Analisis forensik digital juga bertujuan membantu penyidik untuk tidak hanya menemukan bukti, tetapi juga memahami pola serangan siber, teknik yang digunakan oleh pelaku, serta hubungan antara berbagai bukti yang

ditemukan. Dengan demikian, *IT Forensics* berperan penting dalam membantu pihak berwenang mengidentifikasi pelaku serta motif dan metode kejahatan mereka (*Forensic analysis can reveal patterns of activity that help reconstruct the sequence of events in digital incidents*) (Cyberhaven, 2025).

Secara keseluruhan, *IT Forensics* merupakan pendekatan komprehensif yang memadukan prinsip teknologi, metodologi ilmiah, dan standar hukum untuk menangani bukti digital dengan tujuan investigatif dan hukum. Tanpa prosedur yang tepat, bukti digital berisiko terkontaminasi sehingga dapat kehilangan nilai hukumnya, yang pada gilirannya akan menghambat penegakan hukum secara efektif (*evidence must be collected and preserved carefully to retain legal value*) (IBM, 2024).

5.3 Ruang Lingkup IT Forensics

IT Forensics tidak hanya terbatas pada pemeriksaan komputer, tetapi mencakup seluruh ekosistem teknologi digital modern. Setiap jenis perangkat dan sistem memiliki karakteristik data, metode akuisisi, serta teknik analisis yang berbeda. Oleh karena itu, IT Forensics terbagi ke dalam beberapa bidang utama sebagai berikut.

1. ***Computer Forensics***

   Computer Forensics merupakan cabang paling klasik dan fundamental dalam IT Forensics. Bidang ini berfokus pada investigasi data yang terdapat dalam komputer, laptop, dan media penyimpanan seperti hard disk, SSD, flashdisk, dan kartu memori. Data yang dianalisis mencakup sistem operasi, file pengguna, aplikasi, email, log sistem, registry, serta file yang telah dihapus.

Dalam praktiknya, computer forensics digunakan untuk:

a. Mengungkap aktivitas pengguna (misalnya dokumen yang dibuat, dibuka, atau dihapus)
b. Menelusuri riwayat akses dan login
c. Mengidentifikasi malware atau aktivitas ilegal
d. Mere konstruksi kronologi kejadian

Teknik yang digunakan meliputi disk imaging, file carving, analisis metadata, dan *recovery* data terhapus. Computer forensics sering menjadi dasar dalam penyelidikan kasus pencurian data, sabotase sistem, maupun penyalahgunaan komputer di lingkungan organisasi.

2. Mobile Forensics

Mobile Forensics berfokus pada investigasi perangkat seluler seperti smartphone, tablet, dan perangkat komunikasi lainnya. Perangkat ini menyimpan data yang sangat kaya, termasuk:

a. Pesan SMS, WhatsApp, Telegram, dan email
b. Riwayat panggilan dan lokasi (GPS)
c. Foto, video, dan metadata
d. Aktivitas aplikasi dan akun pengguna

Karena perangkat mobile selalu terhubung dengan pengguna, mobile forensics sangat penting dalam mengungkap aktivitas, relasi sosial, dan pergerakan pelaku. Tantangan utama pada mobile forensics adalah sistem keamanan seperti enkripsi, penguncian perangkat, dan sistem operasi yang tertutup (Android dan iOS), sehingga diperlukan alat dan teknik khusus untuk mengekstrak data secara forensik.

3. Network Forensics

Network Forensics berfokus pada analisis lalu lintas jaringan dan aktivitas komunikasi digital. Bidang ini digunakan untuk mengungkap bagaimana data berpindah

antar sistem dan apakah terjadi aktivitas mencurigakan seperti penyusupan, pencurian data, atau serangan siber.

Data yang dianalisis meliputi:

a. Log server dan firewall
b. Trafik jaringan (*packet capture*)
c. Aktivitas login dan akses jarak jauh
d. Komunikasi email dan web

Network forensics sangat penting dalam kasus seperti hacking, serangan DDoS, penyadapan, dan penyusupan jaringan, karena sering kali pelaku tidak meninggalkan jejak di satu perangkat saja, tetapi di seluruh jalur komunikasi.

4. Cloud Forensics

Cloud Forensics merupakan bidang yang relatif baru dan semakin penting seiring meningkatnya penggunaan layanan cloud seperti Google Drive, Dropbox, *Amazon Web Services* (AWS), Microsoft Azure, dan layanan email berbasis web. Dalam cloud forensics, bukti tidak berada dalam satu perangkat fisik, melainkan tersebar di pusat data milik penyedia layanan.

Investigasi cloud mencakup:

a. File yang diunggah atau diunduh
b. Log aktivitas pengguna
c. Riwayat akses dan perubahan data
d. Sinkronisasi antar perangkat

Tantangan utama cloud forensics adalah masalah yurisdiksi hukum, akses terbatas, dan multi-tenancy, karena data satu pengguna berada di infrastruktur yang sama dengan pengguna lain. Oleh karena itu, cloud forensics membutuhkan kerja sama dengan penyedia layanan dan pemahaman hukum lintas negara.

5. **IoT Forensics**

   IoT Forensics berfokus pada investigasi perangkat pintar seperti CCTV, smart home, sensor, wearable devices, alat kesehatan digital, dan sistem smart city. Perangkat IoT menghasilkan data dalam jumlah besar secara terus-menerus, termasuk data sensor, log aktivitas, dan komunikasi ke server pusat.

   IoT forensics digunakan untuk:

   a. Mengungkap rekaman CCTV atau sensor
   b. Menelusuri aktivitas pengguna di lingkungan pintar
   c. Menginvestigasi sabotase sistem atau manipulasi data sensor
   d. Mendukung kasus keamanan fisik dan digital secara bersamaan

Karena perangkat IoT sering memiliki daya simpan dan komputasi terbatas, data biasanya tersebar antara perangkat, gateway, dan cloud, sehingga investigasinya bersifat terdistribusi dan kompleks.

5.4 Prinsip Dasar IT Forensics

Keberhasilan suatu proses IT Forensics tidak hanya ditentukan oleh kecanggihan alat atau kemampuan teknis penyelidik, tetapi terutama oleh kepatuhan terhadap prinsip-prinsip dasar forensik digital. Prinsip-prinsip ini memastikan bahwa bukti digital yang dikumpulkan dan dianalisis dapat dipertanggungjawabkan secara ilmiah dan sah secara hukum.

1. **Integritas Data**

   Integritas data berarti bahwa bukti digital harus tetap dalam kondisi yang sama seperti saat pertama kali ditemukan. Tidak boleh ada perubahan, penghapusan, penambahan, atau modifikasi data selama proses

investigasi berlangsung. Karena data digital sangat mudah diubah, IT Forensics menggunakan prosedur khusus untuk menjaga keaslian data, seperti:

a. Pengambilan salinan forensik (*forensic image*)
b. Penggunaan nilai hash (MD5, SHA-1, SHA-256)
c. Analisis dilakukan pada salinan, bukan pada data asli

Jika integritas data tidak terjaga, maka bukti tersebut kehilangan nilai hukumnya karena tidak dapat dibuktikan bahwa data tersebut benar-benar berasal dari sumber asli dan tidak dimanipulasi. Oleh karena itu, menjaga integritas data adalah **fondasi utama** dari seluruh proses IT Forensics.

2. *Chain of Custody*

Chain of custody adalah catatan resmi yang mendokumentasikan seluruh perjalanan bukti digital sejak pertama kali ditemukan hingga disajikan di pengadilan. Catatan ini mencakup:

a. Siapa yang menemukan bukti
b. Kapan dan di mana bukti diambil
c. Bagaimana bukti disimpan
d. Siapa saja yang mengaksesnya

Prinsip ini bertujuan untuk memastikan bahwa tidak ada pihak yang dapat menyentuh, memodifikasi, atau memalsukan bukti tanpa diketahui. Tanpa chain of custody yang jelas, bukti digital dapat dipertanyakan keabsahannya meskipun secara teknis benar. Oleh karena itu, dokumentasi yang lengkap dan transparan merupakan bagian yang tidak terpisahkan dari praktik IT Forensics.

3. *Repeatability*

Repeatability berarti bahwa proses forensik harus dapat diulang oleh pihak lain dan menghasilkan hasil yang sama. Dengan kata lain, jika penyelidik lain menggunakan

metode dan data yang sama, maka mereka harus mendapatkan temuan yang identik.

Prinsip ini menunjukkan bahwa:

a. Metode yang digunakan bersifat ilmiah
b. Tidak ada manipulasi atau subjektivitas
c. Hasil dapat diverifikasi secara independen

Dalam dunia hukum dan sains, hasil yang tidak dapat diulang tidak dapat dianggap sebagai bukti yang kuat. Oleh karena itu, IT Forensics menuntut penggunaan prosedur, alat, dan teknik yang terdokumentasi dengan baik dan dapat diverifikasi oleh pihak lain.

4. **Legal Compliance**

Semua aktivitas IT Forensics harus dilakukan sesuai dengan hukum dan standar yang berlaku. Ini mencakup:

a. Perizinan penyitaan perangkat
b. Perlindungan privasi dan data pribadi
c. Prosedur penggeledahan digital
d. Standar pembuktian di pengadilan

Jika bukti diperoleh dengan cara yang melanggar hukum, misalnya tanpa izin atau dengan melanggar hak privasi, maka bukti tersebut dapat ditolak di pengadilan meskipun secara teknis valid. Oleh karena itu, IT Forensics selalu berada pada irisan antara teknologi dan hukum, dan penyelidik harus memahami keduanya.

Kesimpulan Prinsip Dasar

Keempat prinsip ini — integritas data, *chain of custody, repeatability,* dan *legal compliance* — membentuk satu kesatuan yang tidak dapat dipisahkan. Tanpa salah satu dari prinsip tersebut, hasil IT Forensics akan kehilangan keabsahan ilmiah atau legalnya. Dengan mematuhi prinsip-prinsip ini, IT

Forensics dapat berfungsi sebagai alat yang kuat untuk mengungkap kebenaran di dunia digital dan menegakkan keadilan secara objektif.

5.5 Tahapan Proses IT Forensics

Proses IT Forensics dilakukan melalui serangkaian tahapan yang sistematis dan terstruktur untuk memastikan bahwa bukti digital yang diperoleh bersifat sah, akurat, dan dapat dipertanggungjawabkan secara hukum dan ilmiah. Setiap tahap memiliki fungsi yang berbeda namun saling berkaitan.

1. ***Identification*** **(Identifikasi)**
   Tahap identifikasi bertujuan untuk menentukan apa saja yang harus diselidiki dalam suatu kasus. Pada tahap ini, penyelidik mengidentifikasi:
   a. Perangkat yang terlibat (komputer, ponsel, server, USB, CCTV, dll.)
   b. Sistem operasi dan aplikasi yang digunakan
   c. Jenis data yang berpotensi menjadi bukti
   d. Lokasi penyimpanan data (lokal, jaringan, atau cloud)

   Tahap ini sangat penting karena kesalahan dalam identifikasi dapat menyebabkan bukti penting terlewatkan atau data yang tidak relevan justru dikumpulkan.
2. ***Collection*** **(Pengumpulan Bukti)**
   Pada tahap ini, data digital yang relevan dikumpulkan dengan metode forensik agar tidak mengubah kondisi aslinya. Metode yang umum digunakan meliputi:
   a. *Imaging hard disk*
      Membuat salinan *bit-per-bit* dari seluruh isi media penyimpanan sehingga semua file, termasuk yang tersembunyi atau terhapus, dapat dianalisis.

b. Cloning perangkat
   Menyalin seluruh sistem dari suatu perangkat ke media lain untuk dianalisis tanpa menyentuh perangkat asli.
c. *Live data acquisition*
   Mengambil data dari sistem yang sedang berjalan, seperti memori (RAM), proses aktif, koneksi jaringan, dan sesi pengguna.

Tujuan tahap ini adalah memperoleh salinan bukti digital yang utuh dan autentik tanpa mengganggu sistem sumber.

3. *Preservation* (Pelestarian)

Tahap ini memastikan bahwa bukti digital yang telah dikumpulkan tidak berubah atau rusak selama proses investigasi. Teknik utama yang digunakan adalah:

a. Hashing (MD5, SHA-1, SHA-256) untuk membuat "sidik jari digital" dari data
b. Penyimpanan dalam media yang aman
c. Pembatasan akses terhadap bukti

Jika nilai hash berubah, itu menandakan adanya modifikasi data. Oleh karena itu, hashing menjadi mekanisme kunci untuk menjamin keaslian dan integritas bukti.

4. *Examination* (Pemeriksaan)

Pada tahap ini, penyelidik mulai menelusuri isi bukti digital untuk mencari data yang relevan dengan kasus. Pemeriksaan meliputi:

a. File dokumen, gambar, dan video
b. Log sistem dan aplikasi
c. Riwayat internet dan email
d. Metadata file (waktu pembuatan, pengubahan, akses)
e. Data yang telah dihapus atau disembunyikan

Tujuan tahap ini adalah menyaring data yang relevan dari jutaan data yang tersimpan dalam sistem.

5. ***Analysis*** **(Analisis)**

   Tahap analisis bertujuan untuk menginterpretasikan hasil pemeriksaan dan menyusun hubungan antar bukti. Di sinilah penyelidik:

   a. Menentukan urutan waktu kejadian
   b. Menghubungkan aktivitas pengguna dengan bukti
   c. Mengidentifikasi pola serangan atau pelanggaran
   d. Menarik kesimpulan tentang siapa, bagaimana, dan kapan suatu peristiwa terjadi

   Analisis ini mengubah data teknis menjadi informasi bermakna yang dapat digunakan dalam penyelidikan dan proses hukum.

6. ***Reporting*** **(Pelaporan)**

   Tahap akhir adalah penyusunan laporan forensik yang berisi:

   a. Metode yang digunakan
   b. Bukti yang ditemukan
   c. Hasil analisis
   d. Kesimpulan

Laporan harus ditulis dengan bahasa yang jelas, objektif, dan dapat dipahami oleh pihak non-teknis seperti penyidik, jaksa, hakim, dan manajemen. Laporan ini menjadi dasar dalam pengambilan keputusan hukum dan organisasi.

5.6 Alat dan Teknologi IT Forensics

Keberhasilan proses IT Forensics sangat ditentukan oleh penggunaan alat (*tools*) dan teknologi forensik yang tepat. Alat-alat ini dirancang untuk memperoleh, memeriksa, menganalisis, dan menyajikan bukti digital tanpa merusak integritas data. Setiap kategori alat memiliki fungsi khusus sesuai dengan jenis bukti dan media yang dianalisis.

1. ***Disk Forensics Tools***
   (EnCase, FTK, Autopsy)
   Disk forensics tools digunakan untuk menganalisis media penyimpanan seperti hard disk, SSD, flashdisk, dan kartu memori. Alat ini memungkinkan penyelidik untuk:
   a. Membuat *forensic image* (salinan bit-per-bit)
   b. Menelusuri file sistem dan file pengguna
   c. Memulihkan file yang terhapus
   d. Menganalisis metadata dan timeline aktivitas

   EnCase dan FTK (*Forensic Toolkit*) merupakan perangkat lunak komersial yang banyak digunakan oleh aparat penegak hukum, sedangkan Autopsy merupakan solusi *open-source* yang sangat populer di dunia akademik dan praktisi forensik. Disk forensics menjadi tulang punggung dalam investigasi kasus pencurian data, penyalahgunaan komputer, dan kejahatan siber berbasis file.
2. ***Mobile Forensics Tools***
   (*Cellebrite, Oxygen Forensic*)
   Mobile forensics tools digunakan untuk mengekstrak dan menganalisis data dari perangkat seluler seperti smartphone dan tablet. Data yang dapat diperoleh meliputi:
   a. Pesan SMS dan aplikasi chat
   b. Riwayat panggilan
   c. Lokasi GPS
   d. Foto, video, dan metadata
   e. Aktivitas aplikasi

   Cellebrite adalah salah satu alat paling banyak digunakan oleh aparat penegak hukum untuk membuka, menyalin, dan menganalisis data dari ponsel, termasuk perangkat yang terkunci atau dienkripsi. *Oxygen Forensic* juga banyak

digunakan untuk analisis lanjutan dan visualisasi hubungan antar data pengguna.

3. ***Network Forensics Tools*** **(*Wireshark, TCPDump*)**

   Network forensics tools digunakan untuk menangkap dan menganalisis lalu lintas jaringan. Dengan alat ini, penyelidik dapat:

   a. Melihat paket data yang dikirim dan diterima
   b. Mendeteksi komunikasi mencurigakan
   c. Mengidentifikasi serangan seperti malware, phishing, dan DDoS
   d. Melacak sumber dan tujuan koneksi

   Wireshark menyediakan antarmuka grafis yang memudahkan analisis paket jaringan, sedangkan **TCPDump** adalah alat berbasis baris perintah yang sering digunakan untuk pemantauan jaringan secara real-time. Network forensics sangat penting dalam kasus peretasan dan penyadapan digital.

4. ***Memory Forensics Tools*** **(*Volatility*)**

   Memory forensics berfokus pada analisis RAM (memori utama) dari sistem yang sedang atau baru saja berjalan. Data dalam RAM sering mengandung:

   a. Proses aktif
   b. Kunci enkripsi
   c. Malware yang belum tersimpan di disk
   d. Koneksi jaringan yang sedang berlangsung

   Volatility adalah alat open-source yang sangat kuat untuk mengekstrak dan menganalisis data dari memory dump. *Memory forensics* sering digunakan untuk mendeteksi malware canggih, rootkit, dan serangan yang bersifat sementara (*fileless attack*).

5. ***Log Analysis Tools***
   (Splunk, ELK Stack)
   Log analysis tools digunakan untuk mengelola dan menganalisis log aktivitas sistem, aplikasi, dan jaringan dalam jumlah besar. Log ini berisi informasi penting seperti:
   a. Waktu login
   b. Aktivitas pengguna
   c. Kesalahan sistem
   d. Akses ke file dan server

   Splunk dan ELK Stack (*Elasticsearch, Logstash*, Kibana) memungkinkan penyelidik untuk mencari pola, memvisualisasikan aktivitas, dan mendeteksi anomali yang menunjukkan adanya pelanggaran keamanan atau kejahatan digital.

Kesimpulan

Berbagai alat IT Forensics ini bekerja secara komplementer untuk membentuk ekosistem investigasi digital yang utuh. Disk forensics, mobile forensics, network forensics, memory forensics, dan log analysis memungkinkan penyelidik memperoleh gambaran menyeluruh tentang apa yang terjadi, bagaimana terjadi, dan siapa yang terlibat dalam suatu insiden digital.

5.7 IT Forensics dalam Penegakan Hukum

Dalam era digital, sebagian besar aktivitas manusia meninggalkan jejak elektronik, baik melalui komputer, ponsel, internet, maupun sistem informasi. Oleh karena itu, IT Forensics menjadi pilar utama dalam sistem penegakan hukum modern, khususnya dalam menangani kejahatan siber dan tindak pidana yang melibatkan teknologi informasi. Melalui pendekatan

forensik digital, aparat penegak hukum dapat mengubah data elektronik menjadi alat bukti yang sah dan meyakinkan.

1. **Pembuktian Kasus Kejahatan Siber**
   Dalam kasus kejahatan siber seperti peretasan, penipuan online, ransomware, dan pencurian data, bukti fisik hampir tidak ada. Yang tersedia adalah **bukti digital**, seperti:
   a. Log sistem dan jaringan
   b. File malware
   c. Email dan pesan elektronik
   d. Aktivitas login dan IP address

   IT Forensics memungkinkan penyidik untuk mengekstrak, memverifikasi, dan menghubungkan bukti-bukti ini sehingga dapat membuktikan:
   a. Bahwa suatu serangan benar-benar terjadi
   b. Bagaimana serangan dilakukan
   c. Sistem apa yang disusupi
   d. Siapa yang bertanggung jawab

   Tanpa IT Forensics, kejahatan siber sulit dibuktikan karena pelaku dapat beroperasi secara anonim dan lintas negara.
2. **Penelusuran Transaksi Digital**
   Dalam banyak kasus pidana modern, kejahatan melibatkan **transaksi digital**, seperti:
   a. Transfer perbankan
   b. E-wallet dan kripto
   c. Marketplace dan e-commerce
   d. Pembayaran online

   IT Forensics digunakan untuk melacak alur transaksi, mengaitkan akun dengan perangkat, serta menghubungkan transaksi dengan identitas pelaku. Analisis log, metadata, dan catatan sistem keuangan digital memungkinkan aparat hukum membongkar jaringan kejahatan dan aliran dana ilegal.

3. **Investigasi Kebocoran Data**
   Kasus kebocoran data pribadi dan rahasia negara atau perusahaan semakin meningkat. Dalam situasi ini, IT Forensics digunakan untuk:
   a. Menentukan sumber kebocoran
   b. Mengidentifikasi metode pencurian data
   c. Mengetahui file apa saja yang diakses atau disalin
   d. Menentukan siapa yang bertanggung jawab

   Melalui analisis log sistem, aktivitas pengguna, dan lalu lintas jaringan, penyidik dapat merekonstruksi bagaimana data keluar dari sistem dan siapa yang melakukannya.
4. **Analisis Rekam Jejak Aktivitas Pelaku**
   Setiap aktivitas digital meninggalkan jejak, seperti waktu login, perubahan file, penggunaan aplikasi, dan komunikasi online. IT Forensics memanfaatkan jejak ini untuk membangun profil aktivitas pelaku, termasuk:
   a. Waktu dan durasi aktivitas
   b. Perangkat yang digunakan
   c. Lokasi dan koneksi jaringan
   d. Pola perilaku digital

Rekonstruksi ini membantu aparat hukum membuktikan keterlibatan seseorang dalam suatu peristiwa pidana secara objektif dan berbasis data.

Bukti Digital dalam Proses Pengadilan

Bukti digital hasil IT Forensics dapat digunakan di pengadilan apabila memenuhi dua syarat utama:

1. **Keabsahan hukum** (diperoleh secara legal dan sesuai prosedur)
2. **Integritas teknis** (data tidak berubah dan dapat diverifikasi)

Jika kedua syarat ini terpenuhi, bukti digital memiliki kekuatan pembuktian yang setara, bahkan sering lebih kuat, dibandingkan bukti fisik, karena berbasis rekaman objektif aktivitas sistem.

Kesimpulan

IT Forensics menjadikan dunia digital tidak lagi tanpa hukum. Dengan teknik forensik yang tepat, setiap aktivitas elektronik dapat dilacak, dianalisis, dan dipertanggungjawabkan di hadapan hukum. Inilah yang membuat IT Forensics menjadi instrumen strategis dalam menjaga keadilan, keamanan, dan kepercayaan publik di era teknologi informasi.

5.8 Tantangan dalam IT Forensics

Perkembangan teknologi informasi yang sangat pesat menjadikan IT Forensics tidak hanya semakin penting, tetapi juga semakin kompleks. Penyidik forensik digital saat ini dihadapkan pada berbagai tantangan teknis, hukum, dan operasional yang menuntut kemampuan lintas disiplin. Beberapa tantangan utama dalam IT Forensics meliputi:

1. **Enkripsi Data**

   Banyak sistem modern menggunakan enkripsi tingkat tinggi, baik pada perangkat, aplikasi, maupun komunikasi jaringan. Smartphone, layanan pesan instan, cloud storage, dan sistem keuangan digital semuanya menerapkan end-*to-end encryption.*

   Bagi IT Forensics, hal ini menimbulkan kesulitan besar karena:

   a. Data tidak dapat dibaca tanpa kunci enkripsi
   b. Akses paksa berpotensi merusak integritas bukti

c. Pengadilan tetap menuntut bukti yang dapat diverifikasi

Akibatnya, penyidik harus menggunakan teknik lanjutan seperti memory forensics, key extraction, atau kerja sama dengan penyedia layanan.

2. **Volume Data yang Sangat Besar (Big Data)**

Perangkat modern menyimpan data dalam jumlah luar biasa besar, mencakup:

a. File sistem
b. Media sosial
c. Riwayat browsing
d. Log aplikasi
e. Cloud synchronization

Menganalisis terabyte data membutuhkan waktu, sumber daya komputasi tinggi, serta metode pemfilteran cerdas. Tanpa teknologi otomatisasi dan AI, penyidik berisiko kehilangan bukti penting di antara jutaan data yang tidak relevan.

3. ***Cloud Computing* dan Lintas Negara**

Banyak data kini tidak lagi tersimpan di perangkat lokal, tetapi berada di *server cloud* yang tersebar di berbagai negara. Ini menimbulkan persoalan:

a. Yurisdiksi hukum yang berbeda
b. Prosedur permintaan data lintas negara yang lama
c. Perbedaan standar perlindungan privasi

Situasi ini sering memperlambat atau bahkan menggagalkan proses forensik meskipun secara teknis data masih ada.

4. **Perkembangan Malware dan Artificial Intelligence**

Malware modern tidak lagi sederhana. Kini malware menggunakan:

a. Pola adaptif

b. Enkripsi internal
c. Teknik menyembunyikan jejak
d. Bahkan kecerdasan buatan untuk menghindari deteksi

Ini membuat proses analisis menjadi jauh lebih sulit karena malware dapat memodifikasi diri, menghapus jejak, atau menyamar sebagai proses sistem normal.

5. **Manipulasi dan Anti-Forensik**

   Pelaku kejahatan digital semakin canggih dalam menghapus atau merusak bukti. Teknik anti-forensik meliputi:

   a. Penghapusan aman (*secure deletion*)
   b. Pemalsuan timestamp
   c. Log wiping
   d. Penggunaan software anonymizer dan VPN

Tujuannya adalah membuat penyelidikan gagal atau bukti tidak dapat diterima di pengadilan.

Kesimpulan

IT Forensics menghadapi tantangan yang terus berkembang seiring kemajuan teknologi. Enkripsi, big data, cloud, malware canggih, dan teknik anti-forensik menjadikan penyelidikan digital sebagai medan yang dinamis dan kompleks. Oleh karena itu, keberhasilan IT Forensics sangat bergantung pada kombinasi teknologi mutakhir, keahlian penyidik, serta dukungan hukum dan kebijakan internasional.

5.9 Relevansi IT Forensics dalam Era AI dan IoT

Perkembangan *Artificial Intelligence* (AI), *Internet of Things* (IoT), dan sistem cerdas telah mentransformasi cara data diciptakan, diproses, dan disimpan. Bukti digital tidak lagi hanya berasal dari komputer dan ponsel, tetapi kini dihasilkan

oleh ribuan perangkat pintar yang bekerja secara otomatis dan terdistribusi. Sensor, algoritma, dan sistem cerdas menghasilkan jejak digital yang sangat kaya, sekaligus sangat kompleks untuk dianalisis secara forensik.

Dalam konteks ini, bukti digital modern dapat berasal dari berbagai sumber, antara lain:

1. **Sensor medis** (monitor jantung, alat ukur tekanan darah, alat pemantau gula darah)
2. ***Smart farming systems*** (sensor tanah, drone pertanian, sistem irigasi otomatis)
3. **Sistem rumah sakit digital** (*Electronic Medical Records*, sistem antrian, IoT medis)
4. **Perangkat *wearable*** (*smartwatch, fitness tracker, biosensor*)

Setiap perangkat tersebut secara kontinu merekam waktu, lokasi, kondisi fisiologis, dan aktivitas pengguna. Data ini sangat bernilai dalam konteks forensik karena dapat:

1. Menunjukkan kronologi kejadian
2. Membuktikan kehadiran atau aktivitas seseorang
3. Mengungkap kelalaian, manipulasi, atau penyalahgunaan sistem

Dalam sistem kesehatan digital, misalnya, log dari alat monitoring pasien dan sistem rekam medis dapat digunakan untuk menyelidiki dugaan malpraktik, manipulasi data klinis, atau serangan siber terhadap rumah sakit. Demikian pula dalam *smart farming,* data sensor dan AI dapat membuktikan adanya sabotase digital, pemalsuan data produksi, atau serangan terhadap sistem irigasi dan distribusi pupuk.

Lebih jauh, integrasi AI menimbulkan tantangan baru dalam forensik digital. Sistem AI bersifat:

1. *Black box* (keputusan sulit dijelaskan)
2. *Self-learning*
3. Berbasis data besar

Oleh karena itu, IT Forensics tidak hanya menganalisis file dan log, tetapi juga harus mampu melakukan:

1. Forensik model AI
2. Audit data pelatihan
3. Pelacakan keputusan algoritmik

Dalam konteks pengembangan yang Bapak lakukan—seperti sistem kesehatan digital, IoT medis, dan *smart agriculture*—IT Forensics menjadi pilar penting untuk:

1. Menjamin keamanan dan keandalan sistem
2. Menyediakan mekanisme audit dan pembuktian
3. Mendukung keabsahan data dalam kebijakan dan layanan publik

Dengan demikian, IT Forensics tidak lagi hanya berfungsi sebagai alat penegakan hukum, tetapi juga sebagai komponen fundamental dalam tata kelola sistem digital modern, terutama pada sektor strategis seperti kesehatan dan pertanian berbasis teknologi.

5.10 Penutup

IT Forensics merupakan salah satu pilar utama dalam menjaga keamanan, keadilan, dan kepercayaan di era digital. Di tengah meningkatnya ketergantungan masyarakat terhadap sistem informasi, jaringan, dan teknologi cerdas, setiap aktivitas manusia kini meninggalkan jejak digital yang berpotensi menjadi bukti hukum. Oleh karena itu, kemampuan untuk

mengelola, melindungi, dan menganalisis bukti digital secara ilmiah dan sah menjadi kebutuhan yang tidak dapat dihindari.

Peran IT Forensics tidak hanya terbatas pada pengungkapan kejahatan siber, tetapi juga mencakup perlindungan sistem kritis, audit keamanan, serta pengawasan terhadap penyalahgunaan teknologi. Dalam konteks institusi pemerintahan, rumah sakit, perbankan, pendidikan, dan industri berbasis data, IT Forensics berfungsi sebagai mekanisme akuntabilitas yang memastikan bahwa setiap aktivitas digital dapat dipertanggungjawabkan secara teknis dan hukum.

Dengan semakin berkembangnya AI, IoT, dan sistem cerdas, ruang lingkup IT Forensics akan terus meluas. Bukti digital kini berasal dari sensor, algoritma, sistem otomatis, dan infrastruktur terdistribusi. Hal ini menuntut pendekatan forensik yang lebih canggih, multidisipliner, serta berbasis standar internasional.

Bagi praktisi teknologi informasi, penegak hukum, dan peneliti, penguasaan IT Forensics bukan lagi sekadar keahlian tambahan, melainkan kompetensi strategis untuk menjamin keamanan data, integritas sistem, serta keadilan di masyarakat digital. Dengan penerapan IT Forensics yang kuat, kepercayaan publik terhadap teknologi dapat dipertahankan dan risiko penyalahgunaan teknologi dapat diminimalkan secara signifikan.

DAFTAR PUSTAKA

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.

Casey, E. (2019). *Digital forensic investigation and evidence*. Academic Press.

Carrier, B. (2005). *File system forensic analysis*. Addison-Wesley.

Dogan, S., Akbal, E., & Buldu, A. (2020). Digital forensics in the Internet of Things (IoT). *Journal of Information Security and Applications, 52*, 102470. https://doi.org/10.1016/j.jisa.2020.102470

Karie, N. M., Kebande, V. R., Venter, H. S., & Choo, K. K. R. (2019). On the importance of standardising digital forensic terminology. *Digital Investigation, 28*, S20–S29. https://doi.org/10.1016/j.diin.2019.04.004

Mason, S., & Seng, D. (Eds.). (2017). *Electronic evidence* (4th ed.). Institute of Advanced Legal Studies.

National Institute of Standards and Technology. (2014). *Guide to integrating forensic techniques into incident response (SP 800-86)*. NIST.

National Institute of Standards and Technology. (2020). *Digital forensics and incident response (NISTIR 8425)*. NIST.

Palmer, G. (2001). A road map for digital forensic research. *Digital Forensic Research Workshop (DFRWS)*.

Quick, D., & Choo, K. K. R. (2018). Impacts of increasing volume of digital forensic data. *Digital Investigation, 26*, S85–S93. https://doi.org/10.1016/j.diin.2018.04.006

Raghavan, S. (2013). Digital forensic research: Current state of the art. *CSI Transactions on ICT, 1*(1), 91–114.

Roussev, V. (2016). Digital forensic science: Issues, methods, and challenges. *Synthesis Lectures on Information*

Security, Privacy, and Trust. Morgan & Claypool.

Stallings, W., & Brown, L. (2021). *Computer security: Principles and practice* (5th ed.). Pearson.

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigation of cloud computing systems. *Network Security, 2011*(3), 4–10.

Zawoad, S., & Hasan, R. (2015). FAIoT: Towards building a forensics aware eco system for the Internet of Things. *IEEE International Conference on Services Computing*, 279–284. https://doi.org/10.1109/SCC.2015.47

BAB 6
UU TENTANG HAK CIPTA

6.1 Ketentuan Umum Hak Cipta

Hak cipta merupakan salah satu bentuk hak kekayaan intelektual yang memberikan perlindungan hukum terhadap karya cipta baik di bidang ilmu pengetahuan, seni, dan sastra (Imaniyati, 2024). Di Indonesia, pengaturan hak cipta telah mengalami beberapa kali perubahan. Undang-Undang Hak Cipta (UUHC) di Indonesia pertama kali diatur melalui Undang-Undang Nomor 6 Tahun 1982 tentang Hak Cipta. Selanjutnya, undang-undang tersebut mengalami perubahan dengan diterbitkannya Undang-Undang Nomor 7 Tahun 1987. Pada tahun 1997, pengaturan mengenai hak cipta kembali disempurnakan melalui Undang-Undang Nomor 12 Tahun 1997. Perkembangan selanjutnya terjadi pada tahun 2002 dengan berlakunya Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta. Seiring dengan pesatnya perkembangan teknologi dan kebutuhan perlindungan karya intelektual di era digital, Undang-Undang Nomor 19 Tahun 2002 kemudian dicabut dan digantikan oleh Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, yang berlaku hingga saat ini.

Undang-Undang Nomor 28 Tahun 2014 mendefinisikan hak cipta sebagai hak eksklusif pencipta yang timbul secara otomatis setelah suatu ciptaan diwujudkan dalam bentuk nyata (2014). Prinsip ini menegaskan bahwa perlindungan hak cipta tidak bergantung pada pendaftaran, melainkan pada adanya proses kreatif yang menghasilkan karya orisinal. Dengan

demikian, setiap karya yang telah diwujudkan secara nyata telah memperoleh perlindungan hukum (Haryono, 2025).

Ketentuan umum hak cipta mengatur subjek dan objek hak cipta. Subjek hak cipta meliputi pencipta dan pemegang hak cipta, yang dalam bidang informatika dapat berupa individu, tim, maupun institusi. Objek hak cipta mencakup berbagai karya, termasuk program komputer dan karya digital lainnya, yang memiliki kedudukan hukum setara dengan ciptaan di bidang lain. Objek hak cipta mencakup setiap hasil karya cipta di bidang ilmu pengetahuan, seni, dan sastra yang telah diwujudkan dalam bentuk nyata (Amin, Jenar et al., 2024). Dalam konteks informatika, objek hak cipta meliputi program komputer, basis data, dokumentasi sistem, desain antarmuka, dan berbagai bentuk karya digital lainnya. Pengakuan terhadap karya informatika sebagai objek hak cipta menunjukkan bahwa hasil kerja profesional di bidang teknologi informasi memiliki perlindungan hukum yang setara dengan ciptaan di bidang lainnya (Rizkia and Fardiansyah, 2022).

6.2 Ruang Lingkup Hak Cipta

Ruang lingkup hak cipta menurut Undang-Undang Nomor 28 Tahun 2014 mencakup seluruh ciptaan di bidang ilmu pengetahuan, seni, dan sastra yang telah diwujudkan dalam bentuk nyata. Perlindungan hak cipta diberikan terhadap ciptaan yang merupakan hasil ekspresi kreativitas manusia dan memiliki bentuk tertentu, baik dalam media konvensional maupun digital. Dengan demikian, hak cipta melindungi ekspresi suatu ide, bukan ide atau gagasan itu sendiri (Nainggolan, 2023). Suatu ciptaan dapat memperoleh perlindungan hak cipta apabila memenuhi kriteria tertentu. Ciptaan tersebut harus bersifat orisinal, artinya lahir dari kemampuan intelektual pencipta dan bukan hasil peniruan.

Selain itu, ciptaan harus telah diwujudkan dalam bentuk nyata sehingga dapat dilihat, didengar, atau dibaca. Perlindungan hak cipta tidak diberikan terhadap ide, konsep, atau metode yang belum diwujudkan dalam bentuk ekspresi nyata (Imaniyati, 2024).

Ciptaan yang dilindungi meliputi ciptaan dalam bidang ilmu pengetahuan, seni, dan sastra (Bab V Bagian Kedua Pasal 40). Ciptaan yang dilindungi terdiri atas:

1. Buku, pamflet, perwajahan karya tulis yang diterbitkan, dan semua hasil karya tulis lainnya
2. Ceramah, kuliah, pidato, dan ciptaan sejenis lainnya
3. Alat peraga yang dibuat untuk kepentingan pendidikan dan ilmu pengetahuan
4. Lagu dan/atau musik dengan atau tanpa teks
5. Drama, drama musikal, tari, koreografi, pewayangan, dan pantomim;
6. Karya seni rupa dalam segala bentuk seperti lukisan, gambar, ukiran, kaligrafi, seni pahat, patung, atau kolase
7. Karya seni terapan
8. Karya arsitektur
9. Peta
10. Karya seni batik atau seni motif lain
11. Karya fotografi
12. Potret
13. Karya sinematograh
14. Terjemahan, tafsir, saduran, bunga rampai, basis data, adaptasi, aransemen, modifikasi dan karya lain dari hasil transformasi
15. Terjemahan, adaptasi, aransemen, transformasi, atau modihkasi ekspresi budaya tradisional
16. Kompilasi ciptaan atau data, baik dalam format yang dapat dibaca dengan program komputer maupun media lainnya

17. Kompilasi ekspresi budaya tradisional selama kompilasi tersebut merupakan karya yang asli
18. Permainan video
19. Program komputer

Dalam konteks perkembangan teknologi informasi, ruang lingkup hak cipta juga mencakup ciptaan berbasis digital. Program komputer, basis data, permainan video, dan karya multimedia merupakan ciptaan yang secara tegas dilindungi, sehingga penggandaan, modifikasi, atau distribusinya tanpa izin merupakan pelanggaran hukum sekaligus pelanggaran etika profesi. Perlindungan ini menjadi sangat penting mengingat kemudahan penggandaan dan distribusi karya digital melalui teknologi informasi (Nainggolan, 2023).

Ruang lingkup hak cipta juga berkaitan dengan subjek dan kepemilikan hak cipta, khususnya dalam hubungan kerja dan proyek informatika. Dalam praktik profesional, ciptaan dapat dihasilkan dalam hubungan kerja atau berdasarkan perjanjian tertentu, sehingga kepemilikan hak cipta dapat berada pada pihak pemberi kerja atau pihak yang menyepakati dalam kontrak. Oleh karena itu, kejelasan pengaturan hak cipta sejak awal menjadi penting untuk mencegah sengketa di kemudian hari.

Dalam perspektif etika profesi informatika, pemahaman terhadap ruang lingkup hak cipta mendorong profesional untuk menghormati karya intelektual orang lain dan menggunakan ciptaan secara sah dan bertanggung jawab. Dengan memahami apa saja yang dilindungi dan batas-batas perlindungannya, profesional informatika diharapkan mampu menjaga integritas, keadilan, dan profesionalisme dalam setiap aktivitas yang berkaitan dengan penciptaan dan pemanfaatan karya teknologi informasi.

6.3 Perlindungan Hak Cipta atas Karya

Perlindungan hak cipta merupakan upaya hukum yang diberikan oleh negara kepada pencipta atau pemegang hak cipta untuk menjamin pengakuan dan pengamanan atas karya cipta yang dihasilkannya. Berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, perlindungan hak cipta diberikan sejak suatu ciptaan diwujudkan dalam bentuk nyata, tanpa mensyaratkan adanya pendaftaran. Prinsip perlindungan otomatis ini bertujuan untuk memberikan kepastian hukum dan mendorong lahirnya kreativitas serta inovasi (Amin, Jenar et al., 2024). Undang-Undang Hak Cipta juga membedakan antara hak moral dan hak ekonomi yang melekat pada pencipta (2014).

1. Hak Moral (Bab II Bagian Kedua Pasal 5-7)

Hak yang melekat pada pencipta yang tidak dapat dihilangkan atau dihapus dengan alasan apapun walaupun hak ekonominya telah dialihkan. Hak moral yang berlaku untuk pencipta yakni :

a. Mengubah ciptaan
b. Mengubah judul dan sub judul ciptaan
c. Tetap mencantumkan namanya atau tidak
d. Menggunakan nama alias atau samaran
e. Mempertahankan haknya jika terjadi distorsi, mutilasi, dan modifikasi ciptaan atau hal lain yang bersifat merugikan kehormatan atau reputasi pencipta

Hak moral pada prinsipnya tidak dapat dialihkan kepada pihak lain selama pencipta masih hidup. Namun demikian, pelaksanaan hak moral dapat dialihkan kepada pihak lain melalui wasiat atau cara lain sesuai ketentuan peraturan perundang-undangan. Pengalihan pelaksanaan hak moral tersebut berlaku setelah pencipta wafat. Dalam hal pelaksanaan hak moral telah dialihkan, penerima hak dapat

memilih untuk melaksanakan, melepaskan, atau menolak pelaksanaan hak tersebut, dengan pernyataan yang dibuat secara tertulis.

2. Hak Ekonomi (Bab II Bagian Ketiga Pasal 8 & 9)

Hak pencipta untuk memperoleh manfaat ekonomi atas suatu ciptaan. Hak ekonomi mencakup hak melaksanakan sendiri, memberikan izin, atau melarang pihak lain untuk melakukan :

a. Penerbitan ciptaan
b. Penggandaan ciptaan dalam segala bentuknya
c. Penerjemahan ciptaan
d. Pengadaptasian, pengaransemenan, pentransformasian ciptaan
e. Pendisitribusian ciptaan atau salinannya
f. Pertunjukan ciptaan
g. Pengumuman ciptaan
h. Komunikasi ciptaan
i. Penyewaan ciptaan

Hak ekonomi tetap berada di tangan pencipta atau pemegang hak cipta selama tidakk dialihkan secara hukum. Pengalihan hak cipta dapat dilakukan melalui :

a. Pewarisan
b. Hibah
c. Wakaf
d. Wasiat
e. Perjanjian Tertulis

Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta mengatur bahwa perlindungan hak cipta diberikan dalam jangka waktu tertentu dan tidak berlaku tanpa batas. Pengaturan mengenai jangka waktu perlindungan ini

dimaksudkan untuk memberikan keseimbangan antara kepentingan pencipta dan kepentingan publik dalam mengakses karya cipta. Masa berlaku hak cipta dibagi berdasarkan masa berlaku hak moral dan masa berlaku hak ekonomi (Haryono, 2025).

1. **Masa Berlaku Hak Moral (Bab IX Bagian Kesatu Pasal 57)**
   Hak moral pencipta yang berkaitan dengan hak untuk mencantumkan nama, menggunakan nama samaran, serta mempertahankan reputasi dan kehormatan pencipta berlaku tanpa batas waktu. Hak-hak ini tetap melekat pada pencipta, meskipun hak ekonomi atas ciptaan telah dialihkan kepada pihak lain. Sementara itu, hak moral yang berkaitan dengan hak untuk mengubah ciptaan dan hak untuk mengubah judul atau anak judul ciptaan berlaku selama masa perlindungan hak cipta atas ciptaan tersebut masih berlangsung.

2. **Masa Berlaku Hak Ekonomi (Bab IX Bagian Kesatu)**
   Undang-Undang Hak Cipta mengatur bahwa perlindungan hak cipta tidak bersifat seragam untuk semua jenis ciptaan. Jangka waktu perlindungan berbeda tergantung pada siapa pemiliknya dan jenis ciptaannya.
   a. **Ciptaan dengan Perlindungan Seumur Hidup Pencipta + 70 Tahun (Pasal 58)**
      Hak cipta individu : hak cipta berlaku selama hidup pencipta dan terus berlangsung selama 70 tahun setelah pencipta meninggal dunia, terhitung mulai tanggal 1 Januari tahun berikutnya.
      Hak cipta lebih dari 2 orang : masa perlindungan hak cipta berlaku selama hidup pencipta yang meninggal dunia paling akhir dan terus berlangsung selama 70 tahun

setelahnya, terhitung sejak tanggal 1 Januari tahun berikutnya.

Hak cipta badan hukum : perlindungan hak cipta diberikan selama 50 tahun sejak ciptaan pertama kali diumumkan kepada publik.

Hak cipta sebagaimana diatur dalam Pasal 58 mencakup ciptaan berupa :

1) Buku, pamflet, dan semua hasil karya tulis lainnya
2) Ceramah, kuliah, pidato, dan ciptaan sejenis lainnya
3) Alat peraga yang dibuat untuk kepentingan pendidikan dan ilmu pengetahuan
4) Lagu atau musik dengan atau tanpa teks
5) Drama, drama musikal, tari, koreografi, pewayangan, dan pantomim
6) Karya seni rupa dalam segala bentuk seperti lukisan, gambar, ukiran, kaligrafi, seni pahat, patung, atau kolase
7) Karya arsitektur
8) Peta
9) Karya seni batik atau seni motif lain

b. Ciptaan dengan Perlindungan 50 Tahun Sejak Pengumuman (Pasal 59)

Perlindungan hak cipta sebagaimana diatur dalam Pasal 59 Undang-Undang Nomor 28 Tahun 2014 diberikan terhadap ciptaan tertentu dengan jangka waktu perlindungan selama **50 tahun** sejak pertama kali dilakukan pengumuman. Ketentuan ini berlaku bagi ciptaan yang karakteristiknya erat dengan perkembangan teknologi, media, dan karya turunan.

Ciptaan yang termasuk dalam Pasal 59 meliputi:

1) Karya fotografi;

2) Potret;
3) Karya sinematografi;
4) Permainan video;
5) Program komputer;
6) Perwajahan karya tulis;
7) Terjemahan, tafsir, saduran, bunga rampai, basis data, adaptasi, aransemen, modifikasi, dan karya lain hasil transformasi;
8) Terjemahan, adaptasi, aransemen, transformasi, atau modifikasi ekspresi budaya tradisional;
9) Kompilasi ciptaan atau data, baik dalam format yang dapat dibaca dengan program komputer maupun media lainnya; dan
10) Kompilasi ekspresi budaya tradisional, sepanjang kompilasi tersebut merupakan karya yang asli.

Selain itu, perlindungan hak cipta atas ciptaan berupa karya seni terapan diberikan selama 25 tahun sejak pertama kali dilakukan pengumuman.

c. Ciptaan dengan Perlindungan Khusus oleh Negara (Pasal 60)

Perlindungan hak cipta atas ekspresi budaya tradisional yang dipegang oleh negara berlaku tanpa batas waktu. Ketentuan ini bertujuan untuk menjaga dan melindungi warisan budaya bangsa agar tidak disalahgunakan oleh pihak lain. Sementara itu, hak cipta atas ciptaan yang penciptanya tidak diketahui dan dipegang oleh negara dilindungi selama 50 tahun sejak pertama kali ciptaan tersebut diumumkan kepada publik. Perlindungan yang sama juga berlaku terhadap ciptaan yang diumumkan oleh pihak yang melakukan pengumuman, dengan jangka

waktu perlindungan selama **50 tahun** sejak pengumuman pertama.

6.4 Pelanggaran Hak Cipta

Pelanggaran hak cipta adalah setiap perbuatan yang dilakukan tanpa izin pencipta atau pemegang hak cipta yang melanggar hak moral dan/atau hak ekonomi atas suatu ciptaan (Haryono, 2025). Undang-Undang Nomor 28 Tahun 2014 menegaskan bahwa hak cipta memberikan hak eksklusif kepada pencipta, sehingga setiap pemanfaatan ciptaan di luar ketentuan yang diizinkan dapat dikenakan sanksi hukum (Imaniyati, 2024). Dalam praktik, pelanggaran hak cipta banyak terjadi pada karya berbasis teknologi informasi dan digital, seperti program komputer, permainan video, basis data, serta konten digital lainnya. Pelanggaran tersebut dapat dilakukan secara sengaja maupun tidak sengaja, baik untuk kepentingan pribadi maupun komersial (Sophar Maru Hutagalung, 2022).

Dalam etika profesi informatika, kepatuhan terhadap hak cipta mencerminkan sikap profesional, jujur, dan bertanggung jawab. Profesional informatika diharapkan mampu menghargai karya intelektual orang lain, menggunakan perangkat lunak secara legal, serta menghindari praktik pelanggaran hak cipta dalam setiap aktivitas akademik maupun profesional.

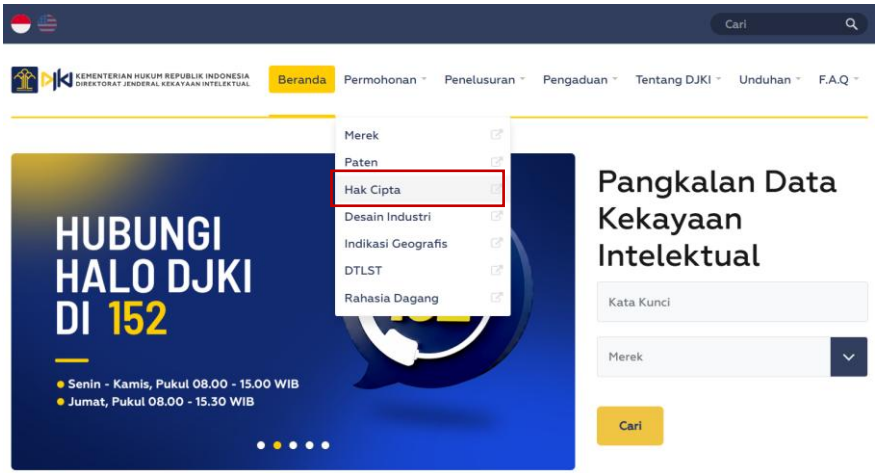
Ketentuan pidana pelanggaran hak cipta dijelasakan pada UU No. 28 Tahun 2014 Pasal 112 sampai dengan 120 sebagai berikut.

Pasal	Tindak Pelanggaran	Sanksi
Pasal 112	Menghilangkan, mengubah, merusak informasi manajemen hak cipta dan/atau sarana pengendali teknologi yang melindungi ciptaan	Pidana penjara paling lama 2 tahun dan/atau denda paling banyak Rp300.000.000
Pasal 113	Ayat (1) Melanggar hak ekonomi pencipta tanpa izin	Pidana penjara paling lama 1 tahun dan/atau denda paling banyak Rp100.000.000
	Ayat (2) Menggandakan ciptaan untuk tujuan komersial tanpa izin	Pidana penjara paling lama 3 tahun dan/atau denda paling banyak Rp500.000.000
	Ayat (3) Menggandakan dan/atau mendistribusikan ciptaan secara komersial	Pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp1.000.000.000
	Ayat (4) Melakukan pembajakan ciptaan secara komersial	Pidana penjara paling lama 10 tahun dan/atau denda paling banyak Rp4.000.000.000
Pasal 114	Pelanggaran hak ekonomi tertentu secara berulang atau dalam skala besar	Pidana penjara dan/atau denda sesuai ketentuan pemberatan
Pasal 115	Pelanggaran hak pelaku pertunjukan, produser fonogram, atau lembaga penyiaran	Pidana penjara dan/atau denda
Pasal 116	Pelanggaran hak ekonomi produser fonogram	Pidana penjara dan/atau denda
Pasal 117	Penggunaan ciptaan tanpa izin dalam bentuk atau media tertentu	Pidana penjara dan/atau denda

Pasal	Tindak Pelanggaran	Sanksi
Pasal 118	Pelanggaran hak cipta yang dilakukan oleh korporasi	Pidana denda dan/atau pidana tambahan bagi korporasi
Pasal 119	Barang hasil pelanggaran hak cipta	Perampasan dan/atau pemusnahan barang hasil pelanggaran
Pasal 120	Ketentuan penuntutan tindak pidana hak cipta	Tindak pidana hak cipta merupakan delik aduan

6.5 Prosedur Pendaftaran Hak Cipta - HKI

Pendaftaran hak cipta merupakan proses pencatatan resmi suatu ciptaan pada negara yang diselenggarakan oleh Direktorat Jenderal Kekayaan Intelektual (DJKI). Pencatatan hak cipta tetap memiliki nilai strategis sebagai alat bukti hukum yang kuat apabila terjadi sengketa di kemudian hari (Sophar Maru Hutagalung, 2022). Oleh karena itu, pemahaman terhadap prosedur pendaftaran hak cipta menjadi penting, khususnya bagi profesional dan akademisi di bidang informatika (Juwita, 2022). Prosedur pendaftaran hak cipta dilakukan secara elektronik melalui sistem resmi yang disediakan oleh DJKI yang dapat diakses di www.dgip.go.id. Proses ini terdiri atas beberapa tahapan administratif yang harus dilalui oleh pencipta atau pemegang hak cipta.



Prosedur pendaftaran hak cipta yakni sebagai berikut :

1. Registrasi dan Login Akun DJKI
   Pemohon terlebih dahulu melakukan pendaftaran akun pada sistem pendaftaran hak cipta yang disediakan oleh DJKI di hakcipta.dgip.go.id. Akun ini berfungsi sebagai identitas resmi pemohon dan digunakan untuk seluruh proses permohonan hak cipta.
2. Pemilihan Jenis Permohonan Hak Cipta
   Pemohon memilih opsi "Hak Cipta - Permohonan Baru" pada dashboard setelah login. Pada tahap ini, pemohon memastikan bahwa permohonan yang diajukan adalah pencatatan hak cipta atas ciptaan yang belum pernah dicatatkan sebelumnya.
3. Pengisian Formulir Permohonan
   Pemohon mengisi formulir permohonan secara lengkap dan benar, yang mencakup identitas pencipta dan/atau pemegang hak cipta, judul ciptaan, jenis ciptaan, serta waktu dan tempat pertama kali ciptaan diumumkan. Informasi ini akan dicantumkan dalam Daftar Umum Ciptaan.

4. Pengunggahan Dokumen Pendukung
   Pemohon mengunggah dokumen pendukung sesuai dengan ketentuan, antara lain contoh ciptaan, surat pernyataan kepemilikan ciptaan, serta dokumen identitas pencipta atau pemegang hak cipta. Untuk karya di bidang informatika, contoh ciptaan dapat berupa berkas digital yang merepresentasikan program komputer atau aplikasi.
5. Pembayaran Biaya Pendaftaran
   Setelah seluruh data dan dokumen diunggah, sistem akan menerbitkan kode billing sebagai dasar pembayaran Penerimaan Negara Bukan Pajak (PNBP). Pemohon wajib menyelesaikan pembayaran agar permohonan dapat diproses lebih lanjut.
6. Pemeriksaan Administratif oleh DJKI
   DJKI melakukan pemeriksaan administratif terhadap permohonan yang diajukan untuk memastikan kelengkapan dan kesesuaian data. Pemeriksaan ini bersifat administratif dan tidak mencakup penilaian substansi atau keaslian ciptaan.
7. Pencatatan dan Penerbitan Surat Pencatatan
   Apabila permohonan dinyatakan memenuhi persyaratan, ciptaan akan dicatat dalam Daftar Umum Ciptaan. Pencatatan ini menandai bahwa ciptaan telah terdaftar secara resmi pada negara.
8. Unduh Dokumen Pencatatan
   Setelah pencatatan dilakukan, DJKI menerbitkan Surat Pencatatan Ciptaan. Pemohon dapat mengunduh surat tersebut melalui sistem sebagai bukti formal pencatatan hak cipta yang dapat digunakan untuk kepentingan hukum, kerja sama lisensi, maupun pengelolaan kekayaan intelektual.

DAFTAR PUSTAKA

2014. Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta. Indonesia, Jaringan Dokumentasi dan Informasi Hukum Direktorat Jenderal Kekayaan Intelektual.

Amin, F. et al. 2024. *Hukum Kekayaan Intelektual*: Sada Kurnia Pustaka.

Haryono 2025. *PENGAKUAN DAN PERLINDUNGAN HAK CIPTA DALAM KONTEKS FILOSOFI DAN TEORI*: Magnum Pustaka.

Imaniyati, N.S. 2024. *Hukum Kekayaan Intelektual: Kekayaan Intelektual, Hak Kekayaan Intelektual, Hak Cipta, Paten, dan Merek*: Prenada Media.

Juwita 2022. *Hak Kekayaan Intelektual Sebagai Bentuk Perlindungan Hukum*: Stiletto Book.

Nainggolan, B. 2023. *PEMBERDAYAAN HUKUM HAK CIPTA DAN LEMBAGA MANAJEMEN KOLEKTIF*: Penerbit Alumni.

Rizkia, N.D. and Fardiansyah, H. 2022. *HAK KEKAYAAN INTELEKTUAL SUATU PENGANTAR*: Penerbit Widina.

Sophar Maru Hutagalung, S.H.M.H. 2022. *Hak Cipta: Kedudukan dan Perannya dalam Pembangunan*: Sinar Grafika.

BAB 7
PROSEDUR PENDIRIAN BISNIS, KONTRAK KERJA, PENGADAAN, KONTAK BISNIS, DAN PAKTA INTEGRITAS

7.1 Pendahuluan

Dalam era digital yang semakin kompleks, profesional di bidang informatika tidak hanya dituntut untuk memahami aspek teknis dan rekayasa sistem, tetapi juga aspek hukum, etika, dan sosial yang menyertai praktik bisnis teknologi. Etika profesi informatika berperan sebagai pedoman moral yang menuntun perilaku profesional agar tetap selaras dengan prinsip keadilan, kejujuran, transparansi, serta tanggung jawab sosial terhadap masyarakat dan organisasi.

Penerapan etika dalam konteks bisnis informatika bukanlah hal yang bersifat tambahan atau simbolik, melainkan fondasi moral dari kepercayaan publik terhadap profesi TI. Ketika seorang profesional mendirikan usaha, menandatangani kontrak, melakukan pengadaan, atau menjalin kontak bisnis, setiap tindakan tersebut menjadi refleksi dari integritas profesi. Oleh karena itu, pembahasan dalam bab ini tidak hanya menyoroti prosedur administratif dan legal, tetapi juga mengurai aspek etika dan nilai-nilai kemanusiaan yang melekat pada setiap prosesnya.

7.2 Prosedur Pendirian Bisnis di Bidang Informatika

7.2.1 Makna dan Tujuan Pendirian Bisnis

Mendirikan bisnis di bidang informatika bukan sekadar membangun badan hukum atau mengembangkan produk teknologi; lebih dari itu, ia merupakan proses membangun kepercayaan dan legitimasi profesional di hadapan publik. Bisnis yang dibangun oleh seorang profesional TI idealnya merepresentasikan nilai-nilai etika seperti tanggung jawab sosial, akuntabilitas, dan transparansi.

Tujuan pendirian bisnis di bidang ini antara lain:

1. Memberikan layanan TI yang berorientasi pada solusi dan nilai kemanusiaan.
2. Menjamin bahwa aktivitas bisnis sejalan dengan hukum dan norma profesi.
3. Mengembangkan ekosistem teknologi yang berkelanjutan dan bebas dari praktik manipulatif.

7.2.2 Tahapan Pendirian Bisnis

Prosedur pendirian bisnis TI di Indonesia umumnya mencakup beberapa tahapan formal dan substantif:

1. **Perencanaan Konseptual dan Studi Kelayakan**
   Sebelum mengajukan izin, seorang pendiri harus memahami potensi pasar, kebutuhan sosial, serta risiko etis yang mungkin muncul. Misalnya, bisnis pengumpulan data pelanggan harus memastikan adanya perlindungan privasi sesuai prinsip *data minimization* (GDPR, 2018).
2. **Pemilihan Bentuk Badan Usaha.**
   Pilihan bentuk hukum — seperti PT, CV, atau koperasi TI — menentukan tanggung jawab dan mekanisme pengawasan etika. PT biasanya lebih disarankan untuk perusahaan

teknologi karena mengandung prinsip pemisahan tanggung jawab pribadi dan organisasi.

3. **Pendaftaran Legal dan Administratif.**
   Termasuk pengurusan akta pendirian, pengesahan Kemenkumham, Nomor Induk Berusaha (NIB), NPWP, hingga perizinan OSS. Proses ini memastikan bahwa entitas TI tersebut tunduk pada hukum dan peraturan nasional.
4. **Penetapan Tata Kelola dan Etika Internal.**
   Di sinilah **etika profesi** menjadi landasan manajerial. Perusahaan TI harus menyusun *Code of Conduct* yang mencakup prinsip integritas data, non-discrimination, dan penggunaan teknologi untuk tujuan yang sah.

7.2.3 Integritas dalam Proses Pendirian

Integritas dalam mendirikan bisnis TI tercermin dari cara profesional mematuhi hukum, tidak menyalahgunakan data publik, dan menghindari *unethical startup practices* seperti *data scraping* tanpa izin. Sebagaimana dikemukakan oleh Spinello (2021), "technological entrepreneurship without ethics is merely algorithmic opportunism." Dengan demikian, keberhasilan bisnis tidak hanya diukur dari laba, tetapi dari sejauh mana organisasi tersebut berkontribusi terhadap tatanan sosial yang adil.

7.3 Kontrak Kerja dan Hubungan Profesional dalam Informatika

7.3.1 Definisi dan Prinsip Dasar

Kontrak kerja merupakan instrumen legal yang mendefinisikan hubungan antara pihak pemberi kerja (*employer*) dan pekerja (*employee*) berdasarkan prinsip keadilan dan kesetaraan. Dalam dunia informatika, kontrak kerja memiliki kompleksitas tambahan, seperti perlindungan

kekayaan intelektual, kerahasiaan algoritma, dan pengelolaan hak cipta perangkat lunak.

Prinsip dasar kontrak kerja meliputi:

1. Keseimbangan hak dan kewajiban.
2. Kejujuran dalam kesepakatan.
3. Transparansi terhadap klausul risiko dan tanggung jawab.
4. Perlindungan terhadap data dan hasil kerja karyawan

7.3.2 Jenis-Jenis Kontrak dalam Dunia TI

1. **Perjanjian Kerja Waktu Tertentu (PKWT)**
   Biasanya digunakan untuk proyek jangka pendek seperti pengembangan aplikasi atau konsultasi sistem. Etika profesi mengharuskan pemberi kerja memberikan kompensasi sesuai beban kerja dan hasil proyek.
2. **Perjanjian Kerja Waktu Tidak Tertentu (PKWTT)**
   Diperuntukkan bagi posisi permanen seperti *software engineer*, *network administrator*, atau *data analyst*. Perusahaan wajib menyediakan lingkungan kerja yang aman secara psikologis dan digital.
3. **Kontrak Outsourcing atau Freelance**
   Dalam praktik outsourcing TI, etika menuntut adanya kejelasan kepemilikan hasil kerja, batas waktu, serta pengakuan kontribusi. Banyak pelanggaran etika terjadi karena pemanfaatan tenaga kerja tanpa penghargaan atas hak kekayaan intelektualnya.

7.3.3 Etika dalam Penyusunan dan Pelaksanaan Kontrak

Etika kontrak menuntut keterbukaan dalam negosiasi, tidak adanya penipuan (*fraudulent misrepresentation*), serta adanya penghormatan terhadap hak-hak pekerja. Dalam setiap hubungan kerja, profesional TI dituntut memegang teguh prinsip *fidelity* (kesetiaan terhadap komitmen profesional), sebagaimana diatur dalam *ACM Code of Ethics (2020)*

7.4 Prosedur dan Etika Pengadaan Barang dan Jasa TI

7.4.1 Konsep Dasar Pengadaan

Pengadaan (*procurement)* merupakan aktivitas penting dalam ekosistem teknologi — mulai dari pembelian perangkat keras, perangkat lunak, hingga layanan konsultasi dan pengembangan sistem. Setiap tahapan pengadaan harus didasari prinsip *value for money*, akuntabilitas, dan integritas.

7.4.2 Prinsip Etika dalam Pengadaan

1. **Transparansi.**
   Semua proses tender harus terbuka, dengan dokumentasi yang dapat diaudit publik.
2. **Keadilan.**
   Penyedia barang/jasa tidak boleh diistimewakan berdasarkan hubungan personal atau politik.
3. **Akuntabilitas.**
   Setiap keputusan pembelian atau pemilihan vendor harus dapat dijelaskan secara rasional dan terdokumentasi.
4. **Integritas Profesional.**
   Tidak menerima gratifikasi, suap, atau imbalan dalam bentuk apa pun.

Pelanggaran prinsip di atas bukan hanya kesalahan administratif, tetapi juga pelanggaran etika profesi, karena dapat merusak kepercayaan publik terhadap profesi TI.

7.4.3 Peran Teknologi dalam Etika Pengadaan

Ironisnya, banyak penyimpangan etika justru terjadi melalui teknologi: manipulasi data tender, rekayasa dokumen elektronik, atau pemanfaatan sistem pengadaan digital untuk kepentingan kelompok tertentu. Karena itu, profesional

informatika memiliki tanggung jawab moral untuk mengembangkan sistem e-procurement yang etis, transparan, dan anti-manipulasi.

7.5 Kontak Bisnis dan Jaringan Profesional

7.5.1 Definisi dan Peran Strategis

Kontak bisnis adalah individu, lembaga, atau mitra kerja yang menjalin hubungan profesional untuk mendukung aktivitas bisnis. Dalam dunia informatika, jaringan ini meliputi vendor, klien, regulator, hingga komunitas open-source.

Kontak bisnis bukan sekadar *networking*, melainkan mekanisme moral interaksi profesional. Sebagaimana dinyatakan oleh Floridi (2013), "*every digital contact is an ethical contact — a potential act of moral consequence*."

7.5.2 Etika dalam Hubungan Bisnis

Etika profesional dalam kontak bisnis mencakup:

1. Menjaga kerahasiaan informasi mitra kerja.
2. Menghindari praktik kolusi atau insider information.
3. Menjalin komunikasi berbasis kejujuran dan tanggung jawab sosial.

Hubungan bisnis yang etis menciptakan reputasi yang kuat — aset tak ternilai bagi perusahaan teknologi di era keterbukaan informasi.

7.6 Pakta Integritas: Pilar Kejujuran dalam Dunia Informatika

7.6.1 Definisi dan Tujuan

Pakta Integritas adalah pernyataan moral dan legal yang menegaskan komitmen individu maupun organisasi untuk menjunjung tinggi nilai-nilai anti korupsi, transparansi, dan

akuntabilitas dalam setiap proses bisnis. Di sektor TI, pakta ini menjadi penting karena proyek pengadaan teknologi sering kali bernilai besar dan rawan intervensi kepentingan.

7.6.2 Definisi dan Tujuan

Implementasi pakta integritas mencakup:

1. Penandatanganan dokumen komitmen etika oleh semua pihak yang terlibat.
2. Penunjukan lembaga independen untuk memantau kepatuhan.
3. Pelaporan pelanggaran melalui mekanisme *whistleblowing*.

Namun demikian, tantangan muncul ketika pakta hanya dijadikan formalitas administratif tanpa penginternalisasian nilai. Di sinilah peran profesional TI dibutuhkan — bukan hanya sebagai pelaksana sistem, tetapi juga penjaga moralitas digital (*digital integrity guardian*).

7.7 Refleksi Etika Profesi dalam Praktik Bisnis Informatika

Dalam konteks globalisasi dan otomatisasi, etika profesi informatika harus menjadi penyeimbang antara ambisi ekonomi dan tanggung jawab sosial. Seorang profesional TI tidak cukup sekadar patuh hukum; ia harus berpikir etis sebelum berpikir efisien.

Etika dalam pendirian bisnis, kontrak kerja, dan pengadaan menunjukkan satu benang merah: bahwa keberlanjutan bisnis bergantung pada integritas moral para pelakunya. Perusahaan TI yang etis tidak hanya bertahan karena produknya unggul, tetapi karena ia dipercaya oleh manusia yang menggunakannya.

7.8 Refleksi Kritis dan Keterbatasan

Bab ini menegaskan bahwa dalam profesi informatika, keberhasilan tidak ditentukan semata oleh kemampuan teknis atau strategi bisnis, melainkan oleh integrasi etika dalam seluruh dimensi profesionalitas.

Mulai dari tahap pendirian bisnis, penyusunan kontrak, proses pengadaan, hingga penandatanganan pakta integritas — semua merupakan arena penerapan nilai moral yang mengukuhkan martabat profesi.

Dengan demikian, seorang profesional informatika sejati adalah mereka yang mampu menggabungkan kecerdasan logika dan kejujuran hati, menjadikan etika bukan sekadar kewajiban, tetapi identitas profesional yang membedakan antara teknisi dan manusia berintegritas.

DAFTAR PUSTAKA

ACM Code of Ethics. (2020). *Association for Computing Machinery.* https://ethics.acm.org

Floridi, L. (2013). *The Ethics of Information.* Oxford University Press.

Spinello, R. (2021). *Cyberethics: Morality and Law in Cyberspace.* Jones & Bartlett Learning.

Transparency International. (2024). *Integrity Pacts for Technology Procurement.* https://www.transparency.org

Procurement Tactics. (2024). *Procurement Ethics and Integrity Principles.* https://procurementtactics.com

SpringerLink. (2025). *Business Ethics in Digital Contexts.* https://link.springer.com

Republik Indonesia. (2023). *Peraturan Pemerintah No. 5 Tahun 2021 tentang OSS dan Perizinan Usaha.*

IEEE Global Initiative. (2023). *Ethically Aligned Design v2.* IEEE Standards Association.

UN Global Compact. (2024). *Principles for Ethical ICT Entrepreneurship*

BAB 8
JENIS-JENIS PROFESI DI BIDANG IT

8.1 Pendahuluan

Teknologi Informasi (IT) telah berevolusi dari sekadar alat bantu operasional menjadi faktor strategis yang menentukan daya saing organisasi. Saat ini, hampir seluruh aktivitas organisasi—mulai dari layanan pelanggan, manajemen rantai pasok, pendidikan, kesehatan, hingga industri—bergantung pada sistem digital yang terintegrasi. Konsekuensi logis dari kondisi tersebut adalah meningkatnya kebutuhan akan profesional IT dalam berbagai spesialisasi dengan tingkat kompetensi yang semakin tinggi.

Transformasi digital tidak hanya menuntut organisasi untuk mengadopsi teknologi baru, tetapi juga mengubah cara organisasi bekerja, menyusun kebijakan, membentuk proses bisnis, dan memanfaatkan data. Transformasi ini menuntut kapabilitas SDM yang tidak lagi berfokus pada keterampilan teknis semata, melainkan kemampuan adaptasi, kolaborasi lintas fungsi, dan pemahaman implikasi sosial teknologi. Studi yang memetakan keterampilan transformasi digital menegaskan bahwa kompetensi SDM digital berkorelasi dengan keberhasilan implementasi transformasi digital dan kualitas kebijakan pendukungnya (Defining Digital Excellence: Requisite Skills and Policy Implications for Digital Transformation, 2022).

Di tengah kebutuhan tersebut, profesi IT berkembang cepat dan melahirkan banyak jabatan baru seperti DevOps engineer, AI/ML engineer, data engineer, *dan cloud architect*. Namun, pertumbuhan profesi ini juga memunculkan tantangan besar: **kesenjangan keterampilan (*skills gap*)**. Banyak organisasi mengeluhkan bahwa lulusan atau tenaga kerja tersedia belum selaras dengan kompetensi yang dibutuhkan industri. Studi longitudinal tentang keterampilan IT/IS yang dicari industri menunjukkan bahwa kebutuhan employer berubah, tetapi beberapa keterampilan inti seperti pemrograman, database, networking, keamanan, dan problem solving tetap stabil sebagai tuntutan dasar (Cummings & Janicki, 2020).

Dengan demikian, pembahasan profesi IT tidak bisa dipisahkan dari standar profesional dan standar kompetensi. Standar ini diperlukan agar profesi IT memiliki pijakan: (1) kualitas kerja dapat diukur, (2) akuntabilitas terhadap publik dapat dijamin, dan (3) pengembangan karier dan pendidikan dapat diarahkan. Pada tingkat global, standar profesi banyak mengacu pada ACM dan IEEE. Pada tingkat nasional Indonesia, standar kompetensi kerja mengacu pada SKKNI dan sertifikasi kompetensi melalui BNSP dan LSP.

8.2 Jenis Jenis Profesi di Bidang IT

8.2.1 Rasional Klasifikasi Profesi IT

Profesi IT mencakup spektrum tugas yang luas. Agar pembahasan sistematis, profesi IT dapat diklasifikasikan berdasarkan fungsi utama: pembangunan aplikasi, pengelolaan data, keamanan, infrastruktur dan jaringan, manajemen layanan IT, serta teknologi baru (*emerging technologies*). Klasifikasi semacam ini juga membantu organisasi dalam pemetaan

kebutuhan SDM, membantu pendidikan dalam merancang kurikulum, dan membantu individu dalam memilih jalur karier.

Dalam transformasi digital, tuntutan organisasi meluas karena sistem digital semakin terintegrasi dan semakin kritis. Akibatnya, profesi IT berkembang menjadi struktur yang mirip ekosistem, bukan lagi "satu divisi IT" yang menangani semuanya. Kebutuhan akan keterampilan digital yang makin kompleks menegaskan urgensi pembentukan profesi dan kompetensi yang spesifik (Defining Digital Excellence: Requisite Skills and Policy Implications for Digital Transformation, 2022).

8.2.2 *Domain Software Development dan Engineering*

Profesi *software development* adalah fondasi utama IT karena produk digital diwujudkan melalui software. Perubahan penting yang terjadi dalam dekade terakhir adalah meningkatnya standar kualitas proses *software engineering*. Software kini tidak hanya harus "jalan", tetapi juga harus aman, *scalable, maintainable,* dan *reliable.*

Smuts dan Smuts (2022) menyatakan bahwa era Society 5.0 menuntut software engineer menguasai keterampilan teknis sekaligus keterampilan masa depan seperti adaptive learning, kolaborasi, dan kemampuan mengelola kompleksitas. Software engineer bukan lagi pekerja individual yang menulis kode, melainkan bagian dari sistem kerja tim yang menggabungkan metode agile, version control, code review, dan pipeline rilis.

Profesi yang termasuk dalam domain ini mencakup:

1. Software Developer/Software Engineer
2. Front-End Developer
3. Back-End Developer
4. Full Stack Developer
5. Mobile App Developer

6. Software Architect

Software architect mendapat posisi penting karena sistem modern membutuhkan rancangan arsitektur yang mempertimbangkan integrasi layanan, skalabilitas, dan keamanan. Pada konteks *cloud-based system*, peran ini bahkan bersinggungan langsung *dengan cloud architect* dan *security architect* (Demchenko et al., 2019).

8.2.3 Domain DevOps dan Cloud Engineering

DevOps muncul sebagai respons terhadap kebutuhan mempercepat *delivery software* dan memperkuat reliability sistem. Dalam DevOps, batas antara *developer* dan *operations* diperkecil melalui otomasi, pipeline CI/CD, serta monitoring *real-time*. Demchenko et al. (2019) menekankan bahwa DevOps dan *cloud-based software engineering* merupakan kompetensi penting yang perlu dimasukkan ke kurikulum universitas karena industri telah mengadopsinya secara luas.

Hamza et al. (2025) memperkuat temuan tersebut dengan studi penerapan integrasi DevOps pada mata kuliah software engineering. Hasilnya menunjukkan DevOps meningkatkan keterkaitan teori dan praktik industri serta relevan dalam menutup gap pembelajaran.

Profesi utama pada domain ini:

1. DevOps Engineer
2. *Site Reliability Engineer* (SRE)
3. *Cloud Engineer*
4. *Cloud Architect*

Khedkar (2024) menyajikan jalur karier *cloud* yang menekankan kompetensi *platform, security*, dan arsitektur. Profesi cloud engineer dan cloud architect berkembang pesat

karena sebagian besar organisasi bermigrasi ke *cloud,* baik *public cloud* maupun hybrid.

8.2.4 Domain Data dan Analytics

Data dan analitik merupakan pilar besar transformasi digital. Hampir semua organisasi kini berupaya mengadopsi keputusan berbasis data, sehingga memunculkan profesi data science dan analitik.

Cao (2019) menyatakan data science telah berkembang menjadi profesi dengan kebutuhan pendidikan dan standardisasi yang jelas. Data science bukan hanya aktivitas teknis, tetapi profesi yang memerlukan kompetensi terstruktur, termasuk domain knowledge, komunikasi, dan etika penggunaan data.

Fayyad dan Hamutcu (2020) mengusulkan knowledge framework untuk data science dan analytics sebagai dasar pengembangan standar profesional. Davenport (2020) juga menekankan pentingnya klasifikasi dan sertifikasi business data scientist agar organisasi dapat membedakan peran, kompetensi, dan jalur karier.

Profesi utama:

1. Data Scientist
2. Data Analyst
3. Data Engineer
4. *Business Intelligence Analyst*
5. *Business Data Scientist*

Koshta dan Pandey (2024) menunjukkan jalur karier data science berkembang dan memerlukan pemetaan kompetensi yang sistematis agar individu dapat meningkatkan kompetensi sesuai tahapannya.

8.2.5 *Domain Artificial Intelligence* (AI)

AI dan *machine learning* (ML) mengalami pertumbuhan kebutuhan tenaga kerja yang cepat. Verma et al. (2021) menganalisis iklan lowongan kerja AI/ML dan menemukan pola kebutuhan skill yang menekankan kombinasi kemampuan statistik, pemrograman, dan penerapan machine learning pada konteks industri.

Stojanovic et al. (2023) menekankan perusahaan mencari kompetensi applied AI, yaitu kemampuan menerapkan AI pada kebutuhan nyata, termasuk integrasi sistem dan penyelesaian masalah riil. Patel (2024) membahas kerangka transisi karier ke AI software engineering, menandakan meningkatnya kebutuhan AI talent lintas sektor.

Singh (2025) menyoroti bahwa AI turut mengubah struktur pekerjaan ML engineer, termasuk otomatisasi beberapa aktivitas dan munculnya tuntutan skill baru.

Profesi utama AI:

1. AI/ML Specialist
2. Machine Learning Engineer
3. Applied AI Engineer
4. AI Software Engineer

8.2.6 *Domain Cybersecurity*

Cybersecurity adalah domain yang paling kritis karena keamanan sistem menjadi syarat dasar dari keberlangsungan layanan digital. Furnell (2021) menegaskan bahwa kebutuhan tenaga kerja keamanan siber meningkat, namun terdapat kekurangan tenaga ahli dan gap kompetensi. Furnell et al. (2020) menyatakan bahwa pengembangan *skill cybersecurity* harus dipahami sebagai spektrum yang luas, bukan silo terpisah.

Goupil et al. (2022) menunjukkan adanya skill gap yang nyata dan perlunya pemahaman menyeluruh terhadap kompetensi yang dibutuhkan industri. Untuk memperkuat struktur pendidikan dan profesi, Shoemaker et al. (2020) menyusun body of knowledge cybersecurity sebagai rujukan ACM/IEEE/AIS/IFIP.

Sertifikasi memegang peran penting dalam penguatan *workforce cybersecurity* (Certifications in Cybersecurity Workforce Development, 2022).

Profesi utama *cybersecurity:*

1. Information Security Analyst
2. Security Engineer
3. SOC Analyst
4. Penetration Tester/Ethical Hacker
5. Security Architect

Nkongolo et al. (2024) menunjukkan bahwa profesi keamanan informasi memiliki kebutuhan kompetensi yang kompleks, termasuk kombinasi skill teknis dan governance.

82.7 *Domain Network* dan *Infrastructure*

Networking dan infrastruktur merupakan tulang punggung konektivitas layanan digital. Hanson et al. (2020) menunjukkan *competency-based assessment* dapat digunakan untuk menilai skill dalam kelas *network security*. Pada era cloud, networking berkembang menjadi cloud network engineering.

Panduan *cloud network engineer* (Ipsale & Gilioli, n.d.) menegaskan bahwa cloud network engineer harus mampu mendesain, mengimplementasikan, mengelola, serta mengamankan arsitektur jaringan pada platform cloud.

Profesi:

1. Network Engineer

2. Network Administrator
3. Systems Administrator
4. Cloud Network Engineer

8.2.8 Domain IT Support dan IT Management

Tidak semua organisasi membutuhkan AI engineer, tetapi hampir semua organisasi membutuhkan dukungan operasional IT. Domain IT support dan IT management berperan memastikan sistem berjalan, pengguna terlayani, dan risiko IT terkelola. Kebutuhan ini berkorelasi dengan transformasi digital yang menekankan kesiapan organisasi dan kemampuan mengelola perubahan (Defining Digital Excellence: Requisite Skills and Policy Implications for Digital Transformation, 2022).

Profesi:

1. IT Support Specialist / Help Desk
2. IT Manager
3. IT Service Management Staff

8.2.5 Domain IT *Project Management*

Manajemen proyek IT adalah fungsi penting untuk memastikan implementasi teknologi tidak gagal. Akkermans et al. (2020) menekankan bahwa karier project manager terbentuk melalui integrasi antara ilmu karier dan praktik manajemen proyek. Project manager tidak hanya mengelola deliverables, tetapi juga membentuk jalur profesional dan kompetensi kepemimpinan.

Profesi:

1. IT Project Manager
2. *Digital Transformation Project Manager*

8.2.5 *Domain Research Software Engineering* (RSE)

RSE menjadi profesi yang makin penting dalam ekosistem riset. Goth et al. (2025) memetakan kompetensi RSE yang meliputi kemampuan engineering, reproducibility, dokumentasi, testing, dan tanggung jawab profesional untuk menjaga kualitas software riset.

Profesi:

- Research Software Engineer

8.3 Deskripsi Kerja Profesi IT

8.3.1 Prinsip Umum Deskripsi Kerja

Deskripsi kerja adalah instrumen penting yang menghubungkan organisasi dengan profesional IT. Secara umum, job description profesi IT terdiri dari:

1. Tujuan peran,
2. Tanggung jawab utama,
3. Kompetensi teknis inti,
4. Kompetensi pendukung (soft skills),
5. Indikator performa (kpi/okr).

Cummings dan Janicki (2020) menunjukkan bahwa employer secara konsisten mencari kombinasi skill teknis dan skill pendukung, termasuk komunikasi dan problem solving. Ini berarti job description IT yang baik harus mencerminkan kebutuhan real, bukan sekadar daftar teknologi.

8.3.2 Deskripsi Kerja *Software Developer / Software Engineer*

Tujuan Peran

Mengembangkan aplikasi atau sistem perangkat lunak yang mendukung proses bisnis dan layanan organisasi.

Tanggung Jawab Utama

1. Menganalisis kebutuhan pengguna dan spesifikasi sistem.
2. Mengembangkan software menggunakan prinsip SDLC.
3. Menulis kode yang maintainable dan dapat diuji.
4. Melakukan debugging dan memperbaiki defect.
5. Berpartisipasi dalam code review.
6. Menyusun dokumentasi teknis.
7. Berkolaborasi dengan QA, DevOps, dan manajemen produk.

Kompetensi Inti

1. Pemrograman dan software engineering practices
2. Kolaborasi tim agile
3. Kemampuan adaptasi teknologi
   (Smuts & Smuts, 2022)

8.3.3 Deskripsi Kerja DevOps Engineer

Tujuan Peran

Mengintegrasikan development dan operations agar delivery software cepat, stabil, dan dapat diandalkan.

Tanggung Jawab Utama

1. Merancang pipeline CI/CD.
2. Mengotomasi deployment dan provisioning infrastruktur.
3. Monitoring performa dan reliability sistem.
4. Menangani incident response terkait availability sistem.
5. Mengelola container dan konfigurasi environment.

Kompetensi Inti

1. Cloud dan otomasi
2. IaC dan CI/CD
3. *Observability* dan *reliability practices*
   (Demchenko et al., 2019; Hamza et al., 2025)

8.3.4 Deskripsi Kerja *Cloud Engineer / Cloud Architect*

Tujuan Peran

Merancang dan mengelola layanan cloud agar aman, efisien, dan scalable.

Tanggung Jawab Utama

1. Menyusun arsitektur cloud berdasarkan kebutuhan organisasi.
2. Implementasi compute, storage, networking.
3. Mengelola keamanan cloud (IAM, policy).
4. Optimasi biaya dan performa.
5. Migrasi aplikasi dari on-premise ke cloud.

Kompetensi Inti

1. *Platform cloud* dan arsitektur
2. *Security* dan *governance cloud*

(Khedkar, n.d.; Demchenko et al., 2019)

8.3.5 Deskripsi Kerja Data Scientist

Tujuan Peran

Menghasilkan insight dan model prediktif berbasis data untuk mendukung keputusan.

Tanggung Jawab Utama

1. Mengumpulkan dan membersihkan data.
2. EDA dan analisis statistik.
3. Mengembangkan model machine learning.
4. Evaluasi performa model.
5. Menyampaikan insight ke stakeholder.

Kompetensi Inti

1. Standardisasi kompetensi profesi data science
2. Framework knowledge profesional

(Cao, 2019; Fayyad & Hamutcu, 2020; Davenport, 2020)

8.3.6 Deskripsi Kerja Machine Learning / AI Engineer

Tujuan Peran

Menerapkan AI dalam sistem produksi dan meningkatkan performa model secara berkelanjutan.

Tanggung Jawab Utama

1. Implementasi model ML pada pipeline aplikasi.
2. Feature engineering dan tuning model.
3. Deployment model dan monitoring drift.
4. Integrasi model ke layanan dan aplikasi.
5. Memastikan model dapat digunakan pada skala produksi.

Kompetensi Inti

1. Kebutuhan skill AI/ML industri meningkat dan terukur
2. Applied AI competence
   (Verma et al., 2021; Stojanovic et al., 2023; Patel, 2024)

8.3.7 Deskripsi Kerja Cybersecurity Analyst

Tujuan Peran

Mengurangi risiko serangan siber dan menjaga keamanan layanan digital.

Tanggung Jawab Utama

1. Monitoring log dan aktivitas jaringan.
2. Deteksi ancaman dan incident response.
3. Vulnerability assessment.
4. Pembuatan laporan keamanan dan rekomendasi perbaikan.
5. Security awareness internal.

Kompetensi Inti

1. *Cybersecurity skill gap* dan kebutuhan spektrum skill
2. Rujukan *body of knowledge cybersecurity* (Furnell, 2021; Furnell et al., 2020; Goupil et al., 2022; Shoemaker et al., 2020)

8.3.8 Deskripsi Kerja *Network Engineer / Cloud Network Engineer*

Tujuan Peran

Menjamin konektivitas jaringan dan keamanan arsitektur komunikasi data.

Tanggung Jawab Utama

1. Mendesain topologi jaringan dan kebijakan keamanan.
2. Konfigurasi *routing/switching*.
3. Monitoring dan *troubleshooting*.
4. Dokumentasi jaringan.
5. Pada cloud: desain *network architecture cloud* dan *security*.

Kompetensi Inti

1. *Competency-based assessment* untuk network security
2. Kebutuhan desain dan keamanan arsitektur jaringan cloud (Hanson et al., 2020; Ipsale & Gilioli, n.d.)

8.3.9 Deskripsi Kerja IT Project Manager

Tujuan Peran

Memastikan proyek IT selesai sesuai scope, waktu, biaya, kualitas, dan risiko.

Tanggung Jawab Utama

1. Menyusun perencanaan proyek, WBS, timeline.
2. Mengelola tim dan komunikasi stakeholder.
3. Mengendalikan scope, biaya, dan jadwal.

4. Mengelola risiko dan issue.
5. Menyusun laporan progres.

Kompetensi Inti

1. Kepemimpinan, komunikasi, manajemen risiko
2. Pembentukan karier PM dan praktik profesional (Akkermans et al., 2020)

8.3.10 Deskripsi Kerja Research Software Engineer

Tujuan Peran

Mengembangkan software riset yang maintainable, reproducible, dan berkualitas engineering tinggi.

Tanggung Jawab Utama

1. Membuat software pendukung eksperimen/riset.
2. Testing, dokumentasi, dan version control.
3. Kolaborasi dengan peneliti lintas disiplin.
4. Menjamin *reproducibility* dan *maintainability*.

Kompetensi Inti

1. Kompetensi dan tanggung jawab RSE (Goth et al., 2025)

8.4 Standar Profesi IT Menurut ACM dan IEEE

8.4.1 Mengapa Standar Profesi Diperlukan?

Standar profesi memastikan bahwa profesional IT tidak bekerja secara sembarangan dan tidak semata mengejar delivery cepat dengan mengorbankan keamanan dan dampak sosial. Dalam sistem digital modern, software dan AI dapat berdampak luas—bahkan menjadi bagian dari infrastruktur publik. Karena itu, etika profesi bukan pelengkap, melainkan kewajiban.

8.4.2 ACM *Code of Ethics and Professional Conduct*

ACM *Code of Ethics* merupakan rujukan etika paling kuat untuk profesi computing. Kode ini menekankan bahwa profesional harus mengutamakan kesejahteraan publik, menghindari bahaya, jujur, adil, menghormati privasi, dan menjaga kerahasiaan (ACM, 2018). Prinsip ini relevan bagi seluruh profesi IT karena semua sistem digital memiliki risiko sosial: kebocoran data, bias algoritma, kerusakan layanan publik, dan lain-lain.

Kode etik ACM mencakup dua lapisan utama:

1. *General Ethical Principles* (prinsip moral umum), dan
2. *Professional Responsibilities* (tanggung jawab kerja profesional).

Misalnya, ACM menuntut profesional computing untuk:

1. Menjaga kualitas tinggi pada proses dan produk,
2. Memelihara kompetensi profesional,
3. Melakukan evaluasi menyeluruh terhadap dampak sistem,
4. Membangun sistem yang robust dan secure
   (ACM, 2018).

Dalam era cloud dan AI, tuntutan "*robustly and usably secure*" sangat penting karena sistem modern makin kompleks dan sering digunakan masyarakat luas.

8.4.3 ACM Curricula Recommendations dan Standar Kompetensi Pendidikan

ACM juga menghasilkan rekomendasi kurikulum computing untuk standardisasi pembentukan SDM profesional (ACM, n.d.). Ini penting karena profesi IT bergantung pada rantai pasok kompetensi dari pendidikan formal maupun pelatihan profesi.

Dalam *cybersecurity, body of knowledge* menjadi rujukan penyusunan kurikulum yang lengkap dan konsisten (Shoemaker et al., 2020). Ini membantu menjawab masalah skill gap yang ditemukan pada industri.

8.4.4 IEEE dalam Standar Profesi IT

IEEE secara historis kuat dalam membangun standar engineering yang menjaga kualitas sistem teknologi. Dalam profesi IT, kontribusi IEEE terutama pada:

1. Standardisasi proses engineering,
2. Standardisasi testing/verification,
3. Penguatan profesionalisme engineering.

Catatan akademik (penting untuk buku kamu): daftar referensi yang kamu batasi tidak memasukkan dokumen IEEE *Code of Ethics* sebagai sumber formal. Jadi pembahasan etika profesi global secara eksplisit lebih dominan merujuk ke ACM *Code of Ethics* (ACM, 2018), sedangkan posisi IEEE dijelaskan sebagai standar *engineering* dan kompetensi global computing bersama ACM (ACM, n.d.; Shoemaker et al., 2020).

8.5 Standar Profesi IT di Indonesia

8.5.1 Kerangka Nasional: SKKNI

Standar profesi IT di Indonesia bertumpu pada standar kompetensi kerja nasional. SKKNI adalah rumusan unit kompetensi yang menjadi dasar pendidikan vokasional, pelatihan kerja, dan uji sertifikasi kompetensi (Kementerian Ketenagakerjaan Republik Indonesia, n.d.). Sistem ini membuat kompetensi profesi dapat diukur melalui unit-unit kerja yang spesifik dan dapat diuji.

Dalam konteks IT, SKKNI dapat digunakan untuk menyusun:

1. Standar pelatihan tenaga IT
2. Standar uji kompetensi sertifikasi
3. Acuan rekrutmen berbasis kompetensi

8.5.2 Sistem Sertifikasi Nasional: BNSP dan LSP

Untuk memastikan kompetensi yang distandarkan dapat diakui secara formal, Indonesia menerapkan mekanisme sertifikasi kompetensi.

BNSP berfungsi sebagai lembaga nasional yang memberikan lisensi kepada LSP untuk melaksanakan sertifikasi kompetensi (Badan Nasional Sertifikasi Profesi [BNSP], n.d.). LSP menjadi pelaksana uji kompetensi, sedangkan sertifikat menjadi bukti seseorang kompeten sesuai skema.

LSP Informatika tercatat pada BNSP sebagai salah satu penyelenggara sertifikasi bidang informatika (Badan Nasional Sertifikasi Profesi [BNSP], n.d.). Selain itu, LSP berbasis institusi pendidikan juga berkontribusi memperluas sertifikasi kompetensi IT, misalnya LSP Institut Teknologi Nasional Yogyakarta (LSP Institut Teknologi Nasional Yogyakarta, n.d.).

8.5.3 Standar Profesi dan Daya Saing Industri

Standar kompetensi profesi IT juga terkait dengan agenda peningkatan daya saing industri nasional. SIDIA sebagai sistem informasi daya saing industri merupakan salah satu indikator dan rujukan untuk mendukung penguatan daya saing industri (Kementerian Perindustrian Republik Indonesia, n.d.). Penguatan SDM IT yang tersertifikasi dapat menjadi instrumen untuk meningkatkan daya saing organisasi, khususnya pada sektor industri yang semakin terdigitalisasi.

8.6 Penutup

Profesi IT berkembang cepat karena transformasi digital memperluas kebutuhan organisasi pada cloud, AI, data, dan keamanan siber. Perkembangan ini menuntut klasifikasi profesi yang jelas, deskripsi kerja yang terukur, dan standar profesional yang kuat. Literatur menunjukkan adanya skill gap di banyak domain, terutama cybersecurity dan AI, sehingga pendidikan, pelatihan, dan sertifikasi perlu diperkuat secara serius (Furnell, 2021; Goupil et al., 2022; Verma et al., 2021).

Pada tingkat global, ACM menyediakan pijakan etik dan rekomendasi kurikulum computing sebagai standar pembentukan profesional IT (ACM, 2018; ACM, n.d.). Dalam *cybersecurity*, rujukan *body of knowledge* menjadi kerangka penting bagi pendidikan dan pengembangan kompetensi (Shoemaker et al., 2020). Pada tingkat nasional, Indonesia membangun standar profesi melalui SKKNI dan mengimplementasikannya melalui sertifikasi kompetensi berbasis BNSP dan LSP (Kementerian Ketenagakerjaan Republik Indonesia, n.d.; Badan Nasional Sertifikasi Profesi [BNSP], n.d.).

Dengan integrasi standar global dan sistem kompetensi nasional, profesional IT Indonesia memiliki peluang memperkuat daya saing dan kredibilitas kompetensi di pasar kerja

DAFTAR PUSTAKA

ACM. (2018). *ACM Code of Ethics and Professional Conduct*. https://www.acm.org/code-of-ethics

ACM. (n.d.). *Curricula Recommendations*. https://www.acm.org/education/curricula-recommendations

Akkermans, J., Keegan, A., Huemann, M., & Ringhofer, C. (2020). Crafting project managers' careers: Integrating the fields of careers and project management. *Project Management Journal, 51*(2), 135–153. https://doi.org/10.1177/8756972819877782

Badan Nasional Sertifikasi Profesi (BNSP). (n.d.). *LSP Informatika*. https://bnsp.go.id/lsp/informatika

Cao, L. (2019). Data science: Profession and education. *IEEE Intelligent Systems, 34*(5), 35–44. https://doi.org/10.1109/MIS.2019.2936705

Certifications in Cybersecurity Workforce Development. (2022). In *Cybersecurity workforce development*. https://doi.org/10.4018/978-1-6684-3554-0.ch006

Cummings, T., & Janicki, T. (2020). What skills do students need? A multi-year study of IT/IS knowledge and skills in demand by employers. *The Journal of Information and Systems in Education, 19*(1), 1–12.

Davenport, T. H. (2020). Beyond unicorns: Educating, classifying, and certifying business data scientists. *Harvard Data Science Review, 2*(2). https://doi.org/10.1162/99608F92.55546B4A

Defining Digital Excellence: Requisite Skills and Policy Implications for Digital Transformation. (2022). *IEEE Access, 10*, 39895–39915. https://doi.org/10.1109/access.2022.3171924

Demchenko, Y., Gruengard, E., & Klous, S. (2019). Teaching DevOps and cloud based software engineering in university curricula. In *2019 15th International Conference on eScience (eScience)* (pp. 548–552). IEEE. https://doi.org/10.1109/ESCIENCE.2019.00075

Fayyad, U., & Hamutcu, H. (2020). Toward foundations for data science and analytics: A knowledge framework for professional standards. *Harvard Data Science Review, 2*(2). https://doi.org/10.1162/99608F92.1A99E67A

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security, 100*, 102080. https://doi.org/10.1016/J.COSE.2020.102080

Furnell, S., Fischer, P., & Finch, A. (2020). Addressing cyber security skills: The spectrum, not the silo. *Computer Fraud & Security, 2020*(2), 6–11. [https://doi.org/10.1016/S1361-3723(20)30017-8](https://doi.org/10.1016/S1361-3723%2820%2930017-8)

Goth, G., Katz, D. S., Chue Hong, N., Hettrick, S., Jay, C., Lamprecht, A. L., … & Struck, A. (2025). Foundational competencies and responsibilities of a research software engineer: Current state and suggestions for future directions. *F1000Research, 14*, 1. https://doi.org/10.12688/f1000research.157778.2

Goupil, L., Palisse, A., & Lanet, J. L. (2022). Towards understanding the skill gap in cybersecurity. In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (pp. 1–10). https://doi.org/10.1145/3538969.3544421

Hamza, M. F., Yusuf, R. O., & Adebiyi, M. O. (2025). Integrating DevOps knowledge using a university-based software engineering course in Nigerian universities. In *2025 International Conference on Information Systems Engineering and Computing* (pp. 1–6). IEEE. https://doi.org/10.1109/isec64801.2025.11147360

Hanson, C., Taylor, B., & Kaza, S. (2020). The use of competency-based statements in assessing student knowledge, skills, and abilities: A study in a network security class. *Information Systems Education Journal, 18*(4), 4–13. https://doi.org/10.62273/cogs3790

Ipsale, A., & Gilioli, A. (n.d.). *Google Cloud Certified Professional Cloud Network Engineer Guide: Design, implement, manage, and secure a network architecture in Google Cloud*.

Kementerian Ketenagakerjaan Republik Indonesia. (n.d.). *SKKNI: Standar Kompetensi Kerja Nasional Indonesia*.

https://skkni.kemnaker.go.id/

Kementerian Perindustrian Republik Indonesia. (n.d.). *SIDIA: Sistem Informasi Daya Saing Industri dan Produk*. https://sidia.kemenperin.go.id/

Khedkar, S. (n.d.). *Navigating the cloud computing career path: A comprehensive guide*.

Koshta, N., & Pandey, S. (2024). Career path for data science professional and data scientist. *NBER Working Paper Series*, 1–8. https://doi.org/10.58532/nbennurch291

Nkongolo, M., Mennega, S., & van Zyl, J. (2024). Requirements for a career in information security: A comprehensive review. In *Algorithms for Intelligent Systems* (pp. 123–145). Springer. https://doi.org/10.1007/978-981-99-7962-2_7

Patel, R. (2024). Navigating the AI frontier: A comprehensive framework for career transition into AI software engineering. *International Journal for Science Technology and Engineering, 12*(8), 1–15. https://doi.org/10.22214/ijraset.2024.64188

Shoemaker, D., Kohnke, A., & Sigler, K. (2020). *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP recommendations for a complete curriculum in cybersecurity*. CRC Press. https://doi.org/10.1201/9781003022596

Singh, A. (2025). The impact of AI on the job market of machine learning engineers. *Indian Scientific Journal of Research in Engineering and Management, 9*(1), 1–8. https://doi.org/10.55041/ijsrem50434

Smuts, H., & Smuts, M. (2022). Society 5.0 and the future of work skills for software engineers and developers. *EasyChair Preprint*, 1–12. https://doi.org/10.29007/9kzd

Stojanovic, L., Dinic, M., & Stojanovic, N. (2023). Employer requirements for graduate competencies in applied artificial intelligence. In *2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1–6). IEEE. https://doi.org/10.1109/telsiks57806.2023.10315726

Verma, A., Yurov, K. M., Lane, P. L., & Yurova, Y. V. (2021). An investigation of skill requirements in artificial intelligence and machine learning job advertisements. *Industry and Higher Education, 35*(4), 469–483. https://doi.org/10.1177/0950422221990990

LSP Institut Teknologi Nasional Yogyakarta. (n.d.). https://lsp.itny.ac.id/

BIODATA PENULIS

Deyidi Mokoginta, S.T., M.Si.

Deyidi Mokoginta lahir di Kotamobagu pada tanggal 19 September 1981. Pendidikannya dimulai dari Sekolah Dasar di SD Inpers 6 Bilalang hingga tahun 1993, kemudian melanjutkan pendidikan menengahnya di SMP Negeri Bilalang (kini SMP Negeri 7 Kotamobagu) hingga tahun 1996. Setelah itu, ia menyelesaikan pendidikan menengah atasnya di SMK 23 Maret Kotamobagu pada tahun 1999.

Gelar sarjananya dalam bidang Teknik Elektro diperoleh dari Fakultas Teknik Universitas Teknologi Sulawesi Utara pada tahun 2011. Tak berhenti di situ, Deyidi kemudian melanjutkan pendidikan pascasarjananya di Jurusan Program studi Pengelolaan Sumberdaya Pembangunan (PSP), Program Pasca Sarjana Universitas Sam Ratulangi, dan berhasil meraih gelar S2 pada tahun 2016.

Riwayat pekerjaan Deyidi sangatlah beragam. Selain menjadi anggota Polri yang berdinas di Polda Sulawesi Utara, ia juga terlibat dalam dunia akademis sebagai pengajar beberapa mata kuliah di Program Studi Teknik Elektro Universitas Teknologi Sulawesi Utara. Selain itu, ia juga dikenal sebagai pendiri sekaligus Ketua Ikatan Alumni Universitas

Teknologi Sulawesi Utara sejak tahun 2012 hingga saat ini, di kampus Universitas Teknologi Sulawesi Utara, dia juga banyak aktif dalam berbagai kegiatan kemahasiswaan karena Ia merupakan dosen pembina Badan Eksekutif Masahasiswa di kampus tersebut.

Melalui pengalaman dan dedikasinya dalam berbagai bidang tersebut, Deyidi Mokoginta telah menjadi sosok yang memiliki kontribusi yang berarti dalam pengembangan pendidikan dan pelayanan masyarakat di Sulawesi Utara, serta memberikan inspirasi bagi generasi muda untuk berprestasi dan berkontribusi dalam memajukan bangsa dan negara.

BIODATA PENULIS

Edy Prayitno, S.Kom., S.E., M.Eng
Fakultas Teknologi Informasi Universitas Teknologi Digital Indonesia

Selain mengajar, penulis aktif meneliti dan menulis pada bidang data mining, AI, dan e-commerce. Penulis memiliki latar belakang pendidikan S1 Teknik Informatika (STMIK AKAKOM Yogyakarta), S1 Akuntansi (STIE Widya Wiwaha Yogyakarta), dan S2 Teknik Elektro dan Teknologi Informasi (Universitas Gadjah Mada). Sebagai seorang akademisi, penulis telah menghasilkan sejumlah artikel ilmiah yang diterbitkan di jurnal nasional dan internasional. Buku ini merupakan bagian dari upayanya untuk membagikan pengetahuan dan pemikirannya kepada khalayak yang lebih luas dalam tema Etika Profesi Informatika. Penulis dapat dihubungi melalui edyprayitno@utdi.ac.

BIODATA PENULIS

Jama Toyo, M.Kom
Dosen Program Studi Teknologi Informasi
Institut Teknologi dan Bisnis Muhammadiyah Wakatobi

Penulis lahir di Desa Laimu Kabupaten Maluku Tengah tanggal 17 Maret 1985. Penulis adalah dosen tetap pada Program Studi Teknologi Informasi pada Institut Teknologi dan Bisnis Muhammadiyah Wakatobi. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Sistem Informasi. Penulis baru menekuni di bidang menulis dan Alhamdulillah ini adalah tulisan yang ke 5 (Lima) saya selama mengikuti kolaborasi. Semoga Kita tetap istiqamah dalam menulis dan semoga bermanfaat bagi yang membacanya.

BIODATA PENULIS

Rizal Lamusu, S.Kom, M.T
Dosen Program Studi Ilmu Komputer
Fakultas Sains dan Ilmu Komputer
Universitas Muhammadiyah Gorontalo

Penulis lahir di Gorontalo tanggal 29 April 1981. Penulis adalah dosen tetap pada Program Studi Ilmu Komputer Fakultas Sains Dan Ilmu Komputer, Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Program Studi teknik Elektro, Bidang Ilmu Teknik Informatika.
Penulis dapat dihubungi melalui e-mail : rizal_lamusu@umgo.ac.id

BIODATA PENULIS

Dr. Mohamad Ilyas Abas, S.SI, M.Kom
Dosen Program Studi Ilmu Komputer
Fakultas Sains dan Ilmu Komputer

Penulis lahir di Padang tanggal 26 Agustus 1991. Penulis adalah dosen tetap pada Program Studi Ilmu Komputer Fakultas Sains dan Ilmu Komputer Universitas Muhammadiyah Gorontalo. Menyelesaikan pendidikan S1 pada prodi Sistem Informasi dan melanjutkan S2 pada Prodi Teknik Informatika dan S3 Pada prodi Elektro Konsentrasi Informatika. Penulis menekuni bidang Data Mining, Computer Vision, AI dan juga informatika pada umumnya.

Penulis dapat dihubungi melalui e-mail: ilyasabas26@gmail.com

BIODATA PENULIS

Rafika Rahmawati, S.Kom., M.Kom., MBA
Dosen Program Studi Sistem Informasi
Fakultas Ilmu Komputer Universitas Pembangunan Nasional
"Veteran" jawa Timur

Dosen Program Studi Sistem Informasi Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jawa Timur dengan fokus keilmuan di Manajemen Sistem Informasi. Menyelesaikan pendidikan S1 pada Jurusan Sistem Informasi di Institut Teknologi Sepuluh Nopember (ITS) Surabaya. Melanjutkan studi S2 double degree di Sistem Informasi ITS dan Industrial Management di National Taiwan University of Science and Technology (NTUST). Penulis dapat dihubungi melalui profil profesional di Linkedin www.linkedin.com/in/rafikarahmawati12 atau melalui e-mail rafika.rahmawati.fasilkom@upnjatim.ac.id.

BIODATA PENULIS

Widya Eka Pranata, S.Si., M.Si
Dosen Program Studi Ilmu Komputer
Fakultas Sains dan Ilmu Komputer
Universitas Muhammadiyah Gorontalo

Penulis lahir di Gorontalo tanggal 26 November 1998. Penulis adalah dosen tetap pada Program Studi Sarjana Ilmu Komputer Fakultas Sains dan Ilmu Universitas Muhammadiyah Gorontalo. Menyelesaikan pendidikan S1 pada Program Studi Matematika di Universitas Negeri Gorontalo dan melanjutkan S2 pada Program Studi Sains Komputasi menekuni bidang analisis data dan pembelajaran mesin. Penulis dapat dihubungi melalui e-mail: widyapranata@umgo.ac.id

BIODATA PENULIS

Alimuddin Yasin S.Kom, M.Kom
Dosen Program Studi Bisnis Digital
Fakultas Sains dan Ilmu Komputer
Universitas Muhammadiyah Gorontalo

Penulis lahir di Gorontalo tanggal 24 Juli 1992. Penulis adalah dosen tetap pada Program Studi Bisnis Digital Fakultas Sains dan Ilmu Komputer, Universitas Muhammadiyah Gorontalo. pendidikan S1 Teknik Informatika STMIK AMIKOM Yogyakarta dan melanjutkan S2 Informatika STMIK AMIKOM Yogyakarta.

Penulis menekuni bidang jaringan komputer (*computer network*), sistem informasi, *Internet of Things* (IoT), administrasi sistem (*system administration*), serta *cloud computing*. Dalam aktivitas akademik, penulis aktif dalam pengajaran dan penelitian yang berorientasi pada penguatan kompetensi digital dan penerapan teknologi informasi untuk kebutuhan organisasi dan masyarakat. Rekam jejak publikasi ilmiah penulis dapat ditelusuri melalui profil Google Scholar. Penulis dapat dihubungi melalui e-mail: alimuddiny@gmail.com