PENANGANAN BUKTI DIGITAL

Oleh : 516-KUNDANG K JUMAN

Modul : 3

PENDAHULUAN

Latar Belakang

Memasuki abad 21, Teknologi Informasi merupakan bagian yang tak terpisahkan disetiap lini kehidupan di pelbagai kalangan masayrakat. Pertumbuhan bidang Teknologi Informasi khususnya di Indonesia yang pesat dapat dirasakan dengan meningkatnya angka pengguna *gadget*. Data dari Emarketer melaporkan bahwa Indonesia merupakan salah satu negara yang mempunyai pertumbuhan terbesar, di bawah China dan India. Berdasarkan laporan yang sama, Indonesia pun akan melampaui 100 juta pengguna *smartphone* aktif pada tahun 2018, serta akan menjadikan Indonesia dengan populasi pengguna *smartphone* terbesar keempat didunia.

Selain dari pada itu, hal yang dapat kita rasakan sebagai akibat dari poin yang telah disebutkan adalah Digitalisasi. Kemajuan teknologi akan berbanding lurus dengan masifnya digitalisasi. Hal ini dikarenakan digitalisasi membutuhkan dukungan elektronik atau komputer didalamnya.

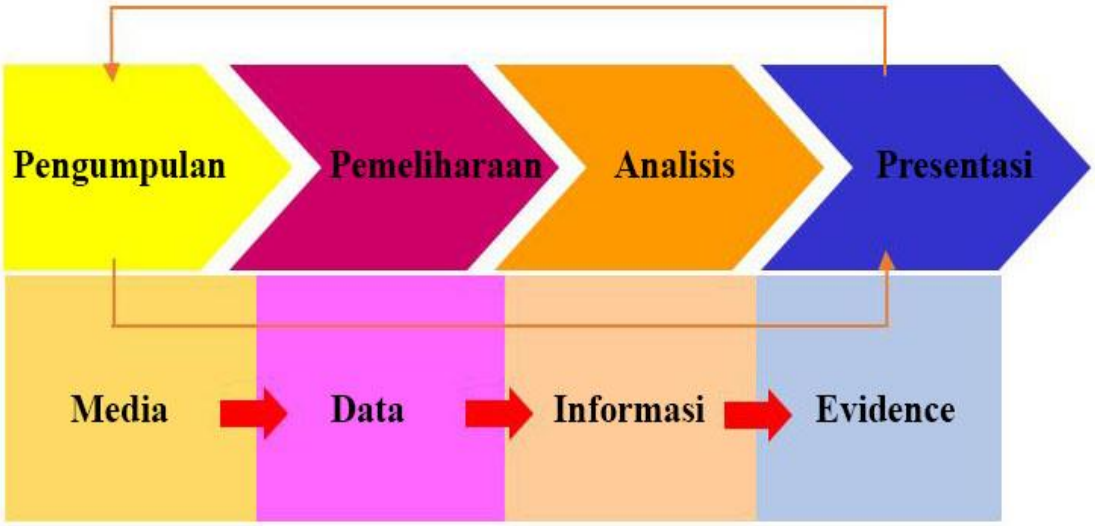
Merambahnya digitalisasi ke hamper setiap bidang dalam kehidupan menjadikan terjadinya distorsi gaya hidup manusia masa kini. Yakni, terdapat peran teknologi disetiap harinya, baik yang membantu meringankan pekerjaan manusia, hingga yang menjadikan candu atau bahkan yang dijadikan media kejahatan. Hal ini berarti, tindak kejahatan pun telah memanfaatkan peranan teknologi informasi. Baik tindak kejahatan yang berhubungan dengan dunia maya atau pun tindak kriminalitas seperti pembunahan, penculikan, dll.

Dalam pengungkapan kasus-kasus tindak kejatan yang memanfaat kan teknologi tersebut akan menghasilkan bukti digital. Bukti-bukti digital ini yang akan berpengaruh untuk melihat rekam jejak tindak kejahatan tersebut.

Berdasarkan pada penjelasan diataslah yang melatar belakangi penulis untuk menulis makalah yang berjudul Penanganan Bukti Digital ini.

Forensik Digital

Bicara mengenai Barang Bukti Digital beserta tindak kejahatan yang dilakukan, maka tidak lepas dari bidang ilmu Forensik Digital. Menurut Dr Edmond Locard, Istilah Forensik berasal dari bahasa yunani yaitu “Forensis” yang berarti debat atau perdebatan merupakan bidang ilmu pengetahuan yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu (sains). Prinsip dasar ilmu forensik dipelopori oleh Dr Edmond Locard. Ia berspekulasi bahwa setiap kontak yang Anda buat dengan orang lain, tempat, atau hasil objek dalam pertukaran materi fisik. Ini dikenal sebagai Locar exchange principle . Ini pertukaran materi fisik dapat dapat digunakan untuk membuktikan tidak bersalah seseorang atau bersalah di pengadilan hukum. Saat ini ilmu forensic semakin luas, diantaranya adalah forensic digital.Digital forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti digital dalam kejahatan computer. Istilah ini relatif baru dalam bidang komputer dan teknologi, tapi telah muncul diluar term teknologi (berhubungan dengan investigasi bukti-bukti intelijen dalam penegakan hukum dan militer) sejak pertengahan tahun 1980-an.Sebelum tahun 1980-an kejahatan yang melibatkan komputer ditangani dengan ketentuan hukum yang ada. Kejahatan komputer pertama kali diakui dalam Undang-Undang Pidana Komputer Florida 1978 (*the 1978 Florida Computer Crimes Act*) termasuk undang-undang yang melarang modifikasi tidak sah atau penghapusan data pada sistem komputer. Pada tahun-tahun berikutnya, ruang lingkup *cybercrime* mulai berkembang, dan beberapa undang-undang kemudian disahkan untuk mengatasi permasalahan hak cipta, privasi/pelecehan (misalnya intimidasi dunia maya, *cyber stalking*, dan predator daring) serta pornografi anak. Baru pada tahun 1980-an undang-undang federal mulai memasukkan pelanggaran komputer. Kanada adalah negara pertama yang mengeluarkan undang-undang terkait kejahatan



Gambar 1. Prosesforensik digital

komputer pada tahun 1983. Hal ini diikuti oleh Amerika Serikat dengan *Computer Fraud and Abuse Act* pada tahun 1986, Australia mengamandemen undang-undang kriminalnya pada tahun 1989 dan Inggris menerbitkan Undang-Undang Penyalahgunaan Komputer (*Computer Misuse Act*) pada tahun 1990. Dalam suatu model forensik digital melibatkan tiga komponen terangkai yang dikelola sedemikian rupa sehingga menjadi sebuah tujuan akhir dengan segala kelayakan serta hasil yang berkualitas. Ketiga komponen tersebut adalah:

1. Manusia (*People*), diperlukan kualifikasi untuk mencapai manusia yang berkualitas. Memang mudah untuk belajar komputer forensik, tetapi untuk menjadi ahlinya, dibutuhkan lebih dari sekadar pengetahuan dan pengalaman.
2. Peralatan (*Equipment*), diperlukan sejumlah perangkat atau alat yang tepat untuk mendapatkan sejumlah bukti yang dapat dipercaya dan bukan sekadar bukti palsu.

3. Aturan (*Protocol*), diperlukan dalam menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat. Dalam komponen aturan, diperlukan pemahaman yang baik dalam segi hukum dan etika, kalau perlu dalam menyelesaikan sebuah kasus perlu melibatkan peran konsultasi yang mencakup pengetahuan akan teknologi informasi dan ilmu hukum.

Karena luasnya lingkup yang menjadi objek penelitian dan pembahasan digital forensik maka ilmu digital forensik dibagi kedalam beberapa bagian yaitu:

1. Komputer Forensik

   Tujuan dari komputer forensik adalah untuk menjelaskan keadaan saat ini artefak digital, seperti sistem komputer, media penyimpanan atau dokumen elektronik. Disiplin biasanya meliputi komputer, embedded system (perangkat digital dengan daya komputasi dasar dan memori onboard) dan statis memori (seperti pen drive USB). Forensik komputer dapat menangani berbagai informasi, mulai dari log (seperti sejarah internet) melalui file yang sebenarnya di drive.
2. Forensik Perangkat Mobile

   Forensik perangkat mobile merupakan cabang sub-forensik digital yang berkaitan dengan pemulihan bukti digital atau data dari perangkat mobile. Ini berbeda dari Komputer forensik dalam perangkat mobile akan memiliki sistem komunikasi inbuilt (misalnya GSM) dan biasanya, mekanisme penyimpanan proprietary. Investigasi biasanya fokus pada data sederhana seperti data panggilan dan komunikasi (SMS / Email) daripada mendalam pemulihan data yang dihapus. Perangkat mobile juga berguna untuk memberikan informasi lokasi, baik dari gps inbuilt / lokasi pelacakan atau melalui situs sel log, yang melacak perangkat dalam jangkauan mereka.
3. Jaringan Forensik

Jaringan forensik berkaitan dengan pemantauan dan analisis jaringan komputer lalu lintas, baik lokal dan WAN / internet, untuk tujuan pengumpulan informasi, pengumpulan bukti, atau deteksi intrusi.Lalu Lintas biasanya dicegat pada paket tingkat, dan baik disimpan untuk analisis kemudian atau disaring secara real-time. Tidak seperti daerah lain jaringan data digital forensik sering stabil dan jarang login, membuat disiplin sering reaksioner.

4. Forensik Database

   Forensik database adalah cabang dari forensik digital yang berkaitan dengan studi forensik database dan metadata mereka.Investigasi menggunakan isi database, file log danRAM data untuk membangun waktu-line atau memulihkan informasi yang relevan

Forensik Digital di Indonesia

Indonesia telah memiliki Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang mengatur perbuatan-perbuatan yang dilarang serta ancaman pidananya. Menurut Rudiantara, TIK di Indonesia berkembang pesat Indonesia sehingga perlu diimbangi dengan kemampuan forensik digital. Kementerian Kominfo mendukung baik pembentukan Asosiasi Forensik Digital Indonesia, mengingat jumlah personil ahli forensik digital yang terbatas sedangkan kasus *cyber crime* di Indonesia sangat banyak. Setelah melalui diskusi yang cukup intensif antar beberapa pihak penggiat forensik digital di Indonesia, akhirnya secara resmi pada tanggal 17 November 2015 bertempat di Ruang Serbaguna Kominfo telah di bentuk Asosiasi Forensik Digital Indonesia (AFDI). Tujuan mulia dari AFDI ini adalah untuk menjadi rumah besar bagi para penggiat forensik digital di Indonesia, baik yang sifatnya profesional maupun akademik. Secara garis besar Tujuan dari pendirian AFDI ini adalah sbb:

1. Menghimpun dan mengkoordinir para analis dan peminat forensik digital dalam suatu wadah Asosiasi sehingga menghasilkan manfaat

untuk kemajuan anggota Asosiasi itu sendiri maupun bagi bangsa dan negara.

2. Memberikan edukasi dan sosialisasi tentang forensik digital kepada masyarakat Indonesia.
3. Menjadi referensi bagi antar anggota Asosiasi untuk memahami, mengerti dan menambah wawasan/pengetahuan tentang seluk beluk forensik digital.
4. Menjadi sarana komunikasi, sarana tukar informasi dan interaksi anggota Asosiasi sehingga mampu mengakselerasi perkembangan dan penerapan forensik digital di Indonesia.
5. Menjalin hubungan profesional dengan stakeholder lain termasuk menjadi mitra kritis dan konstruktif bagi pemerintah.
6. Menyusun dan mengembangkan standar kompetensi analis forensik digital, standar mutu hasil pemeriksaan/analisa forensik digital, dan kode etik profesi analis forensik digital di Indonesia.
7. Membantu proses akreditasi ISO untuk laboratorium-laboratorium forensik digital di Indonesia.
8. Mendukung pengembangan solusi teknologi berupa hardware dan software dalam negeri di bidang forensik digital.

Barang Bukti Digital

Gambar 2 Contoh Barang Bukti Digital

Menurut Kavrestad, Bukti digital adalah data-data yang dikumpulkan dari semua jenis penyimpanan digital yang menjadi subjek pemeriksaan forensik komputer. Dengan demikian segala sesuatu yang membawa informasi digital dapat menjadi subjek penyelidikan, dan setiap pembawa informasi yang ditargetkan untuk pemeriksaan harus diperlakukan sebagai bukti.

Menurut Zuhri, Evidence yang dimaksud dalam kasus forensik pada umumnya tidak lain adalah informasi dan Evidence.Menurut salah satu ahli forensik Indonesia Muhammad Nuh, beberapa klasifikasi barang bukti digital forensic yaitu:

1. Barang Bukti Elektronik

Barang bukti ini bersifat fisik dan dapat dikenali secara visual, sehingga data. Cara pandangnya sama saja, tetapi dalam kasus komputer forensik, kita mengenal subjek tersebut sebagai Digital investigator dan analis forensic harus sudah memahami barang bukti tersebut ketika sedang melakukan proses pencarian barang bukti di TKP.

Contoh dari barang bukti elektronik fisik adalah seperti:

1. Komputer pc, *laptop*, *netbook*, *tablet*
2. Handphone, smartphone
3. Flashdisk/thumb drive
4. Floppydisk
5. Harddisk
6. Cd/dvd
7. Router, switch, hub
8. Kamera video, cctv
9. Kamera digital
10. Digital recorder
11. *Music/video player*, dan lain-lain

2. Barang Bukti Digital

Barang bukti digital bersifat digital yang diekstrak dari barang bukti elektronik. Di dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah *informasi elektronik dan dokumen elektronik*.

Berikut contoh barang bukti digital (informasi/dokumen elektronik) :

1. Logical file
2. Deleted file
3. Lost file
4. File slack
5. Log file
6. Encrypted file

a. Steganography file
b. Office file
c. Audio file
d. Video file
e. Image file
f. Email
g. User id dan password
h. Sms (short message service)
i. Mms (multimedia message service)
j. Call logs : incoming, outgoing & missed

Rules of evidence merupakan sebuah pengaturan barang bukti dimana barang bukti harus memiliki keterkaitan dengan kasus yang diinvestigasi dan memiliki kriteria sebagai berikut:

1. Layak dan dapat diterima (Admissible)

   Artinya barang bukti yang diajukan harus dapat diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai ke pengadilan.
2. Asli (Authentic)

   Barang bukti harus mempunyai hubungan keterkaitan yang jelas secara hukum dengan kasus yang diselidiki dan bukan rekayasa.
3. Akurat (Accurate)

   Barang bukti harus akurat dan dapat dipercaya.
4. Lengkap (Complete)

   Barang bukti dapat dikatakan lengkap jika didalamnya terdapat petunjuk-petunjuk yang lengkap dan terperinci dalam membantu proses investigasi.

Penanganan Barang Bukti Digital

Kualifikasi Keahlian

Untuk menjadi ahli di bidang digital forensic, seseorang harus memiliki pengetahuan yang mendalam mengenai teknologi informasi baik hardware maupun software. Selain itu harus mendapatkan pelatihan khusus mengenai

digital forensic dari berbagai lembaga dangan dibuktikan dengan sertifikat yang banyak dari :

- Certified Information System Security Professional(CISSP)
- Certified Forensics Analyst(CFA)
- Experienced Computer Forensic Examiner(ECFE)
- Certified Computer Examiner(CCE)
- Computer Hacking Forensic Investigator(CHFI)
- Advanced Information Security(AIS)

Selain itu, yang menjadi penilaian lain adalah seberapa lama jam terbang dalam bidang ini, kasus-kasus yang sudah pernah ditangani dan menjadi saksi ahli dalam perkara tersebut. Seperti profesi lainnya, ahli forensic juga memiliki kode etik seperti mengutamakan kejujuran, kebenaran, ketelitian, ketepatan tindakkan, tidak merusak barang bukti, dan independen.

Digital Forensic Toolskit

Alat forensic digital adalah perangkat lunak yang telah ditentukan atau metode yang tersedia untuk aplikasi forensik digital. Beberapa alat-alat berikut tercantum di bawah ini:

- FTK (Toolkit Forensik) adalah toolkit Unicode yang mampu memberikan akses terhadap code breaking dan pemulihan terhadap password, support terhadap email dan juga memiliki interface yang mudah untuk digunakan.
- Encase adalah sebuah software yang mampu menyelidiki / menganalisis banyak device secara bersamaan. Encase mampu membatasi dampak dari downtime sistem dengan kemampuan respon yang cepat. Funsi encase sangat variatif, antara lain mampu mengidentifikasi penipuan, kejadian-kejadian pada keamanan dan isu-isu integritas karyawan.

- Sleuthkit adalah toolskit digital forensic berbasis UNIX yang menganalisa berbagai teknik strukturmetadata, keyword search, timeline generation,dan menyortir file berdasarkan jenis tipe dan jenisnya.
- Autopsy adalah GUI untuk Sleuthkit, menganalisa kasus dengan menggunakan model client server.
- FIT4D (Forensik Investigasi Toolkit 4 Developing Countries) adalah sebuah toolkit perangkat lunak memanfaatkan sumber daya yang terbatas di negara-negara berkembang. Meningkatkan efisiensi, privasi dan kegunaan.

Selain toolkit digital forensik diatas ada beberapa toolkit yang dapat digunakan bukan hanya sebagai alat untuk mengumpulkan barang bukti, namun juga memiliki fitur untuk memperbaiki kerusakan secara langsung dari device ataupun komputer pasca insiden yang terjadi, toolkit tersebut antara lain :

- Key Logger Award

  Key logger Award adalah sebuah program untuk melacak penekanan tombol pada keyboard. Key logger Award mencatat setiap keystroke ke file log, yang akan menggambarkan segala sesuatu yang diketik (pencarian Google, cache, dll). Program ini dapat mengirim file log diam-diam melalui email atau FTP ke penerima tertentu.
- Recuva

  Recuva merupakan recovery file penting perangkat lunak yang digunakan untuk membuat cadangan data dan informasi yang sengaja dihapus oleh pengguna dari Windows PC, recycle bin mereka atau dari MP3 player.
- USBDeview

USBDeview adalah utilitas kecil yang berisi daftar semua perangkat USB yang sedang terhubung ke komputer Anda, serta semua perangkat USB yang sebelumnya digunakan.

- WinHex

  Winhex adalah editor heksadesimal yang universal, khususnya membantu dalam bidang forensik komputer, data recovery, pengolahan data tingkat rendah, dan keamanan IT. Digunakan untuk memeriksa dan mengedit semua jenis file, memulihkan file yang dihapus atau data hilang dari hard drive dengan sistem file yang korup atau dari kartu kamera digital.

- OpenPuff

  OpenPuff adalah alat steganografi profesional. Openpuff 100% gratis dan cocok untuk data transmisi rahasia yang sangat sensitif. OpenPuff digunakan terutama untuk berbagi data anonymous asynchronous, yaitu pengirim menyembunyikan aliran tersembunyi di dalam beberapa file induk publik yang tersedia

Prosedur Penanganan Barang Bukti Digital

Menurut Assosiation of Chief Police Officer (ACPO) yang merupakan salah satu guidlines Internasional, terdiri dari asosiasi para pemimpin kepolisian di Inggris dan bekerjasama dengan 7 Safe, menerapkan beberapa standar prosedural dalam menangani barang bukti yang menjadi acuan ahli forensik dalam menangani barang bukti digital yaitu:

1. Identification

   Merupakan proses indentifikasi untuk mengenali peristiwa yang terjadi, mengetahui hal yang dibutuhkan dan melakukan penyelidikan.

2. Authorization (approval)

   Adanya otorisasi atau surat persetujuan yang diberikan untuk menyelidiki perkara yang sedang terjadi

3. Preparation

   Melakukan persiapan apa saja yang digunakan dalam kasus tersebut misalnya menetukan area pencarian, tool yang akan digunakan, dan arahan operasional.

4. Securing and Evaluating the Scene (mengamankan dan mengevaluasi tempat kejadian)

   Memastikan keamanan di area tempat kejadian, mengetahui kemungkinan-kemungkinan yang akan terjadi, mengidentidikasi dan melindungi bukti dan melakukan wawancara kepada pihak yang dianggap perlu.

5. Documenting the Scene (Mendokumentasikan tempat kejadian)

   Membuat catatan permanen dari peristiwa dengan fotografi dan mencatat kondisi dokumen dan lokasi serta komponen computer yang terkait, dan mengumpulkannya sebagai bukti untuk di analisa selanjutnya

6. Evidence Collection (Mengumpulkan Barang Bukti)

   Dalam hal ini barang bukti bisa berupa digital maupun elektronik, berupa data-data dari perangkat computer yang berada di tempat kejadian perkara.

7. Packaging, Transportation and Storage

   Setelah menemukan barang bukti maka wajib bagi investigator atau analis forensic untuk melindungi bukti yang ada dan menjauhkan barang bukti dari kemungkinan kontaminasi yang bisa merusak barang bukti tersebut.

8. Initial Inspection (Pemeriksaan awal)

   Pada tahap ini dilakukan identifikasi perangkat baik internal maupun eksternal dari sebuah computer kemudian menentukan tool yang cocok untuk digunakan.

9. Forensic Imaging and Copying

Imaging bertujuan untuk mengetahui keadaan data baik logis maupun fisik, mengetahui data yang tersembunyi, terhapus dan merecovery data yang dibutuhkan untuk proses investigasi.

10. Forensic Examination and Analysis

    Melakukan Pemeriksaan forensic dan analisis dengan menggunakan teknik forensic dan tools untuk menganalisis dan mengolah bukti data, termasuk didalamnya pembuatan nilai hash cryptograpy dan penyaringan dengan hash libraries, menampilkan file, mengekspor dan menyebarkan file misalnya melalui email, ekstraksi metadata, pencarian dan pengindeksan.

11. Presentation and Report

    Prosedur dokumen analisis dan penemuan barang bukti, penggunaan file log , bookmark, dan catatan yang dibuat selama pemeriksaan, membuat kesimpulan dan mmenyiapkannya dalam bntuk laporan untuk menjadi bukti dipengadilan.

12. Review

    Barang bukti yang sudah dibuat laporan diserahkan kepada yang berwenang atau badan pemeriksa, dan ketika terjadi ketidak sepakatan maka badan pemeriksa tersebut harus mempunyai kebijakan dan menetapkan protocol teknis secara admnistratif dan menentukan tindakan yang akan dilakukan.

Hal yang sangat mendasar untuk dipahami oleh seorang ahli digital forensik adalah memahami penanganan barang bukti elektronik di TKP dengan benar. Hal ini memegang peranan yang sangat penting dan krusial, dikarenakan bersifat volatility (mudah berubah, hilang, atau rusak) dari barang bukti digital oleh karena itu harus dijaga keasliannya, sehingga tidak ada manipulasi bentuk, isi, dan kualitas data digital tersebut. Proses penanganan barang bukti hingga presentasi data dalam digital forensik sebagai berikut:

A. Prosedur Penanganan Awal Di TKP

1. Persiapan (Preparations)

   Hal-hal yang harus dipersiapkan dan dimiliki oleh analisis forensic dan investigator sebelum melakukan proses penggeledahan di TKP diantaranya:

   a. Administrasi penyidikan : seperti surat perintah penggeledahan dan surat perintah penyitaan.
   b. Kamera digital : digunakan untuk memotrek TKP dan barang bukti secara fotografi forensic (foto umum, foto menengah dan foto close up).
   c. Peralatan tulis : untuk mencatat antara lain spesifikasi teknis computer dan keterangan para saksi.
   d. Nomor, skala ukur, label lembaga, serta sticker label kosong : untuk menandai masing-masing barang bukti eletronik yg ditemukan di TKP.
   e. Formulir penerimaan barang bukti : digunakan untuk kepentingan chain of custody yaitu metodologi untuk menjaga keutuhan barang bukti dimulai dari tkp.
   f. Triage tools : digunakan untuk kegiatan triage forensik terhadap barang bukti komputer yang ditemukan dalam keadaan hidup (on).

2. Identifikasi bukti digital (Identification / Collecting Digital Evidence)

   Merupakan tahapan yang dilakukan untuk identifikasi dimana bukti itu berada, dimana bukti itu disimpan, bagaimana penyimpanannya dan mengumpulkan data sebanyak mungkin untuk mempermudah penyelidikan.

3. Penyimpanan bukti digital (Preserving Digital Evidence)

   Bentuk dan isi bukti digital hendaknya disimpan dalam tempat yang steril. Untuk benar-benar memastikan tidak ada perubahan-perubahan, hal ini vital untuk diperhatikan. Karena sedikit perubahan saja dalam bukti digital, akan merubah juga hasil penyelidikan. Bukti

digital secara alami bersifat sementara (volatile), sehingga keberadaannya jika tidak teliti akan sangat mudah sekali rusak, hilang, berubah, atau mengalami kecelakaan.

4. Menetapkan Data (Confirming)

   Merupakan tahapan kegiatan untuk menetapkan data-data yang berhubungan dengan kasus yang terjadi

5. Mengenali Data (Identifying)

   Merupakan serangkaian kegiatan untuk melakukan proses identifikasi terhadap data-data yang sudah ada agar memastikan bahwa data tersebut memang unik dan asli sesuai dengan yang terdapat pada tempat kejadian perkara. Untuk data digital, misalnya melakukan identifikasi dengan teknik hashing (sidik jari digital terhadap barang bukti).

B. Prosedur Penanganan Di Laboratorium

1. Administrasi Penerimaan

   Pada tahapan ini, barang bukti komputer yang masuk dan diterima petugas laboratorium, yang dalam hal ini analisis forensic harus dicatat secara detail di dalam log book, disamping di formulir penerimaan. Berikut data yang harus dicatat:

   a. Nama lembaga pengirim barang bukti eletronik
   b. Nama petugas pengirim barang bukti eletronik, termasuk identitasnya secara lengkap.
   c. Tanggal penerimaan.
   d. Jumlah barang bukti eletronik yang diterima, dilengkapi dengan spesifikasi teknisnya seperti merek, model, dan serial/product number serta ukuran (size).
   e. system hashing, yaitu suatu sistem pengecekan otentikasi isi dari suatu file (baik image/evidence file maupun file logical) dengan

menggunakan algoritma matematika seperti MD5, SHA1, dan lain-lain.

2. Akuisisi Bukti Digital

   Pada tahapan ini, dilakukan proses forensic imaging yaitu menggandakan isi dari barang bukti elektronik contoh imaging pada harddisk secara physical sehingga hasil imaging akan sama persis dengan barang bukti secara physical. Derajat kesamaan ini dapat dipastikan melalui proses hashing yang diterapkan pada keduanya.

3. Pemeriksaan (Investigation)

   Pada tahapan ini, terhadap image file dilakukan pemeriksaan secara komprehensif dengan maksud untuk mendapatkan data digital yang sesuai dengan investigasi, ini artinya analisis forensik harus mendapatkan gambaran fakta kasus yang lengkap dari investigator, sehingga apa yang dicari dan akhirnya ditemukan oleh analisis forensic adalah sama (matching) seperti yang diharapkan oleh investigator untuk pengembangan investigasinya. Setelah mendapatkan gambaran fakta kasusnya, kemudian analisis forensic melakukan pencarian (searching) terhadap image file untuk mendapatkan file atau data yang diinginkan.

4. Analisis Data (Analyzing)

   Setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan diatas, selanjutnya data tersebut dianalisis secara detail dan komprehensit untuk dapat membuktikan kejahatan apa yang terjadi dan kaitannya pelaku dengan kejahatan tersebut. Hasil analisis terhadap data digital tadi selanjutnya disebut sebagai barang bukti digital yang harus dapat dipertanggungjawabkan secara ilmiah dan hukum di Pengadilan.

5. Mencatat Data (Recording)

   Melakukan pencatatan terhadap data-data hasil temuan dan hasil analisis sehingga nantinya data tersebut dapat

dipertanggungjawabkan atau dapat direkonstruksi ulang (jika diperlukan) atas temuan barang bukti tersebut.

C. Prosedur Penanganan Laporan

1. Laporan

   Tahapan pembuatan laporan terhadap hasil proses pemeriksaan dan analisis yang diperoleh dari barang bukti digital, selanjutnya data tersebut dimasukkan ke dalam laporan teknis.

2. Pembungkusan dan penyegelan

   Pembungkusan dan penyegelan barang bukti : memuat proses pembungkusan dan penyegelan barang bukti yang telah dianalisis secara digital forensic untuk diserahkan kepada pihak lembaga yang telah mengirimnya.

3. Administrasi Penyerahan Laporan

   Selanjutnya laporan hasil pemeriksaan secara digital forensic berikut barang bukti eletroniknya diserahkan kembali kepada investigator atau lembaga pengirimnya.

D. Presentasi Data (Presenting)

   Kegiatan dimana bukti digital akan dipersidangkan, diuji otentifikasi dan dikorelasikan dengan kasus yang ada. Pada tahapan ini menjadi penting, karena disinilah proses-proses yang telah dilakukan sebelumnya akan diurai kebenarannya serta dibuktikan kepada hakim untuk mengungkap data dan informasi kejadian.

Kasus yang Berkaitan dengan Barang Bukti Digital

Berikut merupakan kasus yang didalamnya terdapat sitaan berupa barang bukti digital atau elektronik :

1. Kasus Pembunuhan dengan nomor perkara 374/Pid.B/2016/PN Dps

Tanggal 13 September 2016 PN Denpasar menetapkan I GUSTI AGUNG ADI SASTRA alias GUNG ADI terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana “tanpa hak menguasai, membawa, mempunyai dalam miliknya, Senjata Penikam Atau Senjata Penusuk“.

Beberapa barang bukti yang dikategorikan sebagai barang bukti digital dalam persidangan tersebut berupa :

- 1 (satu) keping CD rekaman CCTV LLAJ KODYA
- 1 (satu) keping CD rekaman CCTV I PARK
- 1 (satu) keping CD rekaman CCTV Rumah makan simpang ampek
- 1 (satu) keping CD rekaman CCTV Klinik Sone Jl Marlboro Denpasar
- 1 (satu) keping CD rekaman CCTV Lapas Kerobokan
- 1 (satu) keping CD rekaman CCTV Bank Mega

Dari barang bukti yang disita, CCTV merupakan barang bukti elektronik yang didalamnya terdapat rekaman video yang menjelaskan kejadian-kejadian sehingga dapat menjelaskan peristiwa yang terjadi.

2. Kasus Gayus Tambunan dengan nomor perkara 54/ PID/ 2012/ PT.BTN

   Tanggal 26 September 2010 dan hari Kamis tanggal 30 September 2010 sampai dengan tanggal 2 Oktober 2010, sekira pukul 12.00 WIB atau setidak-tidaknya pada suatu waktu dalam bulan September sampai dengan bulan Oktober 2010 bertempat di Bandara Internasional Soekarno Hatta atau setidak-tidaknya di suatu tempat yang masih termasuk dalam daerah hukum Pengadilan Negeri Tangerang, dengan sengaja menggunakan Surat Perjalanan Republik

Indonesia sedangkan ia mengetahui atau sepatutnya menduga bahwa Surat Perjalanan itu palsu atau dipalsukan.

Salah satu barang bukti yang disita adalah 1 (satu) lembar print out Pencarian Data Perlintasan pada tempat pemeriksaan Imigrasi An. Sony Laksono pemegang Passport No. T 116444.

Menurut analisa oleh Ruby Alamsyah, bahwa foto Gayus Tambunan yang ada dalam paspor an. Sony Laksono adalah hasil pemotretan (foto) terhadap terdakwa yang telah dimanipulasi. Semua foto dibuat menggunakan kamera yang sama yaitu Sony DSC-T77 pada tanggal yang sama yaitu 17 Juli 2010 pada jam yang hampir bersamaan yaitu sekitar jam 13:27:15 sampai dengan 13:29:26. Adapun tools yang digunakan dalam menganalisa foto-foto tersebut yaitu Encase Forensic v 6.2, Forensic Tool Kit, Exiff Tool, Adobe Photoshop CS dan Image editor lainnya.

Kesimpulan

Barang Bukti Digital berperan penting dalam pengungkapan kasus tindak kejahatan cyber atau digital. Dalam pengungkapan kasus tersebut, barang bukti harus memiliki 4 kriteria yakni admissibile, authentic, accurate dan complete. Selain itu harus ditangani oleh pihak yang telah terkualifikasi dalam hal ini bersertifikasi dalam bidang digital forensic agar penaganan barang bukti digital dilakukan sesuai prosedur sehingga kasus dapat terungkap kebenarannya.

DAFTAR PUSTAKA

Marcella, A. J. & Greenfiled, R. S. (2002). *Cyber Forensics a field manual for collecting, examining, and preserving evidence of computer crimes*, Florida: CRC Press LLC.

Meiyanti, Ruci and Ismaniah, Ismaniah (2015) *Perkembangan Digital Forensik Saat Ini dan Mendatang.* Jurnal Karya Ilmiah, 15 (2).

Kominfo. (2015). *Kick Off Pembentukan Asosiasi Forensik Digital Indonesia*. Diakses 14 September 2018. <https://kominfo.go.id/index.php/content/detail/6417/Kick+Off+Pembentukan+Asosiasi+Forensik+Digital+Indonesia/0/berita_satker>

Kavrestad, Joakim (2018). *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*. Springer International Publishing AG.

Lizarti, Nora dan Utami, Handayani Dwi. (2013). *Penanganan Barang Bukti Forensik*.-.

NIJ. (2001). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, Washington DC: U.S. Department of Justice