BAB 2
Tinjauan Pustaka

2.1 Digital Forensik

Menurut (Nuh Al-Azhar, 2012) digital forensik merupakan *"aplikasi bidang ilmu pengetahuan dan teknologi komputer yang digunakan dalam kepentingan pembuktian hukum (pro justice), untuk melakukan pembuktian kejahatan dengan menggunakan teknologi atau komputer secara ilmiah hingga mendapatkan bukti digital yang digunakan untuk menjerat pelaku kejahatan".* Digital forensik menjadi salah satu bentuk spesialisasi untuk melakukan investigasi yang berhubungan dengan kejahatan komputer (computer related crime). Digital forensik akan melakukan pemeriksaan setiap barang bukti elektronik dalam rangka mencari data-data digital yang berkaitan dengan kasus kejahatan dan pelakunya.

Menurut National Institute of Standards and Technology (NIST) ada empat tahapan dalam digital forensik (Kent, Chevalier, Grance, & Dang, 2006) yaitu *collection, examination, analysis* dan *reporting*. Pada tahap *collection* merupakan tahap pengumpulan data, yang selanjutnya akan di identifikasi, pemberian label, perekaman data yang diperoleh dari sumber data yang relevan dan menggunakan prosedur yang sesuai sehingga integritas data dapat dipertanggunag jawabkan. Selanjutnya adalah tahapan examination untuk melakukan pemeriksaan terhadap data yang telah dikumpulkan dengan menggunakan kombinasi metode otomatis dan manual, sehingga dapat menilai dan melakukan ekstraksi data dengan tetap menjaga integritas data. Kemudian adalah tahap melakukan *analysis* menggunakan metode dan melakukan dokumentasi terhadap setiap langkah yang dilakukan, sehingga dapat memperoleh informasi yang berguna dan menjawab masalah-masalah dalam proses pemeriksaan dan pengumpulan data. Tahapan terakhir adalah reporting untuk melaporkan hasil dari analisa. tahapan ini meliputi beberapa prosedur diantaranya penjelasan bagaimana data diperoleh, penjelasan dari setiap tindakan yang dilakukan, penjelasan bagaimana alat dan prosedur yang dilakukan dan rekomendasi untuk perbaikan dari proses forensik.

Gambar 2.1 Tahapan digital forensic

2.2 Bukti Digital

Penyelesaian kasus-kasus yang berhubungan dengan bukti digital harus mengikuti prosedur-prosedur yang sesuai dengan aturan hukum yang berlaku baik itu hukum yang berlaku di dalam negeri maupun luar negeri. Indonesia telah memiliki undang-undang yang mengatur tentang bukti digital yaitu Undang-Undang Nomor 19 Tahun 2016 yang merupakan Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Dalam Undang-undang Nomor 19 Tahun 2016 Pasal 1 angka 1 dan angka 4 yang berbunyi :

a. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
b. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Dalam digital forensik seorang ahli forensika digital harus memahami prinsip-prinsip dasar digital forensik. Hal ini menjadi dasar seorang ahli digital forensik dalam melakukan invesitigasi computer crime atau computer related crime. Menurut (ACPO, 2012), prinsip-prinsip dasar digital forensik adalah :

a. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
b. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

c. *An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.*
d. *The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.*

Prinsip dasar yang pertama adalah Dalam invesitigasi digital forensik penegak hukum dilarang mengubah bukti digital yang tersimpan dalam media penyimpanan elektronik yang akan dibawa dalam proses persidangan. Hal ini dilakukan untuk menjaga agar informasi yang terdapat dalam bukti digital tersebut tetap terjaga keutuhannya dan terjaga dari kemungkinan rekayasa data digital sehingga dapat dipertanggung jawabkan di pengadilan. Barang bukti digital memiliki juga memiliki sifat *volatile* sehingga mudah hilang atau rusak. Untuk mencegah terjadinya hal ini maka dalam proses penanganan barang bukti digital perlu menerapkan prinsip *chain of custody*. Prinsip *chain of custody* merupakan pendokumentasian barang bukti sejak di terimanya barang bukti digital tersebut sampai dengan proses pengadilan sehingga barang bukti akan tetep terjaga keaslianya. Prinsip dasar yang kedua adalah penyidik yang akan melakukan investigasi terhadap barang bukti digital harus memiliki keahlian atau kopetensi yang jelas dan relevan sehingga dapat menjelaskan relevansi dan implikasi dari tindakan-tindakan yang dilakukan selama pemeriksaan. Dalam bidang digital forensik kompetensi atau keahlian menjadi hal utama karena dengan adanya kopentensi ini setiap tindakan investigasi dapat dijelaskan dan di pertanggung jawabkan.

Prinsip dasar yang ketiga adalah pemeriksaan bukti digital harus memiliki catatan teknis dan praktis terhadap langkah-langkah yang diterapkan, sehingga ketika barang bukti jika diperiksa oleh pihak ketiga akan mendapatkan hasil yang sama dengan hasil yang telah dilakukan oleh investigator sebelumnya. Ketika melakukan pemeriksaan harus sesuai dengan prosedur, serta barang bukti digital yang telah diperiksa siap untuk di periksa kembali oleh pihak ketiga yang independen karena tidak menutup kemungkinan majelis hakim dalam persidangan meminta pihak ketiga untuk melakukan pemeriksaan ulang untuk memastikan hasil pemeriksaan sebelumnya. Prinsip dasar yang terakhir adalah dalam pemeriksaan bukti digital investigator harus dapat memastikan bahwa proses investigasi maupun pemeriksaan barang bukti harus sesuai dengan hukum dan prinsip-prinsip dasar sebelumnya. Hal ini dilakukan agar hasil pemeriksaan dan analisa terhadap media penyimpanan barang bukti elektronik yang berupa data-data digital tidak

bertentangan dengan hukum positif yang berlaku sehingga dapat diterima secara teknis dan hukum oleh majelis hakim di persidangan.

Dalam digital forensik dikenal dua jenis barang barang bukti yaitu barang bukti elektronik dan barang bukti digital. Barang bukti elektronik adalah barang bukti bersifat fisik dan dapat dikenali secara visual sedangkan barang bukti digital adalah barang bukti yang berasal dari extraksi dari barang bukti elektronik.

Tabel 2.1 Barang bukti digital dan elektronik

NO	Barang Bukti elektronik	Barang Bukti Digital
1	Komputer PC,	Logical file
2	laptop/notebook, netbook, tablet	Deleted file
3	Handphone, smartphone	Lost file
4	Flashdisk/thumb drive	File slack
5	Floppydisk	Log file
6	Harddisk	Encrypted file
7	CD/DVD	Steganography file
8	Router, switch, hub	Office file
9	Kamera video, cctv	Audio file
10	Kamera digital	Video file
11	Digital recorder	Image file
12	Music/video player, dan lain-lain	Email
13		User ID dan password
14		Short message service
15		Call logs

Mengamankan bukti adalah proses pertama yang dilakukan ketika suatu kejahatan dicurigai, dan berlanjut setelah pemeriksaan selesai. Jika persidangan, gugatan perdata, atau sidang disipliner telah berakhir, bukti harus tetap aman jika ada banding atau proses hukum lainnya. Karena itu, tanggal retensi harus ditetapkan untuk semua peralatan dan data yang disimpan sebagai bukti. Jika data dan peralatan akan digunakan sebagai bukti, maka perlu memastikan bahwa integritasnya tidak terganggu. Pelestarian data melibatkan praktik-praktik yang melindungi data dan peralatan dari bahaya sehingga bukti asli disimpan dalam keadaan sedekat mungkin dengan saat pertama kali diperoleh. Jika data hilang, diubah, atau rusak, ada kemungkinan tidak dapat menyebutkannya di pengadilan. Ini berarti bukti yang tidak dapat diterima mungkin juga tidak pernah ada sama sekali.

Lebih buruk lagi, kredibilitas bagaimana bukti dikumpulkan dan diperiksa dapat dipertanyakan, membuat bukti lain tidak dapat diterima juga. Oleh karena itu bukti harus aman selama investigasi.

2.3 Media sosial

Media sosial kini semakin berkembang. Beberapa jenis media sosial diantaranya adalah facebook, twitter, instagram, dan linkedin. Media sosial tidak hanya terbatas pada situs jejaring sosial seperti facebook dan twitter, akan tetapi mencangkup juga blog, wikipedia, youtube dan lain-lain. Akan tetapi banyaknya platform media sosial ini juga berdapak pada tindak kejahatan. Media sosial, seperti facebook dan beberapa aplikasi lainnya dapat banyak pengguna yang anonim. Pengguna anonim ini dapat berkomunikasi dan berbagi konten tanpa membuat profil pengguna. Mereka diciptakan pada awalnya sebagai tanggapan atas keprihatinan atas privasi dan keberadaan jejak digital.

Media sosial berisi banyak sumber informasi dan bukti digital yang potensial untuk proses penyelidikan. Konten media sosial memberikan informasi yang sangat beragam untuk penyidik dalam proses investigasi kriminal jika dieksplorasi dengan tepat. Media sosial adalah sumber informasi yang cukup banyak untuk di ekplorasi tentang calon tersangka, korban, dan saksi seperti posting teks, daftar teman, gambar, data lokasi geografis, video, informasi demografis, dan sebagainya. Walaupun berkembang berbagai macam jenis platform media sosial, namun beberapa karakteristik umum akan tersedia bagi penyidik. Selain itu data-data yang ada di media sosial dapat dikategorikan menjadi empat kategori yaitu Pengguna, Aktivitas, Jaringan , dan Konten (Arshad et al., 2019). Data-data yang berada pada setiap platform media sosial dapat di akses melalui API yang telah disediakan oleh masing-masing platform media sosial.

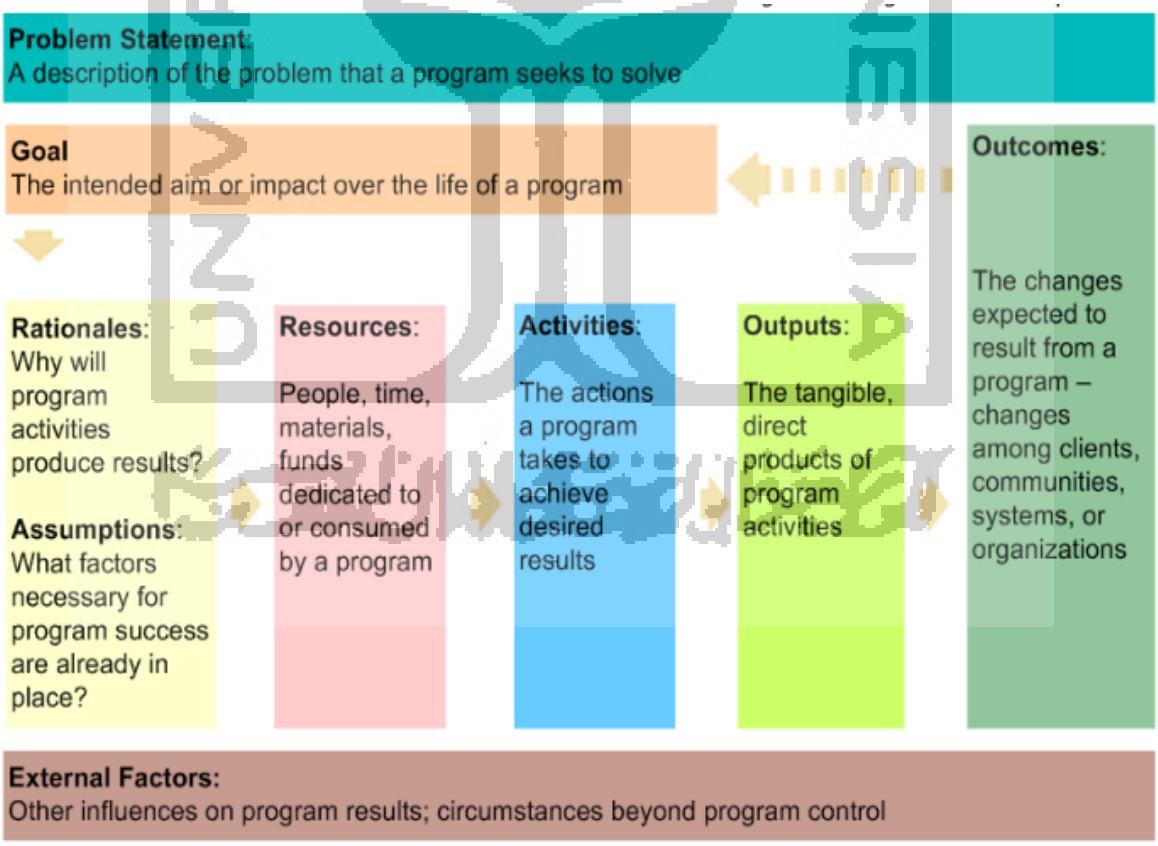
2.4 *Digital Forensics Investigation Models*

Dalam proses penyelesaian kasus-kasus yang berhubungan dengan digital forensik dibutuhkan sebuah model investigasi sehingga bukti digital yang diperoleh dapat diterima dalam proses pengadilan. Menganalisis data sambil menjaga integritasnya merupakan hal penting karena integritas data sebagai bukti digital. Penegakan hukum dalam perlombaan abadi dengan penjahat dalam penerapan teknologi digital, dan membutuhkan pengembangan alat untuk secara sistematis mencari perangkat digital untuk bukti yang relevan (Gregg Gunsch, Clint Carr, 2009).

Telah banyak penelitian yang dilakukan untuk model investigasi digital forensik. Model yang di kembangkan tersebut dilakukan untuk menjawab permasalahan kasus digital forensik. Pada kasus yang berhubungan dengan bukti digital di media sosial tentu akan membutuhkan motedologi untuk menyelesaikan masalah-masalah tersebut. Analisis forensik digital memerlukan bukti digital seperti analisis forensik fisik memiliki bukti fisik. Model investigasi forensik digital membuat bukti digital melalui berbagai fase dalam berbagai tahapan.

2.5 Logic Model

Logic model dapat digunakan untuk identifikasi *Timeframe* yang akan di buat. Hal ini akan membantu dalam memperoleh hasil jangka pendek, menengah, dan jangka panjang serta membuat keputusan yang baik tentang sumber daya dan keputusan. Struktur logic model dapat digunakan untuk perencanaan program dengan menentukan parameter program dengan jelas. Banyak model logic yang ada, namun pada dasarnya semua mengandung konsep yang sama. Model logic akan bermanfaat untuk pemangku kepentingan untuk memperoleh masukan dalan kegiatanya (Mccawley, 2015) .



Gambar 2.2 Template Logic Model

2.6 Comparation Logic Model

Composite Logic digunakan untuk mengkombinasikan beberapa struktur model menjadi sebuah model kesatuan yang tetap mempertahankan hirarki ataupun susunan awal kerangkan model yang ada. Hal yang paling penting dalam *Composite Logic* model adalah menentukan role model dari setiap variabel ataupun pola awal yang ingin dikolaborasikan. Role model menjelaskan bagaimana beberapa objek berkolaborasi, satu ataupun dua peran yang bersamaan dalam sebuah pola untuk mencapai tujuan yang sama. Sebuah peran mewakili sudut pandang dari beberapa objek yang bekerjasama dengan berpegang pada sebuah tujuan. Pemodelan ini dapat membantu peneliti dalam mengeksplorasi keterhubungan dari aktivitas berbeda dengan tujuan yang sama. Sehingga memudahkan peneliti dalam melakukan klasifikasi dan kolaborasi beberapa *framework* yang pada akhirnya akan menghasilkan satu set *framework* (Lizarti et al., 2017).

Kelebihan lain dari composite adalah composite dapat meringkas realitas multi-dimensi yang kompleks dengan maksud untuk mendukung para pembuat keputusan dan Lebih mudah diinterpretasikan untuk banyak indikator terpisah serta mengurangi ukuran yang terlihat dari serangkaian indikator tanpa menjatuhkan basis informasi yang mendasarinya. Dibalik beberapa kelebihan yang dimiliki composite, namun ada beberapa kekurangan antara lain dapat mengirim pesan kebijakan yang menyesatkan jika dibangun dengan buruk atau disalahtafsirkan. Selain itu dapat mengundang kesimpulan kebijakan yang sederhana yang memiliki kemungkinan untuk disalah artikan, serta pemilihan indikator dan bobot bisa menjadi subyek perselisihan politik. (Nardo, Saisana, Saltelli, & Tarantola, 2008).

2.7 Maltego

Maltego adalah sebuah alat yang digunakan untuk mengumpulkan informasi sebanyak mungkin dengan tujuan forensik, *pentesting*, atau *ethical hacking*. Tools ini mengumpulkan informasi tentang target dan menampilkan informasi tersebut dalam format yang mudah dimengerti, memvisualisasikan informasi tersebut ke dalam sebuah format graph, serta sangat cocok untuk link analysis dan data mining. Tools maltego ini merupakan bagian dati tools *Open source Intelligence* yang sering digunakan untuk mengumpulkan data yang bersifat publik di internet.