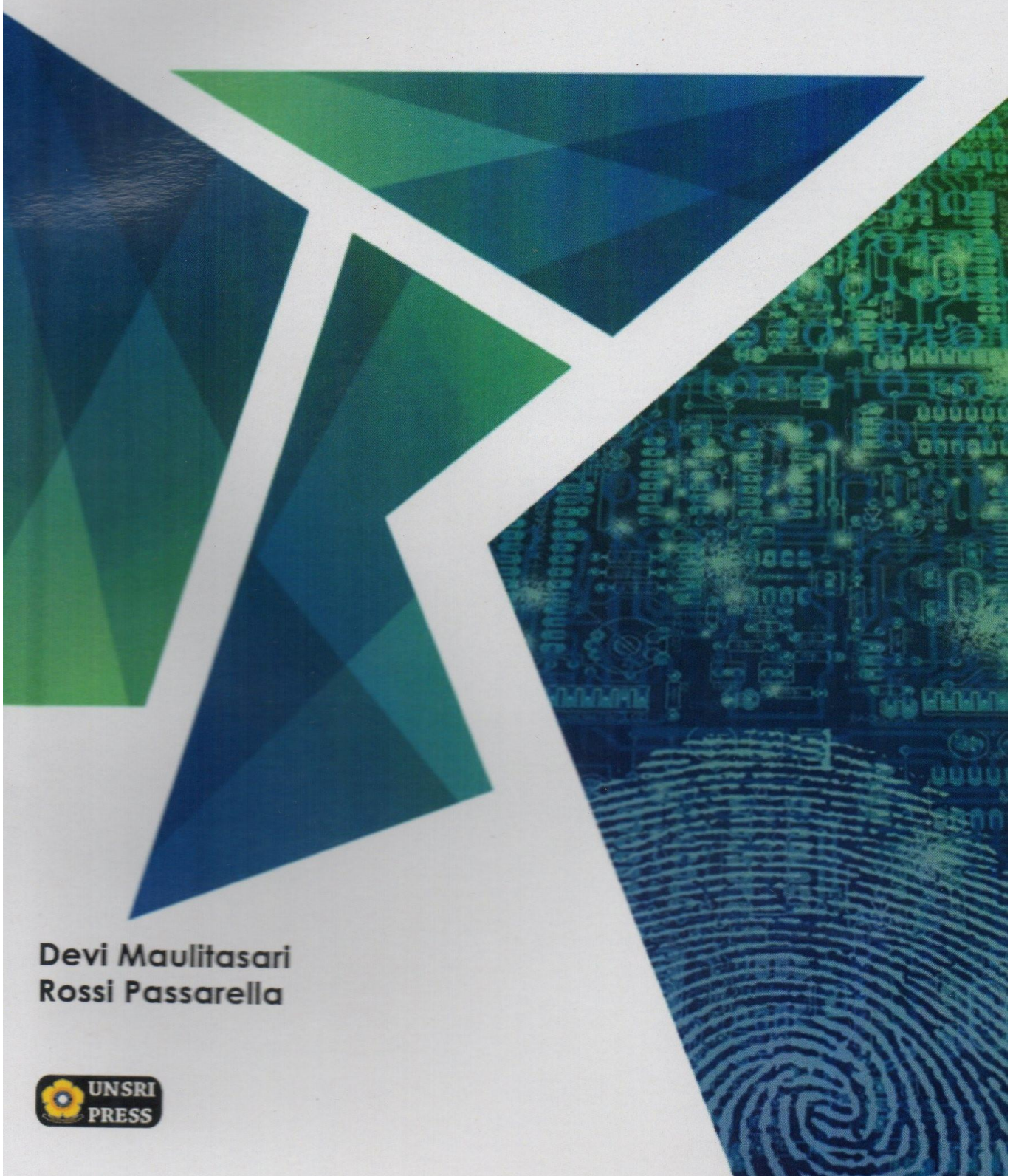
TEORI DAN SEJARAH
CITRA FORENSIK



Devi Maulitasari
Rossi Passarella

UNSRI PRESS

TEORI DAN SEJARAH

CITRA FORENSIK

Sanksi pelanggaran Pasal 72
Undang-undang Nomor 19 Tahun 2002
Tentang Perubahan atas Undang-undang Nomor 12 Tahun 1997
Pasal 44 Tentang Hak Cipta

1. Barang siapa dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 2 ayat (1) atau pasal 49 ayat (1) dan ayat (2) dipidana penjara masing-masing paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp. 1.000.000,00 (satu juta rupiah), atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah)

2. Barang siapa dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu ciptaan atau barang hasil pelanggaran hak cipta atau hak terkait, sebagaimana dimaksud ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau dendan paling banyak Rp.500.000.000,00 (lima ratus juta rupiah)

TEORI DAN SEJARAH CITRA FORENSIK

Disusun Oleh :

Devi Maulitasari, S.Kom

Rossi Passarella, M.Eng

Unsri Press

TEORI DAN SEJARAH CITRA FORENSIK

Oleh

Devi Maulitasari, S.Kom

Rossi Passarella, M.Eng

UPT. Penerbit dan Percetakan

Universitas Sriwijaya 2020

Kampus Unsri Palembang

Jalan Srijaya Negara, Bukit Besar Palembang 30139

Telp. 0711-360969

email : unsri.press@yahoo.com, penerbitunsri@gmail.com

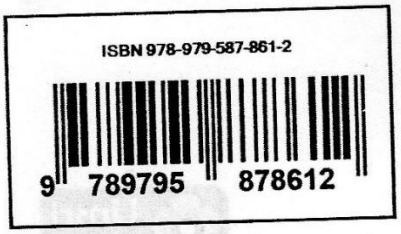
website : www.unsri.unsripress.ac.id

Anggota APPTI No. 026/KTA/APPTI/X/2015

Anggota IKAPI No. 001/SMS/2009

Cetakan Pertama, Maret 2020

94 halaman : 24 x 16 cm



UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER
Jalan Palembang – Prabumulih Km. 32 Inderalaya Ogan Ilir Kode Pos 30662
Telp. (0711)7072729, 379249, 581700 Faksimile. (0711) 379248, 581710
email : ilkom@unsri.ac.id

Sambutan Ketua Jurusan Sistem Komputer

Assalamualaikum Warrahmatullahi Wabarakatuh

Segala Puji bagi Allah SWT, atas berkat Rahmat dan Karunia-Nya kepada dosen sistem komputer yang telah berhasil menghasilkan buku Ajar berjudul Buku Teori dan Sejarah Citra Forensik ini disusun berdasarkan Rencana Pembelajaran Semester (RPS) mata kuliah Citra Forensik (FSK43816) kurikulum 2016. Kurikulum 2016 dirancang untuk memperkuat kompetensi mahasiswa dari sisi sikap dan tata nilai, kemampuan bidang ilmu pengetahuan, serta kemampuan bidang pekerjaan. Proses pencapaiannya melalui pembelajaran sejumlah mata pelajaran yang dirangkai sebagai suatu kesatuan yang saling mendukung pencapaian kompetensi tersebut.

Buku ini merupakan edisi pertama yang dikeluarkan oleh dosen sistem komputer untuk materi ajar mata kuliah Citra Forensik pada pertemuan ke-1 dan ke-2, dengan status ini sangat terbuka untuk terus dilakukan perbaikan dan penyempurnaan dimasa mendatang. Oleh karena itu, kami mengundang para pembaca memberikan kritik, saran dan masukan untuk perbaikan dan penyempurnaan pada edisi berikutnya.

Atas kontribusi tersebut, kami ucapkan terima kasih. Mudah-mudahan kita dapat memberikan yang terbaik bagi kemajuan dunia pendidikan sesuai dengan peta jalan Jurusan Sistem Komputer 2025.

Palembang, Januari 2020

An. Ketua Jurusan Sistem Komputer
Sekertaris Jurusan

Sutarno, M.T.
NIP.197811012010121003

KATA PENGANTAR

Puji syukur penulis ucapkan kepada Tuhan Yang Maha Esa atas rahmat-Nya yang telah tercurah, sehingga penulis bisa menyelesaikan Buku Teori dan Sejarah Citra Forensik. Adapun tujuan dari disusunnya buku ini adalah supaya para mahasiswa dapat mengetahui bagaimana sejarah dan perkembangan citra forensik.

Tersusunnya buku ini dibuat dari usaha tim penulis. Dukungan moral dan material dari berbagai pihak sangatlah membantu tersusunnya buku ini.

Untuk itu, penulis ucapkan terima kasih kepada sahabat, rekan-rekan, dan pihak-pihak lainnya yang membantu secara moral dan material bagi tersusunnya buku ini.

Buku yang tersusun sekian lama ini tentu masih jauh dari kata sempurna. Untuk itu, kritik dan saran yang membangun sangat diperlukan agar buku ini bisa lebih baik nantinya.

Palembang, Januari 2020

Tim Penulis

DAFTAR ISI

1. Sejarah Digital Forensik

1. Sejarah Digital Forensik

1.1 Pendahuluan

Perkembangan teknologi yang terus meningkat di bidang citra digital, membuat manusia harus mampu mengikuti kemajuan yang ada dalam memenuhi kebutuhan hidupnya. Hal ini juga memilki dampak terhadap kasus kejahatan digital yang ikut berkembang, salah satunya seperti kasus manipulasi data digital. Berdasarkan contoh kasus tersebut, perlu adanya teknik untuk memudahkan dalam memecahkan permasalahan yang ada, yaitu dengan digital forensik. Digital forensik adalah salah satu cabang dari ilmu forensik, sedangkan forensik itu sendiri adalah sebuah istilah yang digunakan dalam penyelidikan kejahatan dengan cara ilmiah agar barang bukti yang dikumpulkan dapat ditindaklanjuti menuju proses hukum. Digital forensik mampu memberikan keakuratan data dan dapat digunakan sebagai barang bukti yang mendukung terhadap penuntunan pada proses pengadilan.

Sejarah ilmu forensik ini diawali pada tahun 1247 M dengan munculnya buku ilmu forensik pertama di dunia, yaitu Xiyuan Jilu yang ditulis oleh Song Ci dari Dinasti Song Selatan. Buku tersebut berisi mengenai pengetahuan medis dalam memecahkan masalah kriminal [1]. Adapun landasan dari ilmu digital forensik ini adalah praktik pengumpulan, analisis, serta pelaporan data digital. Ilmu forensik bukan hanya berfokus pada kemampuan teknis, tetapi penguasaan ini juga berkaitan dengan bidang lain, misalnya bidang hukum. Terkait aspek teknis dari penyelidikan, ilmu forensik terbagi menjadi beberapa sub cabang tergantung dengan jenis perangkat digital yang digunakan, seperti forensik komputer, forensik jaringan, forensik peranti bergerak, forensik basis data, dan analisis data forensik. Berbagai hal tersebut akan melewati tahapan berupa penyitaan, forensik akuisisi, analisis media digital, dan

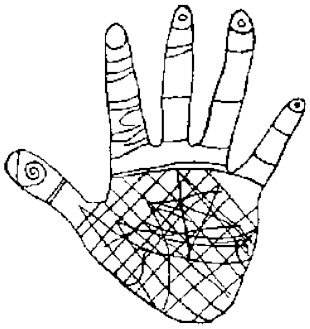
penyusunan laporan. Selain dapat mengidentifikasi bukti secara langsung, digital forensik dapat dijadikan sebagai penguatan pernyataan terkait hubungan antara tersangka dengan kasus yang dialami, mengidentifikasi sumber, serta mengotentikasi dokumen-dokumen, dimana otentikasi ini merupakan suatu proses dalam membuktikan atau menunjukkan sesuatu yang benar atau asli.

1.2 Forensik pada Zaman Pra-sejarah

Sejak zaman pra-sejarah, teknik forensik sudah mulai digunakan dan dikenal sebagai teknik sederhana yang dapat memacu munculnya ilmu-ilmu forensik modern. Perkembangan teknik forensik bermula sekitar abad 700 SM yang ditandai dengan adanya penemuan oleh manusia zaman pra-sejarah berupa bukti sidik jari pada sebuah lukisan serta pahatan batu mady [2] [3] yang dapat dilihat pada gambar 1.1 sebagai berikut:

Gambar 1.1 Bukti Fingerprint Pertama [2] [3]

Bukti tersebut berasal dari proses menekan *handprint* ke tanah liat dan batu, sehingga didapatkan *fingerprint* pertama pada masa itu. Para arkeolog di Kanada yang dikenal sebagai Nova Scotia menjelaskan bahwa bukti *fingerprint* tersebut dapat digambarkan dengan pola *ridge* rinci sidik jari dan tangan yang dapat dilihat pada gambar 1.2 sebagai berikut:



Gambar 1.2 Cetakan Tangan dengan Pola Ridge [2] [3]

Selain itu, pada zaman pra-sejarah terdapat penemuan akumulasi babel kuno dengan isi berupa sidik jari hasil cetakan dari tanah liat sebagai alat transaksi bisnis serta identifikasi [4]. Seperti pada abad 7 SM, Solemn yang merupakan seorang pedagang yang berasal dari Arab telah membuat jejak sidik jari sebagai tagihan hutang. Pada saati tu, sidik jari tersebut telah terdokumentasi sebagai alat bukti hukum yang valid dalam proses transaksi hutang-piutang. Adapun hal lain yang terkait dengan sidik jari, yaitu pada pengenalan sidik jari yang dilakukan oleh orang-orang cina dengan menempelkannya pada patung tanah liat yang bertujuan agar tidak terjadi kesalahpahaman akan identitas seseorang untuk berbisnis dengan bukti dokumen yang jelas atau sah. Kemudian pada abad 44 SM, teknik forensik pertama kali dilakukan oleh seorang dokter Romawi yang bernama Antistius terhadap jasad Kaisar Julius dengan teknik forensik otopsi. Hasil otopsi tersebut mengungkapkan bahwa pada jasad Kaisar Julius terdapat 23 luka tusukan dan 1 dari 23 tusukan tersebut merupakan tusukan yang mengakibatkan tewasnya Kaisar Julius. Contoh lain dari teknik forensik ini terjadi pada tahun 287-212 SM, yaitu Archimedes mampu memberikan keterangan mengenai mahkota emas yang terungkap palsu (tidak terbuat dari emas) melalui proses analisa kepadatan dan ketangguhan. Dilanjutkan pada tahun 250 SM, Erasistratus yang

merupakan dokter Yunani Kuno, pertama kali menemukan prinsip-prinsip tes deteksi kebohongan dengan parameter denyut nadi seseorang [5]. Dari hal tersebut, berkembang alat yang dikenal sebagai alat deteksi kebohongan berdasarkan perubahan denyut nadi, GSR, tekanan darah, dan perubahan besar atau mendadak dalam sistem saraf simpatik [4]. Alat tersebut dapat digunakan ketika investigator melakukan investigasi terhadap tersangka yang tidak bersedia mengakui kesalahannya. Kemudian pada tahun 221-206 SM, terdapat catatan Cina dari Dinasti Qin yang mencakup rincian mengenai penggunaan cetakan tangan pada tanah liat dengan pola *ridge* sebagai bukti dalam penyelidikan pencurian [6] yang dapat dilihat pada gambar 1.3 sebagai berikut:

Gambar 1.3 Cetakan Tangan pada Dinasti Qin [3] [6]

1.3 Forensik pada Zaman Sejarah

Pada zaman sejarah, teknik forensik mulai berkembang sejak tahun 1000 M melalui seorang pengacara di pengadilan Romawi, yaitu Quitilan. Quitilan berhasil melakukan identifikasi sidik jari walaupun dalam kondisi berlumuran darah. Hal tersebut telah berhasil mengungkapkan fakta mengenai kasus orang buta yang telah terperangkap atas pembunuhan ibunya sendiri. Terkait kasus kejahatan yang perlu mengidentifikasi orang yang meninggal, pada tahun 1284 M, Cina mengembangkan dokumentasi

pertama yang tertulis dalam buku Hsi Duan Yun dengan judul *The Washing Away of Wrong* sekaligus dianggap sebagai buku yang mampu menjadi bukti pertama dalam memecahkan kasus kejahatan secara ilmu medis [5]. Selain berisi tentang pengetahuan medis, buku tersebut juga menjelasakan mengenai kemungkinan orang yang meninggal secara alami, tenggelam, atau bahkan dicekik. Berawal dari hal tersebut, ilmu Patology forensik mulai berkembang dan digunakan hingga saat ini. Selain itu, pada tahun 1235 M, dilakukan observasi pada Dinasty Yuan oleh orang Cina Mandarin, yaitu Sung T'zu melalui serangga (lalat). Observasi ini dikenal sebagai kisah sabit berdarah dikarenakan pernah terjadi pembunuhan menggunakan sabit. Dari hal tersebut lahir ilmu entomologi forensik [7]. Entomologi forensik adalah cabang entomologi yang mempelajari peran serangga dalam bidang forensik untuk kepentingan kejahatan terutama yang berkaitan dengan kasus kematian. Dilanjutkan pada tahun 1247-1318 M, Khajeh Rashiduddin Fazlollah Hamdani yang merupakan dokter Iran sekaligus sejarawan, penulis sarjana, dan polisi patriot, memberi tanggapan tentang identifikasi seseorang melalui sidik jari, yaitu pengalaman menunjukkan bahwa tidak ada dua individu memiliki jari persis sama. Khajeh juga pernah menjabat sebagai Menteri sejak tahun 1298 M dan sejarawan Morris Rossabi mencatat bahwa Khajeh merupakan tokoh terkemuka di Iran pada abad ke-14 [8].

Adapun contoh lain terkait forensik pada zaman sejarah adalah kasus pembunuhan yang terjadi pada tahun 1447 M. Masalah tersebut terungkap saat dilakukan identifikasi melalui petunjuk berupa gigi yang hilang dan luka yang ada pada korban. Dengan adanya penemuan tersebut, lahir sebuah ilmu odontology forensik [4]. Odontologi forensik merupakan salah satu metode identifikasi tubuh seseorang yang tidak dapat dikenal,

misalnya korban kebakaran ataupun kecelakaan dan tidak terdapat identitas yang ditemukan di tempat kejadian persitiwa. Maka dari itu, ilmu ini mempelajari tentang identifikasi korban dengan barang bukti berupa gigi. Dilanjutkan pada tahun 1509-1590 M, seorang ahli bedah yang berasal dari Perancis bernama Ambroise Pare berhasil menemukan alat bukti teks pertama yang dipergunakan dalam laporan di pengadilan dengan tujuan sebagai bukti pendukung yang dapat menambah yakin pihak hakim dalam mengambil keputusan. Sehingga pada tahun 1600 M, penemuan ilmu ini semakin berkembang dan dikenal sebagai forensik dokumen atau biasa disebut *Forensic Graphology*. Adapun tokoh bernama Ambroise Pare yang dimaksud dapat dilihat pada gambar 1.4 sebagai berikut:

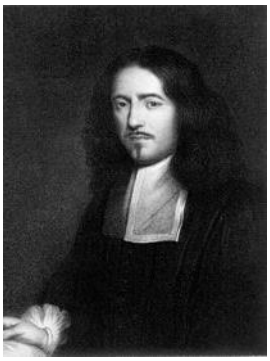
Gambar 1.4 Ambroise Pare [9]

Lalu pada tahun 1601 M, terbit karya pertama dari seorang bernama Francois Damelle yang berasal dari Perancis. Karya tersebut merupakan tulisan pertama yang menjadikan suatu pemerikasaan dokumen secara sistematis. Walaupun dokumen tersebut ditulis sebelum berkembangnya tinta dan kertas, tetapi pengenalan mengenai tulisan tangan yang berbeda dalam hal ini juga dapat teridentifikasi.

Selain itu, pada tahun 1605-1682 M, seorang dokter, ahli biologi, filsuf, dan sejarawan asal Inggris yang bernama Sir Thomas Browne menemukan sistem Adipocere. Adipocere adalah suatu keadaan tubuh mayat yang mengalami hidrolisis dan hidrogenisasi terhadap jaringan lemak yang terdapat pada bukunya yang berjudul "Hydrio Thapia, Urne-Burial" [10]. Adapun tokoh bernama Sir Thomas Browne yang dimaksud dapat dilihat pada gambar 1.5 sebagai berikut:

Gambar 1.5 Sir Thomas Browne [11]

Lalu pada tahun 1686, seorang Profesor yang berasal dari *University of Bologna* Anatomi bernama Marcello Malpighi, meneliti lebih detail mengenai dokumentasi karakteristik yang berbeda dari sidik jari, seperti pola alur berputar-putar, pola *ridge*, *loop*, dan *spiral*. Pada setiap individu, pola-pola tersebut jelas berbeda dan dapat digunakan dalam melakukan identifikasi pelaku kejahatan melalui sidik jari. Adapun tokoh bernama Marcello Malpighi yang dimaksud dapat dilihat pada gambar 1.6 sebagai berikut:



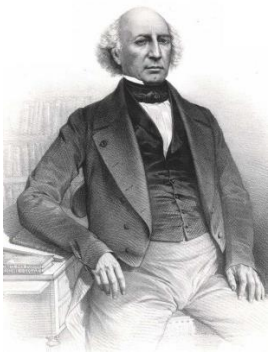
Gambar 1.6 Marcello Malpighi [12]

Kemudian pada tahun 1755 M, terdapat penemuan berupa Arsenious Oxide yang dapat berubah menjadi Asam Arsenious saat bereaksi dengan Seng dan menghasilkan Arsine. Penemuan tersebut merupakan hasil pemikiran dari Karl Willhelm Sceele yang memiliki andil sangat besar dalam forensik arsenik. Adapun tokoh bernama Karl Willhelm Sceele yang dimaksud dapat dilihat pada gambar 1.7 sebagai berikut:

Gambar 1.7 Karl Willhelm Sceele [13]

Dilanjutkan dengan suatu kasus pembunuhan yang terbongkar akibat penemuan sobekan kertas yang tersimpan pada saku serta ditemukannya sebuah pistol yang menjadi alat untuk membunuh. Berdasarkan penyelidikan dengan barang bukti tersebut, John Toms dari Lancaster

Inggris dihukum. Kemudian pada tahun 1813 M, Mathieu Joseph Bonaventure Orfila yang dikenal sebagai bapak Toksikologi modern atau profesor obat kimia dan forensik di *University of Paris* memberikan kontribusi yang signifikan dan membantu pengembangan tes deteksi darah. Mathieu juga mendapatkan penghargaan sebagai orang pertama yang melakukan identifikasi sampel darah dan noda air mani menggunakan mikroskop. Adapun tokoh bernama Mathieu Joseph Bonaventure Orfila yang dimaksud dapat dilihat pada gambar 1.8 sebagai berikut:

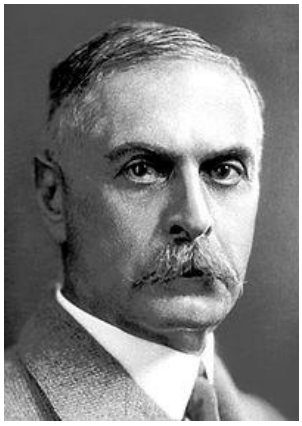


Gambar 1.8 Mathieu Joseph Bonaventure Orfila [14]

Dilanjutkan dengan Henry Goddard yang merupakan salah satu dari *Scotland Yard's* yang dapat mengungkapkan kasus pembunuhan berdasarkan perbandingan peluru. Perbandingannya didasarkan pada cacat yang ada pada peluru dan dilakukan penelusuran kembali ke tempat pembuatannya. Hal tersebut terjadi pada tahun 1835 M dan merupakan langkah awal dari forensik balistik, dimana balistik merupakan ilmu yang mempelajari gerakan, sifat, serta efek dari peluru, bom grafitasi, roket, dan lain-lain. Adapun tokoh bernama Henry Goddard yang dimaksud dapat dilihat pada gambar 1.9 sebagai berikut:

Gambar 1.9 Henry Goddard [15]

Forensik pada zaman sejarah juga berhasil mendapatkan hadiah nobel atas penemuan golongan darah manusia. Penemuan ini sangat menarik dan berguna karena dapat dijadikan sebagai barang bukti yang kuat dalam membantu penyidik dalam mengungkapkan identitas seseorang. Berdasarkan penemuan tersebut, Karl Landsteiner dianugerahi hadiah nobel pada tahun 1901 M. Adapun tokoh bernama Karl Landsteiner yang dimaksud dapat dilihat pada gambar 1.10 sebagai berikut:



Gambar 1.10 Karl Landsteiner [16]

Setelah penemuan golongan darah berkembang, sistem identifikasi kriminal dan juga tes tembak residu, seperti difenilamin juga berkembang

pesat, sehingga pada pertengahan tahun 1950 M, Max Frei Sulzer menunjukkan tanda-tanda detail dengan menemukan metode *lifting tape* untuk mengumpulkan jejak bukti. Kemudian saat itu juga mulai berkembang teknik forensik lain seperti Gas Chromatography. Dilanjutkan dengan metode berbasis gel untuk menguji enzim dalam noda darah kering serta cairan tubuh lainnya yang terjadi pada tahun 1960 M oleh Brian penemuan lain yang melibatkan penggunaan elektron penyebaran teknologi sinar-X dengan teknik yang dikembangkan di *Aerospace Corporation,* pada tahun 1974 M yang dikenal sebagai *Scanning Electron Microscopy*.

Seiring berkembangnya forensik pada zaman sejarah, badan investigasi utama dari Departemen Keadilan Amerika Serikat, yaitu FBI, pada tahun 1977 M memperkenalkan AFIS yang merupakan sidik jari komputerisasi pertama serta pada tahun 1984 M, FBI membuat program media magnetik yang dikenal dengan CART. CART adalah sebuah agensi yang menyediakan layanan digital forensik untuk investigasi agensi, investigasi mitra lokal, negara bagian hingga federal. Setelah itu, Sir Alec Jeffreys yang merupakan seorang peneliti di *Lister Institutte, Leicester University*, menemukan sebuah metode dalam melakukan identifikasi individu dari DNA. DNA adalah asam nukleat yang menyimpan berbagai informasi mengenai genetika. Dari DNA, dapat ditentukan berbagai hal seperti jenis rambut, warna kulit, dan sifat-sifat khusus dari manusia. Berkaitan dengan identifikasi individu melalui DNA, hal tersebut adalah penemuan yang revolusioner serta terbesar pada ilmu forensik pada tahun 1984 M. Hingga pada akhirnya di tahun 1986 M, DNA digunakan untuk pertama kalinya dalam memecahkan kasus pembunuhan sebagai identifikasi Colin Pichfork yang melakukan pembunuhan terhadap dua gadis muda di Inggris.

Dilanjutkan pada tahun 1987 M, perusahaan forensik *cyber* dibentuk (*Access Data*) dan resmi pula dibentuk IOCE pada tahun 1995 M, yang merupakan suatu organisasi yang menangani barang bukti komputer dan hal lain yang berkaitan dengan komputer [18]. Sehingga pada tahun 1990 M, bidang komputer forensik terus berkembang pesat, sehingga semua aparat hukum diberikan bekal berupa pelatihan pada bidang *cybercrime* dan teknik investigasi *internet*. Kemudian pada tahun 1976 M, US Federal Rules of Evidence menyatakan bahwa, hukum lain yang berhubungan dengan kejahatan komputer [19] dapat dibagi sebagai berikut:

a. *Economic Espionage Act* 1996 M, yaitu berhubungan dengan rahasia dagang.
b. *The Electronic Communication Privacy Act* 1986 M, yaitu berhubungan dengan penyadapan terhadap alat elektronik.
c. *The Computer Security* Act 1987 M, yaitu berhubungan dengan keamanan sistem komputer pemerintahan.

Berdasarkan hal tersebut, dapat diketahui bahwa kejahatan komputer dapat dilakukan kapanpun dan dimanapun, baik jarak terdekat atau terjauh. Hal ini dikarenakan kejahatan komputer tidak memiliki jejak geografis. Contohnya adalah kejahatan komputer antara negara pelaku dan negara korban yang berbeda negara. Kasus tersebut sangat mungkin terjadi karena dengan adanya jangkauan *internet* yang makin menyebar keseluruh pelosok dunia. Namun dengan adanya teknik forensik, kejahatan tersebut perlahan dapat terungkap dengan mengetahui siapa pelakunya, darimana asalnya, dan bagaimana teknik yang dipakai dalam merencanakan kejahatan tersebut dengan peran komputer forensik yang mampu memberikan bukti dan membawa kasus tersebut ke ranah hukum.

2. Perkembangan Digital Forensik

2. Perkembangan Digital Forensik

2.1 Kebutuhan Forensik

Perkembangan forensik berlangsung sekitar tahun 1980-1990 M yang menyebabkan butuhnya lembaga-lembaga penegak hukum membentuk tim forensik khusus dalam melakukan penyelidikan. Namun sebelum daripada itu, terdapat kejahatan komputer pertama kali yang diakui dalam Pidana Komputer Florida pada tahun 1978, serta UU yang melarang penghapusan data ataupun modifikasi dari sistem komputer [6]. Selanjutnya, ruang lingkup *cybercrime* semakin berkembang, hingga beberapa UU kemudian disahkan agar dapat menemukan solusi dari permasalahan dalam hal hak cipta, privasi, serta pornografi anak. Adapun negara pertama yang mengeluarkan UU mengenai kejahatan komputer adalah Kanada, yaitu pada tahun 1983 [7]. Kemudian hal tersebut diikuti oleh beberapa negara, seperti Amerika Serikat dengan *Computer Fraud and Abuse Act* pada tahun 1986, negara Australia dengan amandemen UU kriminalnya pada tahun 1989, dan negara Inggris dengan menerbitkan *Computer Misuse Act* pada tahun 1990 [8].

Dengan berbagai kebutuhan forensik yang ada, maka dibentuk lembaga khusus, seperti Tim Analisis dan Tanggapan Komputer dan Departemen Kejahatan Komputer yang didirikan oleh kelompok Anti Penipuan Polisi Metropolitan Inggris. Adapun anggota dari lembaga yang didirikan tersebut merupakan personel penegak hukum profesional dan penggemar atau penggiat komputer yang bertanggungjawab akan penelitian dan petunjuk awal serta langkah atau perkembangan dalam bidang forensik digital [17]. Seperti salah satu contoh kasus publik yang terjadi pada penerapan digital forensik yang pertama adalah kasus pengejaran peretas Markus Hess anpada tahun 1986 oleh Clifford Stoll yang melakukan penyelidikan menggunakan teknik forensik komputer

dan jaringan [18]. Kemudian disepanjang tahun 1990 M, permintaan untuk membentuk tim yang mengelola sumber daya penyelidikan semakin meningkat, seperti dibentuknya National Hi-Tech Crime pada tahun 2001 di Inggris dengan tujuan dapat menjadi penyedia infrastruktur nasional terhadap kejahatan komputer dengan tim yang ada di pusat kota London serta pasukan polisi daerah yang masuk ke dalam SOCA pada tahun 2006 [19]. Dengan begitu, ilmu forensik digital terus berkembang mulai dari sarana dan teknik-teknik *ad-hoc* yang dibuat oleh para penggiat dalam bidang forensik. Sehingga pada tahun 1992, istilah forensik komputer mulai digunakan pada literatur akademik walaupun sebelumnya sudah digunakan tetapi tidak secara formal. Ilmu forensik ini juga akan dimasukkan dalam disiplin baru ke dunia *sains forensic* oleh Collier dan Spaul [20]. Namun dengan perkembangan yang begitu cepat, hal ini mengakibatkan kurangnya standarisasi dan pelatihan-pelatihan. Hal tersebut terdapat pada buku K. Rosenblatt pada tahun 1985 yang berisi bahwa menyita, mengamankan, serta melakukan analisis bukti yang tersimpan dalam komputer merupakan tantangan forensik paling besar yang dihadapi oleh penegak hukum pada tahun 1990 M. Saat sebagian besar pengujian forensik dilakukan, seperti pengujian pada sidik jari dan DNA yang dilakukan oleh para ahli yang dilatih secara khusus, terdapat pula pekerjaan untuk mengumpulkan dan menganlisis bukti komputer yang ditugaskan pada petugas patroli serta detektif [21].

2.2 Perkembangan Standar Forensik

Sejak tahun 2000 M, perkembangan standar forensik mulai menjadi kebutuhan standarisasi dengan berbagai lembaga yang telah menerbitkan pedoman mengenai forensik digital. Kelompok Kerja Ilmiah yang membahas mengenai bukti digital telah menerbitkan makalah pada tahun

2002 dengan judul *Best Practices for Computer Forensics*. Kemudian pada tahun 2004 mulai berlaku sebuah perjanjian internasional Eropa, yaitu Konvensi mengenai Kejahatan Dunia Maya dengan tujuan melakukan rekonsiliasi UU kejahatan komputer nasional, teknik investigasi, serta hubungan kerjasama internasional. Perjanjian tersebut telah ditandatangani oleh 43 negara, seperti Afrika Selatan, Inggris, Amerika Serikat, Kanada, Jepang, serta negara-negara Eropa lainnya. Selang waktu satu tahun dari perjanjian tersebut, muncul publikasi standar ISO 17025 [22] yang merupakan standar utama pada persyaratan kompetensi laboratorium pengujian dan kalibrasi. Ruang lingkup standar ini meliputi metode baku, metode uji, serta metode yang dikembangkan oleh laboratorium itu sendiri.

Selain kebutuhan standarisasi, masalah pelatihan untuk pengembangan standar forensik juga mendapat perhatian. Dalam hal ini terdapat perusahaan komersial, seperti perusahaan yang bergerak pada bidang pengembangan perangkat lunak forensik yang menawarkan program sertifikasi dan topik analisis forensik digital yang digolongkan ke dalam fasilitas pelatihan spesialis penyidik Inggris. Hingga akhirnya pada tahun 1990 M, perangkat seluler semakin berkembang dengan ketersediaan yang makin meluas melebihi perangkat komunikasi sederhana. Dengan kegunaan perangkat ini bahkan mampu mendapatkan informasi yang lebih banyak [23]. Walaupun begitu, analisis digital pada ponsel jauh tertinggal dibanding dengan media komputer tradisional dikarenakan bersifat kepemilikan [24]. Setelah itu, fokus beralih pada bentuk kejahatan *internet* yang dapat menjadikan perang dunia maya dan *cyberterrorism.* Hal ini disimpulkan oleh Komando Pasukan Gabungan Amerika Serikat pada tahun 2010 dengan tanggapan bahwa melalui dunia maya, musuh dapat menargetkan beberapa hal, seperti industri, akademisi,

pemerintah, serta militer, baik di darat, maritim, udara, maupun ruang angkasa. Ditambahkannya bahwa dunia maya telah mematahkan hambatan fisik yang melindungi suatu bangsa dari serangan terhadap perniagaan dan komunikasi. Seperti halnya kekuatan udara yang mampu mengubah medan perang selama Perang Dunia II [25]. Kemudian dilanjutkan dengan permasalahan di bidang forensik digital yang belum terselesaikan pada tahun 2009 oleh Peterson dan Shenoi yang melakukan penelitain dengan judul *Digital Forensic Research: The Good, the Bad, and the Unaddressed*. Penelitian tersebut membahas tentang cara melakukan identifikasi bias pada sistem operasi *Windows* dalam penyelidikan forensik digital [26]. Lalu pada tahun 2010, Simson Garnfinkel melakukan identifikasi mengenai masalah penyelidikan digital di masa yang akan datang, termasuk dengan ukuran media digital yang meningkat, ketersediaan enkripsi yang membuat informasi tidak dapat dibaca apabila tidak ada pengetahuan khusus, sistem operasi yang semakin beragam, meningkatnya individu yang memliki banyak perangkat, serta batasan-batasan hukum terhadap para penyidik.

2.3 Perkembangan Peralatan Forensik

Pada masa pengembangan peralatan forensik, kebanyakan para penyidik melakukan *live analysis* pada media, serta melakukan pemeriksaan komputer dari sistem operasi menggunakan *sysadmin* yang tersedia untuk mengekstrak barang bukti. Hal ini mempunyai resiko yang tinggi baik secara sengaja ataupun tidak sengaja karena dapat menyebabkan klaim kerusakan terhadap barang bukti. Hal tersebut dilakukan karena selama tahun 1980 M, alat digital forensik masih sangat sedikit yang tersedia. Untuk mengatasi hal tersebut, diciptakan berbagai peralatan forensik pada awal tahun 1990 M. Adapun kebutuhan untuk

perangkat lunak ini pertama kali diakui oleh Pusat Pelatihan Penegak Hukum Federal pada tahun 1990 M oleh Michael White dan diikuti dengan *Safe Back* yang dikembangkan oleh Sydex. Perangkat lunak sejenis juga berkembang di negara lain, seperi DIBS yang merupakan solusi perangkat keras serta perangkat lunak yang secara komersial dirilis pada tahun 1991 di Inggris serta dirilis pula *Fixed Disk Image* gartis untuk penegak hukum Australia oleh Rob McKemmish. Kemudian dilanjutkan dengan semakin berkembangnya permintaan untuk memenuhi bukti digital yang semakin banyak, muncul pula peralatan komersial yang canggih, seperti *EnCase* dan FTK. *EnCase* adalah perangkat lunak yang digunakan oleh para pelaksana hukum dalam mendapatkan keterangan, kesaksian, dan bukti kejahatan dengan melakukan *scan* terhadap *hard disk*. Sedangkan FTK adalah sebuah perangkat lunak yang berfungsi untuk melakukan proses akusisi data forensic. Alat tersebut berguna untuk memeriksa salinan media tanpa harus melakukan forensik secara langsung. Namun pembahasan mengenai forensik memori secara langsung mulai berkembang sehingga tercipta alat yang dinamakan *WindowsSCOPE*. *WindowsSCOPE* adalah forensik memori dan produk rekayasa untuk *Windows* yang digunakan untuk memperoleh dan menganalisis memori serta melakukan deteksi dan rekayasa *rootkit* dan *malware* lainnya. Lalu muncul juga alat khusus, yaitu *Radio Tactics Aceso* yang tersedia untuk perangkat seluler dengan kelebihan, yaitu penyidik dapat mengakses data langsung pada perangkat [8].

3. Asal Usul Ilmu Forensik

3. Asal Usul Ilmu Forensik

3.1 Toksikologi

Toksikologi merupakan pemahaman tentang pengaruh-pengaruh bahan kimia yang merugikan bagi organisme hidup. Diawali dengan kejadian penyebaran racun yang terus-menerus terjadi pada abad ke-19, para ahli sejarawan mencatat bahwa keracunan tersebar luas di beberapa tempat, seperti Italia dan Perancis. Pada saat itu, belum ada yang dapat membuktikan bahwa orang-orang disana telah diracuni. Sehingga diadakan sebuah praktikan medis yang bertempat di Eropa oleh angkatan senjata dengan beberapa universitas disana yang mulai bekerjasama untuk menggali informasi terkait racun yang menjadi penyebab kematian. Salah satu dokter bedah yang bernama Ambroise Pare secara sistematis melakukan penelitian mengenai efek dari kematian pada organ dalam [27]. Sedangkan dua dokter ahli bedah yang berasal dari Italia, yaitu Fortunanto Fidelis dan Paolo Zacchia berhasil mendirikan pusat panthology untuk mempelajari struktur dari tubuh manusia.

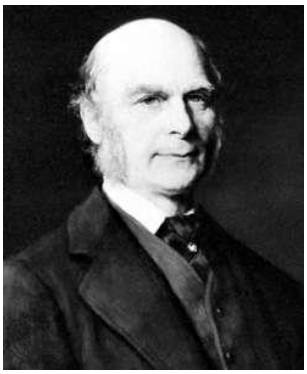
Berawal dari hal tersebut, terdapat banyak peran dokter-dokter lain yang ikut serta dalam melakukan uji forensik terhadap suatu kasus kematian. Sehingga pada tahun 1733 M, ditemukan metode dalam mendeteksi racun arsenik yang berhasil diteliti oleh Carl Wilhelm Scheele yang berasal dari Swedia dan pada tahun 1806 M, ditemukan pula cara melakukan deteksi racun yang ada pada dinding perut manusia oleh seorang kimiawan yang bernama Valentin Ross yang berasal dari Jerman [28]. Kemudian pada tahun 1887 M, lahir seorang tokoh forensik yang bernama Mathieu Orfila yang menyebebakan ilmu forensik semakin berkembang. Mathieu berasal dari Spanyol dan pada tahun 1981 M, Mathieu belajar di Valenica, Madrid, hingga berhasil mendapatkan gelar medisnya. Setelah itu, Mathieu akhirnya menetap di Perancis hingga

berhasil mengembangkan ilmu forensik dan dijuluki sebagai Bapak Toksikologi Forensik.

3.2 Anthropometry

Secara literalur, anthropometry diartikan sebagai pengkuran manusia dan dalam antropologi fisik, hal tersebut merujuk pada pengukuran seorang manusia untuk mengetahui variasi fisik manusia yang terbilang rinci dengan deskripsi dan pengukuran subjek, seperti tinggi, lebar kepala, panjang kaki, dan lain sebagainya. Dalam hal ini, pengaplikasian teknik anthopologi berhasil dilakukan oleh seorang ilmuwan sekaligus polisi yang bernama Alphonse Bertillion yang berasal dari Perancis. Alphonse membentuk sebuah identifikasi berbasis pada parameter pengukuran berupa fisik dan berhasil merancang sistem identifikasi seseorang dengan menggunakan serangkaian ukuran tubuh seseorang. Sistem tersebut dirancang sebagai alat untuk menganalisis hal yang terjadi di TKP. Hingga saat ini, alat tersebut masih digunakan dan sangat bermanfaat untuk membantu menuntaskan tindak kejahatan yang terjadi dimana saja [29].

Dilanjutkan pada tahun 1884 M, Francis Galton yang merupakan seorang ilmuwan asal Inggris, mulai belajar mengenai anthropometry. Galton melakukan penelitian terkait pengukuran karakteristik fisik dan kekuatan, seperti pegangan kekuatan dan ketajaman penglihatan. Hingga pada akhir tahun 1880 M, Francis Galton mulai berpikir bahwa sidik jari merupakan bagian dari karakteristik fisik. Adapun tokoh bernama Francis Galton yang dimaksud dapat dilihat pada gambar 3.1 sebagai berikut:



Gambar 3.1 Francis Galton [31]

3.3 Sidik jari

Sidik jari pertama kali digunakan untuk mengidentifikasi tersangka kriminal. Hal tersebut berhasil dilakukan oleh Sir William Herschel yang merupakan salah satu pengacara pertama yang menggunakan sidik jari sebagai barang bukti. William juga bekerja di *Indian Civil Science* pada tahun 1858 M hingga berhasil membuat penyimpanan dokumen dengan cap jari sebagai bentuk pengaman dalam memastikan tanda tangan [30]. Tidak lama dari itu, muncul juga ilmuwan asal Spanyol yang berhasil menerbitkan sebuah risalah pada deteksi racun. Hingga pada akhir adab ke-19, banyak pejabat administrasi Inggris dan ilmuwan yang berhasil mengungkapkan bagaimana sidik jari dapat difungsikan untuk melakukan identifikasi seseorang serta mengungkapkan kasus kejahatan.

4. Perkembangan Ilmu Forensik

4. Perkembangan Ilmu Forensik

4.1 Penemuan Terdahulu

Seiring dengan berkembangnya ilmu forensik, penyelesaian sebuah kasus juga sangat bergantung pada berbagai kesaksian yang disertai dengan sejumlah keterangan. Namun dengan berbagai kasus kejahatan yang semakin meningkat, seperti halnya banyak barang berharga yang dicuri, perampokan merajalela, hingga pencurian yang bersifat anarksi, membuat pihak yang berwenang tidak mampu lagi untuk menyelesaikan dan memberi keputusan dalam suatu kasus apabila hanya bergantung pada keterangan serta pengakuan dari para saksi yang hadir saat berlangsungnya pengadilan. Tetapi hal tersebut dapat diatasi ketika ditemukan teori mengenai sidik jari manusia. Sidik jari setiap manusia pasti berbeda karena tidak ada dua orang pun yang memiliki sidik jari yang sama. Hingga pada tahun 1901 M, muncul ide baru mengenai sistem pengelompokkan golongan darah yang dikemukakan oleh Karl Landsteiner yang merupakan ahli biologi sekaligus pemegang nobel yang berasal dari Austria. Pada tahun yang sama pula, Paul Uhlenhuth yang merupakan ahli biologi yang berasal dari Jerman menggunakan tes *precipitin* untuk mengetahui tentang sebuah sampel darah yang dapat dibandingkan antara darah manusia atau darah hewan.

Dengan adanya terobosan-terobosan yang revolusioner dan sangat membantu dalam proses investigasi kasus kejahatan, muncul kembali ilmuwan forensik yang berasal dari Perancis pada tahun 1910 yang bernama Edmond Locard. Edmond mampu mengembangkan teori mengenai dua orang yang melakukan kontak fisik meskipun dengan cara atau waktu yang singkat, orang tersebut dapat diketahui jejaknya. Hal ini dikenal sebagai *Locard's Exchange Principle* atau secara sederhana dapat diartikan bahwa setiap kontak pasti meninggalkan jejak. Penerapan

Locard's Exchange dapat dilakukan pada setiap keadaan, seperti halnya jika ada seseorang yang memasuki sebuah ruangan, maka setelah itu ruangan tersebut akan mengalami perubahan. Hal yang dimaksud adalah orang tersebut pasti meninggalkan jejak, seperti sel kulit, sehelai rambut yang jatuh, sehelai serat kain yang tipis dari pakaiannya, dan hal lain sebagainya. Jejak-jejak yang dicontohkan memang berukuran sangat kecil (mikroskopis), namun hal tersebut dapat diteliti secara detail oleh pihak berwenang dalam proses investigasi sebuah kasus kejahatan. Untuk lebih jelasnya, penemuan-penemuan dari berbagai tahap perkembangan ilmu forensik yang ada sejak sebelum masehi [5] dapat dijelaskan sebagai berikut:

- Sebelum Masehi, bukti dari sidik jari yang berasal dari lukisan pada ukiran manusia zaman pra-sejarah
- Tahun 700 M, sidik jari dapat membangun identitas dari dokumen dengan patung tanah liat yang digunakan oleh orang Cina.
- Tahun 1000 M, seorang pengacara di pengadilan Romawi yang bernama Quintilian, menunjukkan cetakan kepala yang berdarah pada kasus orang buta yang membunuh ibunya.
- Tahun 1248 M, terdapat buku dari Cina oleh Hsi Duan Yu yang berjudul *The Washing Away of Wrong* yang berisi tentang cara membedakan kasus tenggelam dari cekikan.
- Tahun 1609 M, muncuk risalah pertama terhadap pemeriksaan dokumen secara sistematis yang diterbitkan oleh Francois Demelle di Perancis
- Tahun 1686 M, seorang profesor anatomi yang bernama Marcello Malphigi dari *University of Bologna*, mencatat karakteristik sidik jari.
- Tahun 1784 M, John Toms yang berasal dari Lancaster, Inggris, dihukum akibat kasus pembunuhan yang diketahui penyebabnya dari

temuan berupa pistol dan sobekan surat kabar yang ada dalam sakunya.

- Tahun 1800 M, Thomas Bewick yang merupakan seorang naturalis asal Inggris, menggunakan ukiran sidik jari sebagai identifikasi buku-buku yang diterbitkan.
- Tahun 1810 M, Eugene Francois Vidocq, menmbuat kesepakatan bersama polisi untuk membangun kekuatan pada langkah detektif pertama. Pada tahun ini pula, tercatat bahwa dokumen yang berhasil diidentifikasi dari sebuah tes kimia untuk tinta tertentu dikenal sebagai dokumen yang berasal dari Konigin Hanschritt.
- Tahun 1813 M, seorang profesor obat kimia di *University of Paris* yang berasal dari Spanyol, yaitu Mathiew Orfila, menerbitkan Traite des Racun Ban des Regnes Mineral. Orfila dianggap sebagai bapak Toksikologi modern yang membuat kontribusi dengan sangat signifikan terhadap pengembangan tes darah dalm bidang forensik dan juga merupakan orang pertama yang mencoba menggunakan mikroskop dalam membantu penelitiannya terkait darah dan noda air mani.
- Tahun 1823 M, seorang profesor anatomi di *University of Breslau*, Czecheslovakia, yang bernama John Evangelist Purkinji, menerbitkan makalah pertama mengenai sifat sidik jari dan memberi saran terkait sistem pengelompokkan berdasarkan sembilan jenis utama sidik jari. Namun hal tersebut gagal dalam pengenalan potensi secara individualistis.
- Tahun 1828 M, terdapat penemuan berupa mikroskop cahaya polariasi oleh William Nichol.
- Tahun 1830 M, seorang ahli statistik Belgia yang bernama Adolphe Quetelet, memberikan landasan utama untuk pekerjaan Bertillon

dengan menyatakan keyakinannya bahwa tidak ada dua tubuh manusia yang persis sama.

- Tahun 1831 M, Leuchs merupakan orang pertama yang mencatat aktivitas amilase pada air lir manusia.
- Tahun 1835 M, salah satu *Scotland Yard*'s yang bernama Henry Goddard, pertama kali menggunakan perbandingan peluru dalam menangkap pembunuh. Perbandingan tersebut didasarkan pada cacat yang terlihat pada peluru yang digunakan dengan menelusuri kembali dari cetakannya.
- Tahun 1836 M, seorang ahli kimia asal Skotlandia yang bernama James Marsh, pertama kali menggunakan toksikologi (deteksi arsenik) dalam sidang.
- Tahun 1839 M, H. Bayard menerbitkan prosedur andalan pertamanya dalam proses deteksi mikroskopis sperma. Bayard juga mencatat karaktersitik terhadap mikroskopis yang berbeda dari berbagai kain substrat.
- Tahun 1851 M, seorang profesor kimia asal Brussels, Belgia, yang bernama Jean Servais Stas, pertama kali berhasil melakukan identifikasi pada racun sayuran yang ada pada jaringan tubuh manusia.
- Tahun 1853 M, Ludwig Teichmann di Kracow, Polandia, pertama kali melakukan pengembangan tes kristal mikroskopis pada hemoglobin menggunakan kristal jenis hemin.
- Tahun 1854 M, seorang dokter Inggris yang bernama Maddox, melakukan perkembangan pelat fotografi kering menggunakan metode timah. Hal tersebut merupakan langkah praktis dalam memotret tahanan untuk catatan penjara.

- Tahun 1856 M, seorang perwira asal Inggris yang bernama Sir William Herschel, bekerja untuk layanan sipil di India dengan menggunakan cap jempol pada dokumen sebagai pengganti tanda tangan untuk buta aksara serta dokumen untuk verifikasi.
- Tahun 1862 M, J. Izzak Van Deen yang merupakan ilmuwan asal Belanda, melakukan pengembangan pada tes dugaan darah menggunakan guaiac.
- Tahun 1863 M, seorang ilmuan asal Jerman yang bernama Schonbein, pertama kali menemukan kemampuan dari hemoglobin sebagai oksidasi hidrogen peroksida, sehingga dapat membentuk busa.
- Tahun 1864 M, Odelbrecht memberi saran dalam hal penggunaan fotografi sebagai identifikasi penjahat dan dokumentas bukti dalam berbagai adegan kejahatan.
- Tahun 1877 M, seorang mikroskopis di Departemen Pertanian Amerika Serikat yang bernama Thomas Taylor, mengungkapkan bahwa tanda dari telapak tangan serta ujung jari dapat difungsikan sebagai identifikasi dalam kasus pidana. Walaupun demikian, ide itu tidak pernah ditanggapi oleh *American Journal of Microscopist*, *Popular Science*, dan *Scientific American*.
- Tahun 1879 M, seorang ahli patologi asal Jerman yang bernama Rudolph Virchow, pertama kali mempelajari tentang keterbatasan pengakuan.
- Tahun 1880 M, seorang dokter yang bernama Henry Fauds yan berasal dari Skotlandia sekaligus bekerja di Tokyo, berhasil menerbitkan sebuah makalah pada *Journal of Nature* yang menunjukkan bahwa sidik jari saat di TKP dapat mengidentifikasi pelaku. Dalam hal ini, Fauds pertama kali menggunakan sidik jari sebagi pemecahan masalah kejahatan yang mengungkapkan bahwa

terdapat seorang tersangka yang tidak bersalah dan kemudian berhasil menunjukkan pelaku sebenarnya pada kasus perampokan di Tokyo.

- Tahun 1882 M, terdapat pembangunan kereta api dengan US *Geological Survey* di New Mexico oleh Gillbert Thompson yang menempatkan cap jempol sendiri untuk melindungi diri dari pemalsuan.
- Tahun 1883 M, seorang karyawan polisi asal Perancis yang bernama Alphonse Bertillon, berhasil mengidentifikasi residivis petama berdasarkan penemuan antropometri.
- Tahun 1887 M, terbit cerita *Sherlock Holmes* pertama oleh Arthur Conan Doyle pada *Christmas* Tahunan Beeton tentang London.
- Tahun 1889 M, seorang profesor kedokteran forensik di *University of Lyons,* Perancis, yaitu Alexander Lacassagne, mencoba melakukan penelitian pertamanya mengenai perbandingan peluru laras senapan yang didasarkan pada parameter jumlah tanah dan alur.
- Tahun 1891 M, Hans Gross melakukan pemerikasaan terhadap hakim dan profesor hukum di *University of Graz,* Austria, dengan memberikan penjelasan pertama menggunakan bukti fisik untuk memecahkan kasus kejahatan.
- Tahun 1892 M, Sir Francis Galton berhasil menerbitkan buku komprehensif pertama mengenai sidik jari disertai dengan langkah-langkah kenggunaannya untuk memecahkan kasus kejahatan. Pada tahun yang sama, seorang peneliti polisi asal Argentina yang bernama Juan Vucetich, berhasil mengembangkan sistem pengelompokkan sidik jari yang akan digunakan di Amerika Latin.
- Tahun 1894 M, Alfred Dreyfus yang berasal dari Perancis, dihukum karena melakukan pengkhianatan berdasarkan pengenalan tulis tangan yang keliru yang berhasil diteliti oleh Bertillon.

- Tahun 1896 M, Sir Edward Richard Henry berhasil mengembangkan sistem pengelompokkan cetak yang akan digunakan di Eropa dan Amerika Utara. Dalam hal ini, Edward menerbitkan klasifikasi dan penggunaan *Finger Prints.*
- Tahun 1898 M, seorang ahli kimia forensik yang sekaligus bekerja di Berlin, Jerman, yaitu Paul Jesrich, melakukan identifikasi terhadap hal-hal kecil, seperti photomicrogrpahs dari dua peluru.
- Tahun 1901 M, seorang imunologi asal Jerman yang bernama Paul Uhlenhuth, berhasil mengembangkan tes precipitin untuk spesies.
- Tahun 1900 M, Karl Landesteiner pertama kali menemukan golongan darah manusia sehingga Karl mendapatkan hadiah Nobel untuk temuannya tersebut.
- Tahun 1901 M, Sir Edward Richard Henry melakukan adopsi pada pengenalan sidik jari untuk menggantikan antropometri. Pada tahun yang sama, Hnery P. DeForrest menjadi pelopor dalam penggunaan sidik jari secara sistematis di Amerika Serikat oleh Komisi Pelayanan *New York Civil*.
- Tahun 1902 M, R.A. Reiss yang merupakan seorang profesor di *University of Lausanne*, Swiss, dan seorang murid dari Bertillon, melakukan penyusunan terhadap salah satu kurikulum akademis pertama pada ilmu forensik.
- Tahun 1903 M, terdapat sistem penjara pertama di New York yang menggunakan sidik jari secara sistematis sebagai identifikasi kriminal.
- Tahun 1904 M, Oskar dan Rudolf Adler berhasil mengembangkan penelitian terkait tes darah untuk dugaan berdasarkan bahan kimia baru yang dikembangkan oleh Merk, yaitu benzidine.

- Tahun 1905 M, Presiden Amerika yang bernama Theodore Roosevelt, berhasil mendirikan FBI.
- Tahun 1910 M, seorang profesor kedokteran forensik di Sorbone, yaitu Victor Balthazard bersama Marcelle Lambert, membuka studi komprehensif pertama kali yang membahas tentang rambut. Seperti halnya kasus pertama yang melibatkan bagian rambut ini adalah Rosella Rousseau yang yakin untuk mengakui bahwa pembunuhan atas Germaine Bichon berawal dari rambut. Pada tahun yang sama, didirikan laboratorium kriminal polisi pertama oleh Edmund Locard yang merupakan penerus Lacassagne sebagai profesor kedokteran forensik di *University of Lyons,* Perancis. Pada tahun ini juga terbit penemuan dokumen yang paling berpengaruh oleh Albert S. Osborne yang berasal dari Amerika.
- Tahun 1912 M, dilakukan pengembangan tes lain dari kristal mikroskopis oleh Masaeo Takayama untuk hemoglobin menggunakan kristal hemochromogen.
- Tahun 1913 M, seorang profesor kedokteran forensik di Sorbone, yaitu Victor Balthazard, pertama kali menerbitkan artikel mengenai individualitas tanda peluru.
- Tahun 1915 M, seorang profesor dari Institut Kedokteran Forensik di Turin, Italia, yaitu Leone Lattes, berhasil mengembangkan tes antibodi pertama untuk golongan darah. Leone pertama kali menggunakan tes tersebut pada penyelesaian kasus sengketa perkawinan. Pada tahun yang sama, dibentuk Asosiasi Internasional terhadap identifikasi kriminal dengan nama IAI yang diselenggarakan di Oakland, Calfornia.

- Tahun 1916 M, Albert Schneider yang berasal dari Berkeley, California, menggunakan alat vakum pertama kali sebagai alat untuk mengumpulkan jejak bukti.
- Tahun 1918 M, Edmond Locard berhasil mengembangkan identifikasi sidik jari dan melahirkan ajaran forensik bahwa setiap kontak meninggalkan jejak.
- Tahun 1920 M, terdapat katalog data dan manufaktur mengenai senjata yang berhasil disusun oleh Charles E. Waite. Pada tahun yang sama, Georg Popp menjadi pelopor dalam menggunakan identifikasi botani pada pekerjaan forensik. Kemudian salah satu kriminalis yang berasal dari Amerika Serikat, yaitu Lukas Mei, juga menjadi pelopor dalam analisis pergoresan seperti pada pisau. Lalu terdapat juga penyempurnaan dari perbandingan mikroskopis yang digunakan untuk membandingkan peluru yang berhsil dilakukan oleh tim, yaitu Calvin Goddard, Charles Waite, Phillip O. Gravelle, dan John H. Fisher.
- Tahun 1921 M, John Larson dan Leonard Keeler berhasil merancang poligraf portabel.
- Tahun 1923 M, Vittorio Siracusa yang bekerja di *Institute of Medicine Law*, *University of Messina*, Italia, berhasil mengembangkan tes penyerapan golongan darah untuk noda darah.
- Tahun 1924 M, seorang kepala polisi asal Los Angeles, California, yang bernama August Vollmer, pertama kali menggunakan penelitian di laboratorium kriminal polisi.
- Tahun 1925 M, seorang ilmuwan asal Jepang yang bernama Saburo Sirai, mengumpulkan penemuan sekresi antigen dari kelompok tertentu yang masuk dalam cairan tubuh selain darah.

- Tahun 1928 M, seorang penyidik medis dan hukum pertama yang bernama Meuller memberi saran mengenai identifikasi ludah amylase sebagai ujian dugaan pada noda saliva.
- Tahun 1929 M, seorang ilmuwan asal Jepang yang bernama Yosida, pertama kali melakukan penyelidikan komprehensif untuk membangun keberadaan isoantibodies serologis dalam cairan tubuh selain darah. Pada tahun yang sama, Calvin Goddard berhasil mendirikan *Scientific Crime Detection Laboratory* di *University of Northwestern,* Evanston, Illinois.
- Tahun 1930 M, staf dari Goddard *Scientific Crime Detection Laboratory* di Chicago berhasil menerbitkan *American Journal of Police Science.*
- Tahun 1931 M, Franz Josef Holzer yang merupakan seorang ilmuwan asal Austria sekaligus bekerja di Institut Kedokteran Forensik dari *University of Innsbruck,* berhasil mengembangkan teknik penyerapan hambatan pada golongan darah.
- Tahun 1932 M, dididirkan laboratorium kirminal FBI.
- Tahun 1935 M, seorang fisikawan asal Belanda, yaitu Frits Zernike, menemukan mikroskop pertama yang dapat mengatur kontras. Dalam hal ini, Frits berhasil mendapatkan hadiah nobel.
- Tahun 1937 M, Walter Specht berhasil mengembangkan luminol reagen chemiluminescent sebagai ujian dugaan darah.
- Tahun 1938 M, terdapat dua orang yang diidentifikasi heptoglobin, yaitu M. Polonvski dan M. Jayle.
- Tahun 1940 M, Landsteiner dan A.S. Wiener pertama kali menjelaskan golongan darah Rhesus. Pada tahun yang sama, seorang ahli kimia (*Etil Corporation*), yaitu Vincent Hnizda, pertama kali

melakukan analisa terhadap cairan ignitable dengan menggunakan peralatan distilasi vakum.

- Tahun 1941 M, Murray Hill dari Bell Labs memulai studi identifikasi *voice print*.
- Tahun 1945 M, Frank Lundquist yang bekerja di Unit Kedokteran Hukum, *University of Copenhagen*, berhasil mengembangkan tes asam fosfatase untuk semen.
- Tahun 1946 M, pertama kali Mourant memberi gambaran mengenai sistem golongan darah Lewis. Pada tahun yang sama, R.R. Ras menjelaskan sistem golongan darah Kell.
- Tahun 1950 M, M. Cutbush bersama rekan-rekannya, pertama kali menjelaskan sistem golongan darah Duffy. Pada tahun yang sama, seorang kepala polisi dari Berkeley, California, yaitu August vollmer, mendirikan sekolah kriminologi di *University of California*, Berkeley. Paul juga merupakan pimpina utama pada bidang ilmu hukum pidana di sekolag tersebut. Kemudian pada tahun ini juga terdapat laboratorium ilmu hukum pidana di Swiss yang didirikan oleh Max Frei Sulzer, dimana laboratorium tersebut digunakan untuk melakukan penelitian terkait pengembangan model rekaman dalam mengumpulkan jejak bukti. Lalu, pada tahun ini pula didirikan AAFS di Chicago, Illinois, serta mulai diterbitkan *Journal of Forencis Science.*
- Tahun 1951 M, F.H. Allen bersama rekan-rekannya, pertama kali memberi gambaran mengenai sistem pengelompokkan darah Kidd.
- Tahun 1953 M, pertama kali diterbitkan *Crime Investigation* sebagai salah satu hukum pidana komprehensif dan mencakup teori dalam melakukan investigasi berbagai kasus kejahatan.

- Tahun 1954 M, seorang kapten Kepolisian Negara India, yaitu R.F. Borkenstein, berhasil menemukan Breathalyzer yang berfungsi untuk pengujian ketenangan lapangan.
- Tahun 1958 M, A.S. Weiner bersama rekan-rekannya memperkenalkan H-lektin yang berguna untuk menentukan jenis darah O+ (positif).
- Tahun 1959 M, Hirshfeld pertama kali melakukan identifikasi sifat polimorfik terhadap komponen kelompok tertentu.
- Tahun 1960 M, Lucas berhasil memberi gambaran dalam penerapan kromatografi gas untuk identifikasi produk minyak bumi di laboratorium forensik dan membahas keterbatasan dalam identitas merek bensin. Pada tahun yang sama, seorang ilmuwan asal Swiss yang bernama Maurice Muller, melakukan adaptasi terhadap ouchterlony antigen-antibodi uji difusi untuk pengujian precipitin dalam menentukan spesies.
- Tahun 1963 M, D.A. Hopkinson bersama rekan-rekannya, pertama kali melakukan identifikasi sifat polimorfik asam fosfatase eritrosit.
- Tahun 1964 M, N. Spencer bersama rekan-rekannya, pertama kali melakukan identifikasi sifat polimorfik phosphoglucomutase sel darah merah.
- Tahun 1966 M, Brian J. Culliford dan Brian Wraxall berhasil mengembangkan teknik immunoelectrophpretic untuk haptoglobin di noda darah. Pada tahun yang sama, R.A. Fildes dan H. Harris pertama kali melakukan identifikasi sifat polimorfik siklase adenat sel darah merah.
- Tahun 1967 M, Culliford menjadi pemerakarsa dalam pengembangan metode berbasis gel yang digunakan untuk menguji isoenzim di noda darah kering. Culliford juga berperan dalam pengembangan serta

penyebaran metode untuk pengujian protein dan isoenzim dalam darah dan cairan tubuh lainnya.

- Tahun 1968 M, Spencer bersama rekan-rekannya, pertama kali melakukan identifikasi sifat polimorfik sel deaminase adenosin.
- Tahun 1973 M, Hopkinson bersama rekan-rekannya, pertama kali melakukan identifikasi sifat polimorfik esterase D.
- Tahun 1974 M, dilakukan deteksi residu tembakan menggunakan teknologi *scanning* pada mikroskop elektron dengan sinar-x yang dikembangkan oleh J.E. Wessel, P.F. Jones, Q.Y. Kwan, R.S. Nesbitt, dan E.J. Rattin di *Aerospace Corporation.*
- Tahun 1975 M, J.Kompf bersama rekan-rekannya yang bekerja di Jerman, pertama kali melakukan identifikasi sifat polimorfik glyoxylase sel darah merah.
- Tahun 1976 M, Zoro dan Hadley pertama kali dievaluasi GC-MS di Inggris untuk tujuan forensik.
- Tahun 1977 M, seorang pemeriksa jejak bukti di *Crime Laboratory*, Saga Prefektur Badan Kepolisian Nasional Jepang, yaitu Fuseo Matsumur, melakukan identifikasi terkait kasus pembunuhan sopir taksi. Pada tahun yang sama, terjadi penyesuaian FTIR untuk digunakan dalam laboratorium forensik. FTIR adalah teknik yang digunakan untuk mendapatkan spektrum inframerah atau emisi zat padat, cair atau gas. Pada tahun ini juga, FBI pertama kali memperkenalkan AFIS dengan *scan* komputerisasi sidik jari.
- Tahun 1978 M, Brian Wraxall dan Mark Stolorow berhasil mengembangkan metode multisistem untuk menguji sistem isoenzim secara bersamaan pada PGM, ESD, dan GLO. Brian dan Mark juga berhasil mengembangkan metode untuk mengetahui protein serum darah, seperti haptoglobin.

- Tahun 1983 M, Kerry Mullis pertama kali menyusun PCR saat bekerja di *Cetus Corporation*. PCR adalah metode untuk memperbanyak DNA secara enzimatik tanpa menggunakan organisme.
- Tahun 1984 M, Alec Jeffereys berhasil mengembangkan tes DNA pertama yang melibatkan deteksi pola RLFP multilokus. RLFP adalah teknik yang mengeksploitasi variasi dalam urutan DNA homolog, yang dikenal sebagai polimorfisme yang dapat membedakan individu, populasi, atau spesies serta untuk menentukan lokasi gen dalam suatu urutan.
- Tahun 1986 M, Alec Jeffereys melakukan tes DNA untuk menyelesaikan kasus kejahatan dengan mengidentifikasi Colin Pitchfork sebagai pembunuh dua orang gadis di Inggris. Pada tahun yang sama, Henry Erlich berhasil mengembangkan teknik PCR dalam beberapa aplikasi klinis dan forensik. Pada tahun ini juga, Edward Blake pertama kali melakukan tes DNA PCR berbasis HLA DQA1. HLA-DQA1 merupakan gen yang menyediakan instruksi dalam membuat protein penting untuk sistem kekebalan tubuh.
- Tahun 1987 M, pertama kali profil DNA diperkenalkan dalam sebuah pengadilan pidana di Amerika Serikat.
- Tahun 1988 M, Lewellen, McCurdy, Horton, Asselin, Leslie, dan McKinley berhasil mempublikasikan makalah tentang prosedur baru untuk menganalisa obat dalam darah oleh immunoassay enzim homogen.
- Tahun 1990 M, K. Kasai bersama rekan-rekannya berhasil menerbitkan makalah tentang analisis DNA forensik.
- Tahun 1991 M, *Walsh Automation Inc*, di Montreal, berhasil meluncurkan pengembangan sistem pencitraan otomatis yang biasa

disebut IBIS. Sistem tersebut berfungsi untuk membandingkan tanda yang tersisa pada peluru. Kemudian sistem tersebut dikembangkan untuk pasar Amerika Serikat yang bekerjasama dengan Biro Alkohol, Tembakau, dan Senjata Api.

- Tahun 1992 M, NRC I pada DNA Forensik menerbitkan Teknologi DNA bidang ilmu forensik dalam menanggapi kekhawatiran terkait praktek analisis DNA forensik. Pada tahun yang sama, FBI melakukan kontrak dengan *Mnemonic Systems* dalam pengembangan *Drugfire*.
- Tahun 1994 M, *Roche Molecular System* yang sebelumnya bernama *Cetus Corporation*, berhasil merilis satu set yang terdiri dari lima penanda DNA tambahan (*polymarker)* yang berfungsi untuk menambah sistem HLA DQA1 pada DNA forensik.
- Tahun 1996 M, NRC II pada DNA forensik diselenggarakan dan diterbitkan Evaluasi Bukti DNA forensik. Pada tahun yang sama, FBI memperkenalkan pencarian komputerisasi pada database sidik jari AFIS.
- Tahun 1998 M, database FBI DNA dengan NDIS melakukan kerjasama antar negara.
- Tahun 1999 M, FBI melakukan *upgrade* terhadap data sidik jari yang terkomputerisasi dan menerapkan IAFIS yang terhubung langsung ke database nasional. Pada tahun yang sama, ditandatangani nota kesepahaman antara FBI dan ATF dalam penggunaan Nasional Terpadu Balistik Jaringan yang berfungsi untuk memberi fasilitas pertukaran data antara *Drugfire* dan IBIS.
- Tahun 2001 M, profil DNA yang beperan sebagai bukti mengalami kemajuan teknologi dari segi waktu mulanya kisaran enam sampai delapan minggu menjadi satu sampai dua hari.

- Tahun 2007 M, Layanan Sains Forensik meluncurkan Teknologi Sepatu Intelijen yang dapat membantu pihak kepolisian dalam melakukan identifikasi tanda alas kaki di TKP secara cepat.
- Tahun 2008 M, Pusat Penelitian Forensik di *University of Leicester*, Inggris, berhasil mengembangkan teknik dalam mengambil sidik jari pada permukaan logam di TKP.
- Tahun 2011 M, terdapat beberapa peneliti yang berasal dari *Michigan State University* yang mengembangkan suatu algoritma dan perangkat lunak secara otomatis berdasarkan sketsa yang dibuat. Pada tahun yang sama, seorang peneliti yang berasal dari Jepang berhasil mengembangkan sistem pencocokan gigi berdasarkan x-ray dari alhi forensik dan berhasil meningkatkan hasil nilai akurasi.

4.2 Timeline Digital Forensik

Secara umum, *timeline* digital forensik dapat dijelaskan sebagai berikut:

- Tahun 1970 M, terdapat sebuah kasus tindak pidana mengenai penipuan keuangan yang pertama kali ditelusuri dengan melibatkan bantuan komputer.
- Tahun 1980 M, mulai dilakukan pelatihan-pelatihan tentang forensik komputer dikarenakan semakin banyak investigator keuangan serta pihak pengadilan yang menyadari bahwa kasus-kasus yang dihadapi dapat dituntaskan apabila dapat menelusuri bukti-bukti yang ada melalui komputer.
- Tahun 1984 M, FBI berhasil membuat program bernama *Magnetic Media Program* yang kemudian berubah menjadi CART.
- Tahun 1987 M, *Access Data* yang merupakan perusahaan di bidang komputer forensik berhasil didirikan.

- Tahun 1988 M, asosiasi internasional yang bernama IACIS berhasil didirikan.
- Tahun 1993 M, pertama kali diselenggarakan konferensi internasional terkait bukti-bukti pada komputer.
- Tahun 1995 M, organisasi internasional yang bernama IOCE berhasil didirikan.
- Tahun 1997 M, terdapat deklarasi di negara-negara *Group of Eight* (Perancis, Jerman Barat, Italia, Jepang, Inggris, Amerika Serikat, Kanada, dan Rusia) yang berisi bahwa para penegak hukum harus diberikan pelatihan serta perlengkapan dalam menghadapi dan menuntaskan berbagai kasus kejahatan yang melibatkan kecanggihan teknologi.
- Tahun 1998 M, di negara-negara *Group of Eight* memberi usul terkait pembuatan prinsip, tata cara, serta prosedur internasional untuk bukti digital.
- Tahun 1999 M, FBI CART terhitung telah menangani lebih dari 2000 kasus terkait kejahatan komputer dan menganalisis 17 TB data.
- Tahun 2000 M, pertama kali didirikan laboratorium forensik komputer regional FBI.
- Tahun 2003 M, FBI CART terhitung telah menangani lebih dari 6500 kasus terkait kejahatan komputer dan menganalisis 782 TB data.

4.3 Fase Digital Forensik

Dalam hal ini, para peneliti membagi sejarah dari digital forensik dalam beberapa fase sebagai berikut:

a. *Ad-hoc phase*

Ad-hoc phase yaitu fase yang didasarkan pada berbagai karakteristik yang ada. Pada fase ini, struktur masih kurang baik, tujuan kurang jelas,

serta peralatan, proses, dan prosedur yang belum memadai. Kemudian masih terdapat isu hukum ketika melakukan proses bukti digital.

b. *Structured phase*

Structured phase yaitu fase yang memiliki solusi lengkap untuk komputer forensik, mulai dari prosedur yang diterima, pengembangan peralatan khusus, serta kejelasan UU yang mengatur berbagai penggunaan bukti-bukti digital.

c. *Enterprise phase*

Enterprise phase yaitu fase yang terdiri dari 3 bagian yang meliputi pengumpulan bukti secara *real-time*, pengembangan alat bukti di TKP, serta forensik yang menjadi sebuah layanan dalam perusahaan.

5. Alur Kerja Forensik

5. Alur Kerja Forensik

5.1 Proses Forensik

Pada penyelidikan digital forensik, terdapat berbagai tahapan digital forensik yang meliputi berbagai proses forensik yang diakui. Peneliti forensik yang bernama Eoghan Casey mendefinisikan hal tersebut sebagai langkah-langkah yang diawali dari sinyal awal suatu insiden hingga pelaporan temuan. Adapun tokoh bernama Eoghan Casey yang dimaksud dapat dilihat pada gambar 5.1 sebagai berikut:

Gambar 5.1 Eoghan Casey [32]

Dalam terminologi hukum, temuan berupa media digital yang disita untuk penyelidikan biasa disebut sebagai barang bukti. Barang bukti berupa bukti digital dapat ditemukan oleh penyelidik menggunakan metode ilmiah dengan tujuan untuk mendukung atau menyangkal hipotesis, baik dalam pengadilan atau proses perdata.

Secara umum, tahapan digital forensik yang membutuhkan pelatihan dan pengetahuan spesialis adalah sebagai berikut:

a. Teknisi digital forensik

Teknisi berperan untuk mengumpulkan dan memproses bukti-bukti di TKP. Sebelumnya, seorang teknisi diberi pelatihan tentang penanganan terkait teknologi secara benar, seperti memelihara atau mempertahankan bukti. Teknisi juga memungkinkan untuk melakukan analisis secara langsung di TKP.

b. Pemeriksa bukti digital

Dalam memeriksa bukti digital, dibutuhkan seseorang yang khusus pada satu bidang bukti digital, baik pada tingkat secara luas (forensik komputer, forensik jaringan, dan lain-lain) atau sebagai subspesialis (analisis gambar).

c. Model pemrosesan

Pada penyelidikan forensik, hal yang sangat penting adalah metodologi yang digunakan dalam melakukan penelitian tersebut dan prosedur standar dari proses investigasi yang lebih akurat, kuat, dan efisien. Adapun upaya yang pertama kali diusulkan dalam mengembangkan model proses digital forensik, yaitu akuisisi, identifikasi, evaluasi, dan admisi. Pada saat itu, banyak model pemrosesan yang dilakukan yang berkaitan dengan tahapan mengidentifikasi, memperoleh, menganalisis, menyimpan, serta melaporkan bukti digital yang diperoleh. Namun dalam beberapa tahun terakhir, model pemrosesan yang berkembang semakin banyak dan lebih canggih. Bahkan dalam dekade terakhir, bidang investigasi digital forensik beralih menjadi model pemrosesan bukti berbasis *cloud computing* yang sangat bermanfaat dalam pengumpulan berbagai bukti.

5.1.1 Pengumpulan

Pada saat mengumpulan bukti, dilakukan pengambilan citra dari RAM atau pada media penyimpanan lain, serta membuat duplikat (duplikat forensik atau citra forensik) dari media tersebut. Dalam melakukan hal tersebut, seringkali dibantu dengan perangkat *write blocking* yang berfungsi untuk mencegah adanya modifikasi dari media asli. Citra yang diperoleh dari media atau data asli, kemudian di-*hash* menggunakan algoritma MD5 yang merupakan fungsi hash kriptografik secara luas dengan *hash value* 128-bit. Algoritma MD5 telah digunakan pada berbagai aplikasi keamanan serta umum digunakan untuk melakukan pengujian integritas terhadap berkas-berkas, lalu nilai-nilainya dibandingkan agar dapat memverifikasi bahwa salinan yang dimaksud akurat. Pengumpulan bukti juga dapat dilakukan dengan pendekatan alternatif atau biasa disebut *hybrid forensics* atau *distributed forensics*. *Hybrid forensics* merupakan proses menggabungkan tahapan forensik digital dan *electronic discovery* yang mengacu pada langkah-langkah suatu data elektronik dicari, ditempatkan, diamankan, serta dicari dengan maksud untuk menggunakannya sebagai bukti dalam kasus hukum perdata atau pidana. Hal tersebut dapat dilakukan secara *offline* pada komputer tertentu atau dapat dilakukan dalam jaringan.

Pendekatan lain yang dilakukan dalam proses forensik adalah pendekatan konvensional. Pendekatan konvensional ini biasanya diterapkan untuk forensik statik yang menggunakan tahapan dimana bukti-bukti diolah secara *bit by bit image* dalam melakukan proses forensik. Proses forensik tersebut berlangsung secara otomatis pada sistem yang tidak sedang menyala. Forensik statik ini berfokus terhadap pemeriksaan hasil *imaging* untuk menganalisis isi dari bukti-bukti digital, seperti terdapat berkas yang dihapus, riwayat dari berkas yang diakses,

riwayat dari *user login*, penjelajahan web, berkas fragmen, koneksi jaringan, dan lain sebagainya. Hal tersebut dilakukan untuk membuat *timeline* berupa rangkuman mengenai kegiatan yang dilakukan sebagai bukti digital ketika diperlukan. Apabila perangkat dalam keadaan tidak menyala, data yang dapat diselidiki adalah data yang hanya tersimpan pada memori statis, seperti *hard disk*. Namun masih terdapat berbagai proses yang perlu dilakukan sebelum melakukan analisis data aktual pada unit penyimpanan. Sehingga pada saat melakukan penyelidikan forensik, terutama dalam proses penegakan hukum, perlu diambil tindakan untuk menghilangkan peluang adanya modifikasi terhadap bukti yang sebenarnya. Apabila ada yang menyalakan perangkat dan mengoperasikannya, data asli tersebut dapat saja dimodifikasi sehingga hal tersebut dapat membuat bukti tidak orisinil. Jadi, bukti yang sudah terkontaminasi sangat sulit bahkan tidak akan layak untuk dibawa ke pengadilan. Sehingga hal tersebut perlu dibuatkan salinan bukti yang identik dengan menggunakan perangkat khusus atau komputer biasa dengan bantuan *write blocker* serta *disk imaging*. Salinan tersebut biasa disebut dengan FDI. Kemudian salinan tersebut akan dianalisis kembali di laboratorium forensik.

Cara pengumpulan bukti lainnya adalah dengan cara semua bukti dikumpulkan ketika sistem sedang berjalan atau disebut secara forensik langsung. Hal tersebut membuat pemeriksa mendapat kesempatan dalam mengumpulkan data yang mudah hilang dengan memuat berbagi informasi mengenai hal yang sedang dilakukan perangkat. Adapun tujuan utama dari penyelidikan secara langsung adalah dapat mengumpulkan data sebanyak-banyaknya. Pendekatan forensik langsung ini juga memberikan kesempatan untuk melakukan pemeriksaan pada *hard dsik* yang aktif dienkripsi, sehingga penyelidik juga dapat mengumpulkan versi

data yang tidak terenkripsi. Terkait cara yang digunakan untuk memastikan semua data pada *hard dsik* tersebut dienkripsi pada saat komputer tidak menyala yaitu dengan implementasi FDE. Namun saat komputer aktif kembali, data tersebut akan dienkripsi. Maka dari itu, penyelidik perlu memastikan dan melakukan pencarian secara menyeluruh untuk perangkat lunak enkripsi yang mungkin terpasang pada komputer. Apabila terdapat tanda-tanda enkripsi, maka penyelidik harus membuat *logical image* dari *hard dsik* tersebut untuk menjamin bahwa data dapat dipertahankan dan tersedia untuk dilakukan dianalisis lebih lanjut.

5.1.2 Analisis

Setelah melalui tahap pengumpulan bukti, seorang penyelidik melakukan analisis menggunakan berbagai metodologi dan instrumen yang beragam. Seperti pada tahun 2002, terdapat sebuah artikel yang berasal dari *International Journal of Digital Evidence* yang menerangkan bahwa tahap analisis ini merupakan pencarian sistematis lebih mendalam terkait bukti-bukti yang diperoleh dengan dugaan kasus kejahatan. Kemudian pada tahun 2006, terdapat seorang peneliti forensik yang bernama Brian Carrier menjelaskan tentang prosedur intuitif. Prosedur intuitif adalah cara mengelola bukti dengan diidentifikasi terlebih dahulu lalu dilakukan pencarian secara menyeluruh untuk melengkapi kekurangannya. Dalam menggali informasi, analisi forensik pada dasarnya dilakukan untuk menjawab pertanyaan penyelidikan dengan melakukan analisis data yang ditemukan pada citra forensik yang dibuat pada saat dilakukan pengumpulan bukti. Namun sebenarnya proses analisis ini bervariasi tergantung kebutuhan, tetapi metodologi secara umum yang dilakukan adalah melakukan pencarian kata kunci di seluruh

media digital, memulihkan berkas yang dihapus dan melakukan ekstraksi informasi, seperti menampilkan akun pengguna atau perangkat USB yang terpasang. Setelah berbagai bukti dianalisis, langkah selanjutnya adalah membuat kesimpulan terkait bukti yang dianalisis untuk merekonstruksi peristiwa yang terjadi.

5.1.3 Pelaporan

Setelah pengumpulan bukti dianalisis, tahap selanjutnya adalah membuat laporan. Pelaporan dilakukan saat penyelidikan telah selesai sehingga keseluruhan data dapat disajikan dalam bentuk laporan tertulis menggunakan istilah-istilah atau bahasa non teknis. Dalam laporan yang dibuat, disajikan berbagai penemuan yang bersifat objektif serta terdapat kesimpulan dari penemuan tersebut. Terkait isi laporan, hal tersebut dapat berbeda-beda tergantung UU dan kebijakan lokal, namun secara umum laporan tersebut berisi hal sebagai berikut:

a. Data Kasus

Langkah awal yang diakukan sebelum menyusun laporan adalah memiliki data kasus yang jelas. Informasi tentang orang yang ditugaskan untuk melakukan pemeriksaan, beberapa *identifier* yang menjadi fokus penyelidikan, dan berbagai informasi yang mengidentifikasi potongan bukti yang harus diperiksa, semua tercantum pada data kasus. Data kasus digunakan sebagai perbandingan agar dapat membedakan suatu pemeriksaan dengan pemeriksaan lain.

b. Tujuan Pemeriksaan

Dalam laporan, sudah semestinya memuat tujuan dari pemeriksaan yang dilakukan. Tujuan yang dibuat dalam laporan harus menyajikan fokus yang dicari selama pemeriksaan serta diawali dengan pertanyaan

oleh orang yang menugaskan untuk melakukan pemeriksaan atau dapat mencakup tujuan yang dilakukan oleh pemeriksa forensik saat menganalisis suatu kasus.

c. Temuan

Temuan yang disajikan dalam laporan merupakan berbagai potongan bukti yang didapatkan selama pemeriksaan. Temuan juga disajikan secara objektif (tidak membuat kesimpulan secara interpretasi subjektif).

d. Kesimpulan

Pada bagian kesimpulan, laporan disusun oleh alhi forensik berdasarkan dari berbagi temuan, pengetahuan, dan pengalaman. Namun dalam laporan forensik ini dipisahkan antara temuan objektif dan temuan subjektif. Penulisan kesimpulan juga harus menggunakan kalimat yang mudah dimengerti agar ketika dibawa ke pengadilan, semua pihak yang terlibat walau tidak memiliki keahlian pada bidang IT dapat mengerti tentang laporan yang dijelaskan.

5.2 Penerapan Forensik

5.2.1 Kegunaan Forensik

Secara umum, digital forensik digunakan dalam hukum pidana dan penyelidikan pribadi. Digital forensik yang dikaitkan dengan hukum pidana berarti bahwa bukti-bukti yang dikumpulkan dapat digunakan sebagai pendukung atau penentang hipotesis di pengadilan. Dalam beberapa kasus, bukti-bukti yang telah terkumpul untuk memenuhi proses pengadilan juga merupakan bentuk pengumpulan intelijen yang digunakan dengan tujuan menemukan, mengidentifikasi, bahkan dapat menutup kemungkinan adanya kejahatan lain. Pada contoh perkara perdata atau permasalahan perusahaan, digital forensik merupakan salah

satu bagian dari proses *electronic discovery* dengan langkah-langkah forensik yang serupa dalam investigasi pidana, namun dengan persyaratan dan batasan hukum yang berbeda. Selain untuk kepentingan pengadilan, digital forensik juga dapat menjadi bagian dari penyelidikan internal sebuah perusahaan.

Adapun contoh dari penyelidikan internal sebuah perusahaan, yaitu terjadinya intrusi jaringan tanpa otorisasi. Hal ini membuat pakar forensik melakukan pemeriksaan terkait sifat dan dampak dari serangan yang dilakukan sebagai upaya untuk membatasi terjadinya kerusakan yang lebih parah dengan menetapkan sejauh mana intrusi tersebut ataupun sebagai upaya untuk melakukan identifikasi penyerang. Serangan seperti ini biasanya dilakukan melalui saluran telepon, seperti yang terjadi pada tahun 1980 M. Namun untuk era modern, hal tersebut sudah menyebar melalui *internet*.

5.2.2 Penyelidikan Forensik

Penyelidikan digital forensik berfokus untuk mengungkap bukti-bukti yang objektif berdasarkan aktivitas kriminal atau disebut sebagai *actus reus* dalam bahasa hukum. Namun dengan adanya berbagai data yang tersimpan pada perangkat digital dapat membantu bidang penyelidikan lainnya. Adapun penyelidikan digital forensik secara keseluruhan membahas beberapa hal sebagai berikut:

a. Keterkaitan

Dalam hal ini, mengaitkan sutau tindakan kepada seseorang dapat menggunakan metadata. Seperti halnya dokumen pribadi pada *drive* komputer yang mungkin dapat mengidentifikasi pemiliknya. Jadi, metadata dapat dikatakan sebagai struktur informasi yang menyediakan data secara detail. Berbagai jenis metadata, yaitu metadata deskriptif

(metadat yang memberikan informasi yang mencakup berbagai elemen, seperti judul, abstrak, penulis, dan kata kunci), metadata struktural (metadata yang menunjukkan bagaimana objek gabungan disatukan, seperti halaman yang disusun untuk membentuk bab), metadata administratif (metadata yang memberikan informasi untuk membantu mengelola sumber daya, seperti jenis sumber daya, izin, dan waktu), metadata referensi (metadata yang berisi informasi tentang isi dan kualitas data statistik), dan metadata statistik (metadata yang dapat menggambarkan proses untuk menghasilkan data statistik).

b. Pernyataan

Pernyataan dalam hal ini merupakan berbagai informasi yang disajikan oleh pihak yang terlibat, dimana hal tersebut dapat diperiksa atau dicocokkan dengan bukti digital. Contohnya pada penyelidikan pembunuhan Soham, pernyataan (alibi) pelaku dibantah ketika catatan ponsel dari pihak yang dia temui menunjukkan bahwa pada saat itu dia sedang berada di luar kota.

c. Tujuan

Adapun tujuan dari penyelidikan adalah menemukan bukti-bukti yang objektif terhadap suatu kasus kejahatan. Selain itu, penyelidikan juga dapat digunakan untuk membuktikan niat yang dalam istilah hukum disebut sebagai *mens rea*. Contohnya pada riwayat *internet* terhadap terpidana pembunuh Niel Entwistle yang merujuk pada situs yang membahas langkah-langkah membunuh orang.

d. Evaluasi Sumber

Dalam mendapatkan sumber yang terpercaya, penyelidik perlu melakukan evaluasi terkait sumber yang dijadikan acuan. Contohnya pada artefak-artefak dan metadata berkas yang dalam hal ini dapat digunakan

untuk melakukan identifikasi asal-usul dari bagian data tertentu. Detailnya seperti versi *Microsoft Word* yang lebih lama menyematkan *Global Unique Identifer* pada berkas-berkas yang dibuat dalam mengidentifikasi komputer, serta memastikan kemungkinan terkait berkas yang dibuat pada perangkat digital yang seang dalam proses pemeriksaan atau berkas yang didapatkan dari tempat lain.

e. Otentikasi Dokumen

Otentikasi dokumen dalam hal ini memiliki kaitan dengan evaluasi sumber, dimana metadata yang berhubungan dengan berkas-berkas digital dapat dengan mudah dimodifikasi. Seperti halnya dengan mengubah jam komputer, maka dapat berpengaruh pada tanggal pembuatan suatu berkas. Otentikasi dokumen juga memiliki hubugan dengan pendeteksian dan identifikasi pemalsuan pada hal tersebut secara rinci.

Selain memastikan berbagai hal dalam melakukan proses penyelidikan, tugas umum selama pemeriksaan forensik juga berkaitkan dengan mendeskripsikan data yang terenskripsi pada berbagai bentuk, mulai dari berkas atau folder yang terenkripsi serta komunikasi yang terenskripsi seperti pada surat elektronik, obrolan, bahkan pada *hard disk* yang telah dienkripsi dengan FDE. Jadi, penggunaan enkripsi ini merupakan salah satu keterbatasan atau penghalang utama dalam penyelidikan forensik. Selain itu, dengan adanya media peyimpanan SSD yang mengaktifkan teknologi TRIM juga menjadi hambatan dalam melakukan penyelidikan forensik dalam hal pemulihan data. Teknologi TRIM tersebut pada dasarnya membuat sebuah fungsi pada data yang telah dihapus dapat dimusnahkan secara permanen dari sistem operasi. Hal tersebut membuat pemulihan data sulit dilakukan. Namun tidak semua SSD memiliki fitur TRIM diaktifkan.

5.3 Pertimbangan Hukum

Pertimbangan hukum mengenai pemeriksaan media digital terdapat pada UU nasional dan internasional. Khusus penyelidikan perdata, UU dapat memberi batas terkait kemampuan analisis saat melakukan proses pemeriksaan. Sedangkan dalam penyelidikan pidana, UU nasional memberi batas dengan banyaknya informasi yang dapat disita. Contohnya pada penyitaan barang bukti di Inggris dengan penegak hukum yang diatur oleh *Police and Criminal Evidence Act 1984*. Selain itu, dengan keberadaan forensik ini membuat salah satu lembaga, yaitu IOCE bekerja untuk menetapkan standar internasional terhadap penyitaan barang bukti.

Pertimbangan hukum yang terkait dengan kejahatan komputer juga dapat mempengaruhi penyelidik forensik, seperti halnya terjadi di Inggris. Sehingga terdapat larangan akses *Computer Misuse Act 1990* yang mengatur larangan akses tanpa otorisasi pada materi komputer. Dengan adanya aturan tersebut, banyak penyidik sipil yang terbatas dalam mengakses kepentingan dibandingkan dengan penegak hukum.

Kemudian terdapat salah satu bidang digital forensik yang sebagian besar belum diputuskan oleh pengadilan, yaitu mengenai hak individu atas privasi. Lalu *Electronic Communications Privacy Act* di Amerika Serikat memberikan batasan kemampuan terhadap penegak hukum atau penyidik sipil dalam menyadap dan mengakses bukti-bukti yang diperlukan. UU tersebut membuat perbedaan antara komunikasi yang tersimpan, seperti arsip surat elektronik dengan komunikasi yang ditransmisikan, seperti VoIP. VoIP merupakan teknologi yang dapat melewatkan trafik suara, video, serta data berbentuk paket melalui jaringan IP. Selain itu, terkait dengan adanya serangan privasi dan lebih sulit dalam mendapatkan surat perintah, *Electronic Communications Privacy Act* juga memberi pengaruh terhadap kemampuan perusahaan dalam menyelidiki komputer dan

komunikasi karyawannya. Kemudian pada tahun 2000 M, kemampuan penegak hukum Inggris dalam melakukan penyelidikan forensik digital diatur oleh *Regulation of Investigatory Powers Act.*

5.3.1 Bukti Digital

Bukti digital merupakan sekumpulan data yang didapatkan dari semua jenis penyimpanan digital yang menjadi subjek untuk pemeriksaan forensik komputer. Berdasarkan hal tersebut, segala sesuatu yang membawa informasi digital dapat menjadi subjek untuk penyelidikan serta setiap pembawa informasi yang melakukan pemeriksaan terkait kepentingan harus dijadikan sebagai bukti. Menurut Pasal 5 UU No. 11/2008 tentang ITE, menyebutkan bahwa, "Informasi elektronik dan atau dokumen elektronik dan atau hasil cetaknya merupakan alat bukti hukum yang sah." Adapun contoh barang bukti digital, yaitu alamat *Email*, berkas *wordprocessor* atau *spreadsheet*, berkas gambar (JPEG, PNG, dan lain-lain), *bookmarks* penjelajah web, *cookies*, kalender, *to do list*, kode sumber perangkat lunak, dan lain sebagainya.

Dalam mengumpulkan data-data yang digunakan sebagai barang bukti legal yang semuanya diatur pada UU, diperlukan seorang pakar digital forensik yang harus benar-benar terlatih dan berpengalaman pada bidang tersebut. Saat bukti-bukti dipergunakan dalam pengadilan, bukti-bukti tersebut berada di bawah pedoman hukum yang sama seperti bentuk bukti lainnya. Seperti halnya *Federal Rules of Evidence Act* di Amerika Serikat digunakan untuk melakukan evaluasi diterima atau tidaknya bukti digital yang diajukan. Selain itu, bukti-bukti digital memiliki kaitan dengan dua permasalahan hukum, yaitu integritas dan keaslian. Dengan adanya integritas, sudah seharusnya tindakan menyita dan memperoleh media digital tersebut tidak ada unsur modifikasi atau mengubah bukti,

baik yang asli ataupun salinannya. Sedangkan keaslian dalam hal ini mengacu pada kemampuan dalam memberikan konfirmasi integritas asli. Contohnya pada media yang dicitrakan sesuai dengan bukti asli.

Selain itu, lembaga penegak hukum juga harus memiliki lacak yang tepat saat menangani bukti digital dan mampu memberi jaminan bahwa segala bukti yang digunakan untuk analisis forensik merupakan bukti yang tepat. Kemudian agensi juga harus mengambil tindakan preventif yang tepat ketika menangani bukti digital. Saat para penyidik mengumpulkan bukti melalui perangkat digital, terdapat kemungkinan ditemukan pula bukti yang terkait dengan kejahatan lain. Ketika dalam keadaan tersebut, penyidik perlu mendapatkan surat tugas kedua agar bukti dapat diterima saat dibawa ke pengadilan. Jadi, secara khusus dalam penanganan bukti digital sangat perlu diperhatikan agar menjadi alat bukti yang sah dan akurat, sebab bukti digital mudah tercemar baik disengaja maupun tidak disengaja. Terlebih data digital juga dapat diciptakan dengan mudah, seperti melakukan modifikasi dengan menambahkan data oleh penyidik yang dapat menyudutkan pemilik perangkat digital. Oleh sebab itu, diperlukan mekanisme yang dapat memastikan bahwa penyidik tidak dapat atau sulit dalam melakukan rekayasa terhadap data selama proses penyelidikan berlangsung. Adapun mekanisme yang dapat dilakukan untuk mengatasi kecurangan tersebut, seperti penggunaan *message digest* terhadap berkas yang akan dilakukan evaluasi serta penggunaan *tools* yang sudah disertifikasi. Selain itu, seorang ahli harus menerapkan metode yang terbukti andal secara ilmiah dalam mencari bukti-bukti digital, serta dapat memastikan bahwa kesimpulan-kesimpulan hasil penyelidikan didasarkan atas bukti faktual serta pengetahuan pada bidang terkait. Contohnya *Federal Rules of Evidence* di Amerika Serikat menyatakan bahwa seorang

saksi dikatakan memenuhi syarat sebagai ahli apabila bentuk pendapat atau lainnya meliputi:

a. Kesaksian yang didasarkan pada fakta atau data yang cukup.
b. Kesaksian merupakan produk dari kaidah-kaidah dan metode-metode yang dapat diandalkan.
c. Ahli telah menerapkan prinsip dan metode secara andal terhadap fakta-fakta kasus.

Pada proses penyelidikan dan penanganan barang bukti, memang terdapat banyak panduan khusus untuk melakukannya. Sebagai contoh lain seperti ponsel yang harus diletakkan dalam sebuah tempat layaknya sangkar selama penyitaan. Hal tersebut dilakukan untuk mencegah adanya lalu lintas radio lebih lanjut ke perangkat. Selain itu, ada juga pendekatan internasional dalam memberikan bantuan mengenai langkah-langkah menangani bukti elektronik, yaitu *Electronic Evidence Guide* oleh Dewan Eropa yang menawarkan kerangka kerja untuk penegak hukum dan otoritas pengadilan di negara-negara yang berusaha mengatur atau meningkatkan pedoman dalam melakukan identifikasi dan penanganan bukti elektronik.

5.3.2 Standar Daubert

Standar Daubert merupakan parameter yang berlaku untuk memastikan bahwa langkah-langkah dan perangkat lunak yang digunakan dalam memperoleh keberadaan bukti digital dapat diterima. Pada tahun 2003 M, dalam sebuah makalah Brian Carrier berpendapat bahwa pedoman Daubert mengharuskan kode pada alat-alat forensik dipublikasikan dan ditelaah oleh rekan penelitian. Brian membuat kesimpulan terkait peralatan dengan sumber yang terbuka mungkin lebih jelas dan komprehensif untuk memenuhi persyaratan pedoman

dibandingkan peralatan dengan sumber yang tertutup. Kemudian pada tahun 2011, Josh Brunty membuat pernyataan terkait validasi ilmiah pada teknologi serta perangkat lunak yang berhubungan dengan kegiataan pemeriksaan digital forensik sangat berperan penting dalam proses pengujian di laboratorium. Josh berpendapat bahwa ilmu digital forensik dilandasi oleh prinsip-prinsip suatu proses yang berulang, memilki bukti yang memadai atau berkualitas, serta dapat mempertahankan proses validasi, sehingga hal-hal tersebut dapat memenuhi syarat utama untuk setiap pemeriksa digital forensik dalam mempertahankan metode yang digunakan di pengadilan [33].

5.4 Alat Digital Forensik

Alat digital forensik berperan penting dalam membantu para penegak hukum selama proses penyelidikan. Alat tersebut dapat berupa perangkat keras dan perangkat lunak yang dapat membantu proses penyeldikan.

5.4.1 Perangkat Keras

Dalam menyelidiki perangkat penyimpanan serta menjaga agar perangkat target tidak berubah demi mempertahankan intergritas bukti, dirancanglah peralatan berupa perangkat keras. Salah satu contoh perangkat keras adalah FDC yang dapat dilihat pada gambar 5.1 sebagai berikut:

Gambar 5.1 FDC [34]

FDC adalah perangkat *read only* yang memungkinkan pengguna dapat membaca data pada perangkat tersebut tanpa risiko terjadi modifikasi atau menghapus konten yang ada di dalamnya. Kemudian terdapat juga perangkat yang berfungsi untuk menyalin berkas-berkas dan menduplikasi data secara aman. Perangkat tersebut adalah HDD *Duplicator* yang dapat dilihat pada gambar 5.2 sebagai berikut:

Gambar 5.2 HDD Duplicator [35]

5.4.2 Perangkat Lunak

Dengan adanya perangkat lunak forensik, penelitian dan investigasi yang dilakukan terhadap suatu kasus menjadi lebih akurat. Berdasarkan beberapa faktor seperti anggaran dan ahli yang tersedia, kepolisian dan lembaga penyelidikan memilih perangkat lunak forensik yang memiliki banyak fungsi serta dapat melakukan berbagai tugas dalam satu aplikasi. Berbagai aplikasi tersebut bersifat terbuka, sehingga kodenya dapat dimodifikasi dalam memenuhi kebutuhan secara spesifik serta hemat biaya bagi penegak hukum. Selain itu, terdapat juga beberapa perangkat yang dapat sekaligus mengelola berbagai sistem operasi, seperti *Windows* (sebuah sistem operasi yang dikembangkan oleh Microsoft, dengan menggunakan GUI) dan *Linux* (sistem operasi yang menganut sistem Unix dengan menggunakan model pengembangan serta distribusi perangkat lunak secara gratis). Berbagai perangkat lunak forensik yang tersedia ini dapat melengkapi perangkat keras yang sudah ada untuk kepentingan penegak hukum dalam memperoleh dan menganalisis bukti-bukti digital yang dikumpulkan melalui perangkat yang digunakan oleh tersangka. Meskipun dalam beberapa kasus tersangka sering menyembunyikan bahkan menghapus berkas pada komputer yang digunakan dengan tujuan agar bukti-bukti sulit ditemukan, namun dengan adanya aplikasi perangkat lunak forensik ini dapat membantu penyidik dalam memulihkan bukti-bukti tersebut, sebagaimana pemulihan dan penyelidikan terkait aktivitas pengguna tertentu dengan menggunakan perangkat lunak digital forensik. Adapun alat-alat forensik yang dimaksud, yaitu alat perekam data, alat penampil berkas, alat analisis data, alat analisis *registry*, alat analisis *internet*, alat analisis surat elektronik, alat analisis peranti bergerak, alat forensik jaringan, dan alat forensik basis data.

5.5 Cabang Forensik

Berdasarkan pengelompokkan tempat data disimpan atau proses data ditransisikan, terdapat lima cabang dari digital forensik sebagai berikut:

5.5.1 Forensik Komputer

Forensik komputer mencakup komputer, memori *onboard*, dan memori statis. Adapun tujuan dari forensik komputer ini adalah untuk menberikan penjelasan mengenai keadaan artefak digital yang ada dari cakupan tersebut. Forensik komputer juga bergantung pada sistem operasi yang digunakan. Seperti halnya kebanyakan pengguna komputer *desktop* menggunakan sistem operasi *Microsoft Windows*. Oleh sebab itu, kemampuan untuk melakukan forensik komputer dengan menggunakan sistem operasi *Microsoft Windows* sangat diperlukan. Apabila pengguna komputer menggunakan sistem operasi yang lain, tentu peletakan data pada berkas yang berbeda menggunakan format yang berbeda pula. Contohnya pada sistem Unix, terdapat catatan yang tersedia pada layanan *syslog*. Sedangkan pada *Microsoft Windows*, catatan seperti itu dapat dilihat menggunakan *Event Viewer.*

Selain itu, forensik komputer juga dapat menangani berbagai informasi dari *log*, seperti riwayat *internet* hingga ke berkas yang sebenarnya ada dalam *drive*. Seperti pada tahun 2006 M, seorang pembunuh Sharon Lopatka berhasil diidentifikasi setelah pesan *Email* dari pembunuh tersebut berisi tentang penyiksaan dan kematian yang ditemukan di komputer Sharon. Lalu pada tahun 2007 M, seorang jaksa pernah menggunakan *spreadsheet* yang dipulihkan dari komputer milik Joseph E. Duncan III dalam mengungkapkan kasus pembunuhan terencana dan memperkuat hukuman mati.

5.5.2 Forensik Peranti Bergerak

Forensik peranti bergerak merupakan salah satu cabang digital forensik yang berhubungan dengan pemulihan bukti digital atau data dari perangkat seluler yang memiliki sistem komunikasi yang terintegrasi, seperti GSM serta dengan mekanisme penyimpanan *proprietary*. Namun investigasi biasanya lebih berfokus pada data yang sederahana, seperti data panggilan dan komunikasi berupa SMS atau *Email* daripada pemulihan mendalam dari pada yang dihapus. Hal tersebut telah terbukti dapat membantu membebaskan Patrick Lumumba dari kasus pembunuhan Meredith Kercher berdasarkan investigasi perangkat seluler melalui data SMS. Perangkat seluler juga menyediakan informasi berupa lokasi, baik dari pelacakan GPS internal atau melalui tower seluler. Hal tersebut telah digunakan pada tahun 2006 M untuk melacak para penculik Thomas Onofri.

5.5.3 Forensik Jaringan

Dalam hal ini, forensik jaringan memiliki kaitan dengan proses pengamatan dan analisis lalu lintas jaringan komputer, baik secara LAN (jaringan komputer dengan cakupan jaringan pada wilayah yang kecil, seperti jaringan komputer gedung, kampus, kantor, sekolah, dan ruangan) maupun WAN (jaringan komputer yang menjangkau area yang lebih luas, seperti jaringan komputer antar daerah, kota, bahkan negara.. Forensik jaringan berfungsi untuk keperluan dalam hal mengumpulkan informasi, bukti, serta deteksi intrusi. Seperti pada tahun 2000 M, FBI mengumpan peretas komputer Aleksey Ivanov dan Gorshkov ke Amerika Serikat untuk wawancara kerja palsu. Dengan melakukan pengawasan lalu lintas jaringan dari masing-masing komputer tersebut, FBI berhasil

mengidentifikasi kata sandi untuk mengumpulkan bukti-bukti langsung dari komputer.

5.5.4 Forensik Basis Data

Forensik basis data merupakan digital forensik yang berhubungan dengan studi forensik basis data dan metedata. Forensik basis data ini memilki fungsi untuk membuat garis waktu atau memulihkan informasi yang relevan. Hal tersebut dapat dilakukan dengan cara melakukan investigasi menggunakan isi basis data, berkas *log*, dan data dalam RAM.

5.5.5 Analisis Data Forensik

Salah satu cabang digital forensik yang berperan dalam menguji data adalah analisis data forensik. Data yang terstruktur diuji dengan tujuan untuk menemukan dan menganalisis beragam bentuk kegiatan penipuan yang dihasilkan seperti pada kasus kejahatan keuangan [33].

6. IT Forensik

6. IT Forensik

6.1 Keberadaan IT Forensik

Dengan perkembangan zaman yang semakin cepat, membuat masyarakat konvensional beralih menjadi masyarakat digital. Peralihan tersebut tentu menimbulkan beragam dampak, mulai dari peluang usaha hingga muncul jenis kejahatan yang lebih canggih. Berdasarkan hal tersebut, perlu adanya seorang IT forensik yang sudah memiliki hak dan privasi yang dilindungi oleh UU agar mampu mengusut tuntas berbagai kejahatan yang timbul serta mencari barang bukti untuk menyelesaikan berbagai kasus walaupun kejahatan dalam dunia digital tentu memiliki tantangan yang berbeda dibandingkan pada dunia nyata. Seperti halnya pada dunia nyata, suatu kejadian yang telah berlangsung tidak dapat di reka ulang, namun pada dunia digital, hal tersebut dapat dimunculkan kembali untuk dijadikan bukti otentik dalam penyelesaian suatu kasus.

Keistimewaan IT forensik secara sederhana dalam menganalisa data dapat dicontohkan pada salinan berkas. Apabila satu berkas pada *Microsoft Word* disalin dari satu folder ke folder lain, perbandingan akan salinan tersebut dapat dilihat pada *properties* masing-masing berkas, dimana pada bagian tersebut akan jelas terlihat perbedaan informasi dari berkas *created, modified,* dan *accessed*. Hal tersebut menandakan bahwa berkas tidak dianggap otentik lagi sebab sudah ada perubahan atau perbedaan dari kondisi awal. Jadi, seorang IT forensik secara sederhananya mampu mengambil data untuk dianalisa akan kebenaran otentiknya atau persis sama sesuai dengan aslinya.

6.2 Kunci Utama IT Forensik

Adapun hal yang harus diperhatikan berkaitan dengan bukti-bukti digital dalam elemen forensik adalah sebagai berikut:

a. Identifikasi dalam bukti digital

Kunci utama dalam IT forensik adalah melakukan identifikasi. Dalam hal ini dilakukan identifikasi terhadap keberadaan bukti terkait dimana bukti itu disimpan dan bagaimana penyimpanannya agar penyelidikan dapat lebih mudah dilakukan.

b. Penyimpanan bukti digital

Penyimpanan bukti digital hendaknya disimpan dalam tempat yang steril serta benar-benar dipastikan tidak ada perubahan mulai dari bentuk, isi, dan makna digital. Jika keberadaan bukti digital tidak teliti, maka bukti tersebut akan mudah rusak, hilang, berubah, bahkan mengalami kekacauan. Hal tersebut dikarenakan bukti digital memiliki sifat sementara. Apabila terdapat sedikit saja perubahan dalam bukti digital, hal tersebut akan merubah juga hasil penyelidikan. Jadi, dalam melakukan proses penyimpanan bukti digital harus dalam kehati-hatian agar tidak bukti-bukti yang telah dikumpulkan tetap orisinal.

c. Analisa Bukti Digital

Analisa bukti digital merupakan proses pengecekan ulang barang bukti sebelum diserahkan kepada pihak yang berwenang. Skema yang diperlukan dalam proses ini bersifat fleksibel sesuai dengan kasus yang dihadapi. Adapun beberapa poin yang perlu dicek kembali terkait dengan tindak pengusutan, seperti apa yang yang telah dilakukan, siapa yang telah melakukannya, proses apa yang dihasilkan, dan kapan hal tersebut dilakukan. Kemudian setiap bukti yang telah ditemukan hendaknya dikelompokkan pada bukti-bukti potensial apa saja yang dapat didokumentasikan.

d. Presentasi Bukti Digital

Presentasi bukti digital yang akan dilakukan di pengadilan merupakan langkah akhir atas semua kesimpulan yang didapatkan selama tahapan penyelidikan dilakukan. Bukti-bukti yang telah dikumpulkan akan menjadi modal pening untuk dibawa ke pengadilan. Setelah bukti-bukti tersebut disajikan, bukti tersebut akan masuk pada tahap proses digital, dimana bukti digital akan dipersidangkan, diuji otentikasi, serta dikorelasikan dengan kasus-kasus yang ada. Tahapan ini merupakan tahap terpenting dikarenakan pada tahap inilah proses-proses yang telah dilakukan sebelumnya akan dijelaskan kembali secara benar dan kebenaran tersebut harus dibuktikan kepada hakim agar dapat mengungkapkan data dan informasi akan suatu kejadian [36].

7. Contoh Kasus Forensik

7. Contoh Kasus Forensik

- Pada hari Rabu tanggal 6 Januari 2016 bertempat di Restaurant Olivier, West Mall, Ground Floor, Grand Indonesia, Kebon Kacang, Tanah Abang, Jakarta Pusat, kasus kematian Wayan Mirna Salihin menjadi perhatian publik. Wanita berusia 27 tahun itu dinyatakan keracunan setelah minum segelas es kopi Vietnam yang mengandung senyawa sianida. Pada saat itu, Mirna ditemani oleh rekannya yang bernama Jessica Kumala Wongso dan Hani. Kasus kematian Mirna ini diambil alih oleh Otoritas Polda Metro Jaya, Polres Jakarta Pusat yang menyatakan bahwa secara kimia, di dalam tubuh Mirna terdapat senyawa sianida yang mengikis jaringan organ. Kemudian, jenazah Mirna dibawa ke Rumah Sakit Polri, Jakarta, untuk dilakukan autopsi oleh Tim forensik. Ternyata zat korosif tersebut bereaksi setelah Mirna mencecap kopi ditandai dengan tubuh Mirna yang menegang dan mulut Mirna yang mengeluarkan buih. Kepolisian lantas menggelar prarekontruksi di Restoran Olivier serta melibatkan Tim INAFIS dan Tim Laboratorium Forensik dari Markas Besar Polri. Salah satu adegan pada prarekonstruksi tersebut memperlihatkan reaksi Mirna yang terkejut usai meminum kopi yang dipesannya. Usai prarekonstruksi, kepolisian membawa sejumlah barang bukti dari Restoran Olivier untuk dilakukan penyelidikan lebih lanjut, antara lain CCTV serta beberapa peralatan untuk menyeduh kopi Vietnam yang diteguk Mirna. Berdasarkan hasil olah TKP dan pemeriksaan saksi, polisi menetapkan Jessica Kumala Wongso sebagai tersangka serta dijerat dengan pasal 340 KUHP tentang pembunuhan berencana [37].

- Pada tanggal 1 Januari 2002 M, Scott Tyree menculik seorang gadis berusia 13 tahun bernama Alicia Kozakewicz. Pada malam yang sama, Tyree mengirim foto Alicia yang diikat di ruang bawah tanahnya melalui *Yahoo Messenger* kepada seseorang di Tampa, FL. Pria dari Tampa itu kebetulan memeriksa situs Pittsburgh Post Gazette dan melihat bahwa gadis yang sama hilang dari rumahnya. Dia kemudian menghubungi FBI pada tanggal 3 Januari dan memberi FBI nama layar *Yahoo* dari orang yang mengiriminya IM: "masterforteenslavegirls." Setelah itu FBI menghubungi *Yahoo* dan mendapatkan alamat IP darimana gambar itu dikirim. Mereka kemudian menghubungi Verizon untuk mendapatkan nama dan alamat pelanggan Verizon kepada siapa alamat IP diberikan. Orang itu adalah Scott Tyree.

- Pada bulan Februari 2009 M, James Cameron dinyatakan dengan 16 dakwaan terkait perdagangan pornografi anak. Dugaan dibuat antara bulan Juli 2006 dan bulan Januari 2008. Cameron telah mengunggah pornografi anak ke album foto *Yahoo* menggunakan berbagai nama samaran. *Yahoo* juga melaporkan menemukan banyak gambar pornografi anak pada bagian foto akun *Yahoo*. Setelah itu, Polisi Negara bagian Maine melakukan penyelidikan dan mengidentifikasi pemilik akun tersebut adalah Barbara Cameron yang merupakan istri dari James Cameron. Lalu pada 21 Desember 2007 M, surat perintah penggeledahan dieksekusi dan empat komputer disita. Setelah diperiksa, pornografi anak ditemukan bersama dengan percakapan dimana orang tersebut mengidentifikasi dirinya sebagai pria yang sudah menikah berusia 45 tahun dengan seorang anak perempuan serta deskripsi yang cocok sebagai Cameron [38].

GLOSARIUM

M (Masehi)	2
SM (Sebelum Masehi)	3
GSR (Galvanic Skin Response)	5
FBI (Federal Bureau of Investigation)	12
AFIS (Automated Fingerprint Identification System)	12
CART (Computer Analysis and Respons Team)	12
DNA (Deoxyribonucleic Acid)	12
IOCE (International Organization on Computer Evidence)	13
US (United States)	13
UU (Undang-Undang)	15
SOCA (Serious Organised Crime Agency)	16
ISO (International Organization for Standardization)	17
DIBS (Digital Indirect Bonding System)	19
FTK (Forensic Tool Kit)	19
TKP (Tempat Kejadian Peristiwa)	22
IAI (International Association of Identification)	32
AAFS (American Academy of Forensic Science)	35
FTIR (Fourier Transform Infra Red)	37
PGM (Phosphoglucomutase)	37
ESD (Esterase D)	37
GLO (Glyoxylase)	37
RLFP (Restriction Fragment Length Polymorphism)	38
PCR (Polymerase Chain Reaction)	38
HLA DQA (Heterodimer Consisting of an Alpha Human Leukocyte Antigen)	38

INDEX

DAFTAR PUSTAKA

[1] Yi, Liang. 2005. "Sejarah Penemuan Buku Forensik". http://en.chinaculture.org/created/2005-08/01/content_71484.htm.

[2] Agrawal, Anil dan Munroe, Richard. "History of Forensic". http://www.crimezzz.net/forensic_history/index.htm.

[3] Hoiriyah. "Historical Perkembangan Forensik", Universitas Islam Indonesia.

[4] Anonim. The History and Development of Forensic Science History Essay. 2015. www.ukessays.com/essays/history/the–history–and development-of-forensic-science-history-essay.php.

[5] Anonim. 2015. "The History of Fingerprint". www. onin. com / fp / fphistory. html.

[6] Brunty, Josh. 2011. "Validation of Forensic Tools and Software: A Quick Guide for the Digital Forensic Examiner".

[7] Carrier, Brian. 2001. "Defining Digital Forensic Examination and Analysis Tools". Digital Research Workshop II.

[8] Carrier, Brian. 2002. "Open Source Digital Forensic Tools: The Legal Argument".

[9] Sack, Harald. 2014. "Ambroise Pare". http://scihi.org/ambroise-pare.

[10] Carrier, Brian. 2006. "Basic Digital Forensic Investigation Concepts".

[11] Auboisdormant. 2016. "Sir Thomas Browne". https://books.discogs.com/credit/78669-sir-thomas-browne.

[12] Wikipedia. 2018. "Mercello Malphigi". https://id.wikipedia.org/wiki/Marcello_Malpighi.

[13] Encyclopaedia Britannica. 2019. “Karl Wilhelm Scheele”. https://www.britannica.com/biography/Carl-Wilhelm-Scheele.

[14] Wikipedia. 2019. “Tokoh Mathieu Joseph Bonaventure Orfila”. https://en.wikipedia.org/wiki/Mathieu_Orfila.

[15] Filearm Examiner Training. “Henry Goddard”. https://projects.nfstc.org/firearms/module02/fir_m02_t04.htm.

[16] Wikipedia. 2019. “Karl Landsteiner”. https://id.wikipedia.org/wiki/Karl_Landsteiner.

[17] Casey, Eoghan. 2004. “Digital Evidence and Computer Crime”. Academic Press.

[18] Casey, Eoghan. 2009. “Handbook of Digital Forensics and Investigation”. Academic Press.

[19] Council of Europe. 2013. “Electronic Evidence Guide”.

[20] Du, Xiaoyu, Le-Khac, Nhien-An, & Scanlon, Mark. 2017. “Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service”. 16 th European Conference on Cyber Warfare adn Security. University Colleger Dublin.

[21] Pratama, Eka & Agus, I Putu. 2017. “Digital Forensic pada Cyber Crime”. Scientific News Magaxine Udayana. Bali: Universitas Udayana.

[22] Federal Evidence Review. 2015. “Federal Rules of Evidence: Rule 702. Testimony by Expert Witnesses”.

[23] Garfinkel, Simson L. 2010. “Digital Forensic Research: The Next 10 years”. Digital Investigation.

[24] Hoelz, Bruno, W.P, Ralha, Celia, & Geeverghese, Rajiv. 2009. “Artificial Intelligence Applied to Computer Forensic”. Proceedings of the 2009 ACM Symposium on Applied Computing. New York: ACM, Inc.

[25] Horenbeeck, Maarten Van, 2006. “Technology Cirme Investigation”.

[26] Horenbeeck, Maarten Van, 2006. “Technology Crime Investigation: Mobile Forensic”.

[27] Feri, S. 2008. “Komputer Forensik”, Jakarta: PT. Elex Media Komputindo.

[28] Abdussalam. 2006. “Forensik”, Jakarta: Restu Agung.

[29] Perdana Kusuma, M. 1984. “Kedokteran Forensik”, Jakarta: Ghalia Indonesia.

[30] Anonim. 2019. Digital Forensic Cases. https:// resources.infosecinstitute.com/category/computerforensics/introduction/notable-computer-forensics-cases.

[31] Encyclopaedia Britannica. 2020. “Tokoh Francis Galton”. https://www.britannica.com/biography/Francis-Galton.

[32] Alchetron. 2018. “Eoghan Casey”. https://alchetron.com/Eoghan-Casey.

[33] Wikipedia. 2019. “Teori tentang Digital Forensik”. https://id.wikipedia.org/wiki/Forensik_digital.

[34] Wikipedia. 2017. “Forensics Disk Controller”. https://en.wikipedia.org/wiki/Forensic_disk_controller.

[35] Storage Heaven. 2019. “Hard Disk Duplication”. https://www.storageheaven.com/FX2042-HDD-Duplicator-p/y 2042.htm.

[36] Digital Munition. 2019. “Tahapan Forensik”. https://www.digitalmunition.me/computer-forensic-investigation-process-cissp-free-by-skillset-com.

[37] Sasongko, Joko Panji. 2016. “Kasus Mirna Hingga Penahanan Jessica”.https://www.cnnindonesia.com/nasional/20160201085309-12-107972/kronologi-kasus-mirna-hingga-penahanan-jessica.

[38] Infosec. 2019. “Kasus Digital Forensik”. https://resources.infosecinstitute.com/category/computerforensics/introduction/notable-computer-forensics-cases/#gref.

Turnitin Originality Report

Processed on: 04-Mar-2020 16:23 WIB
ID: 1269051037
Word Count: 13467
Submitted: 1

buku ajar image forensik By Rossi Passarella

Similarity Index	Similarity by Source	
27%	Internet Sources:	26%
	Publications:	1%
	Student Papers:	5%

12% match (Internet from 22-Dec-2019)
https://id.wikipedia.org/wiki/Forensik_digital

4% match (Internet from 15-Jan-2019)
https://adoc.site/download/sejarah-perkembangan-forensik-dan-digital-forensik--a5b31ea8d53a5e

2% match (Internet from 11-Jun-2019)
https://emmun.wordpress.com/tag/forensics/page/2/

1% match (Internet from 30-May-2016)
http://www.senenkliwon.com/sejarah-forensik-dan-perkembangan-forensik-digital-2327.html

1% match (Internet from 06-May-2019)
https://forensikdigital.com/digital-forensik/

1% match (Internet from 12-Jun-2019)
https://encarnados.blogspot.com/2018/11/kumpulan-contoh-kata-pengantar-buku.html

1% match (Internet from 02-Dec-2019)
https://surabayarumahkusurgaku.blogspot.com/2018/08/digital-forensic.html

1% match (Internet from 21-Jan-2020)
http://adrianhertanto.blogspot.com/

< 1% match (Internet from 25-Dec-2019)
https://traintoforensik.wordpress.com/

< 1% match (Internet from 31-Mar-2019)
http://pakmoko.blogspot.com/2014/07/run-down-sejarah-forensik.html

< 1% match (Internet from 05-Nov-2019)
http://eprints.ums.ac.id/61929/13/BAB%20I.pdf

< 1% match (Internet from 19-Apr-2017)
http://www.forensictv.net/Downloads/forensic_science/forensic_science_timeline_by_norah_rudin_and_keith_inman.pdf

< 1% match (Internet from 13-Mar-2019)
http://septianzeroes.blogspot.com/2018/03/resume-jenis-jenis-jaringan-komputer_18.html

< 1% match (Internet from 22-Jul-2019)
https://es.scribd.com/document/384195243/Profil-Kesehatan-Kotim-2016-pdf

< 1% match (student papers from 15-Apr-2019)
Submitted to Indiana University on 2019-04-15

< 1% match (Internet from 13-Feb-2020)
https://es.scribd.com/doc/285007023/Dna

< 1% match (Internet from 18-Jan-2020)
http://docshare.tips/siegel-knupfer-saukko-encyclopedia-of-forensic-sciences-academic-press-2000_58c442d5b6d87f4a418b5b77.html

“Hadirnya buku ini memberikan banyak ilmu pengenalan untuk pemula ataupun mereka yang sedang tertarik dengan ilmu forensik terutama di citra forensik. Buku ini disajikan dengan tegas dan mudah dimengerti oleh pembaca yang disertai dengan beberapa contoh kasus pada citra forensik. Karenanya, seorang periset dan praktisi di bidang citra forensik akan merugi dengan tidak membaca buku ini.”

Dr. Deris Stiawan. CE|H, CH|FI
Peneliti dan pengamat bidang keamanan cyber UNSRI

Perkembangan teknologi yang terus meningkat di bidang citra digital, membuat manusia harus mampu mengikuti kemajuan yang ada dalam memenuhi kebutuhan hidupnya. Hal ini juga memilki dampak terhadap kasus kejahatan digital yang ikut berkembang, sehingga perlu adanya teknik untuk memudahkan dalam memecahkan permasalahan yang ada, yaitu dengan digital forensik. Sejak zaman pra-sejarah hingga sekarang, teknik tersebut terus berkembang seiring dengan berbagai permasalahan yang semakin signifikan. Dengan perkembangan teknik digital forensik yang lebih baik, hal tersebut mampu memberikan keakuratan data dan dapat digunakan sebagai barang bukti yang mendukung terhadap penuntunan berbagai kasus pada proses pengadilan. Langkah-langkah yang dilakukan dalam menyelesaikan suatu permasalahan dengan teknik digital forensik terbilang kompleks karena harus mengikuti berbagai prosedur serta mendapat dukungan dari berbagai ahli forensik. Maka dari itu, mulai dari perkembangan forensik, alur kerja forensik, hingga contoh kasus forensik dapat dipelajari lebih lanjut melalui buku ini.

ISBN 978-979-587-861-2
9 789795 878612