TUGAS

“KEAMANAN JARINGAN KOMPUTER”

Disusun Oleh :

Nama : Nova Dyati Pradista

Nim : 09011181320005

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

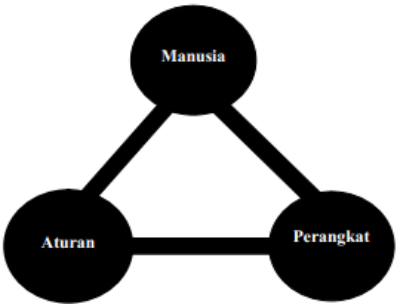
Digital Forensik

“Mobile Digital Forensic for the Military”

(https://www.youtube.com/watch?v=O8DPr6UgFiA)

Digital Forensik merupakan penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti serta informasi yang secara magnetis tersimpan atau disandikan pada komputer atau media penyimpanan digital sebagai alat bukti dalam mengungkap kasus kejahatan yang dapat dipertanggungjawabkan secara hukum.

Komponen digital forensik mencakup manusia *(people)*, perangkat atau peralatan *(equipment)* dan aturan *(protocol)* yang dirangkai, dikelola dan diberdayakan sedemikian rupa dalam upaya mencapai tujuan akhir dengan segala kelayakan dan kualitas sebagaimana bisa dilihat pada gambar berikut:



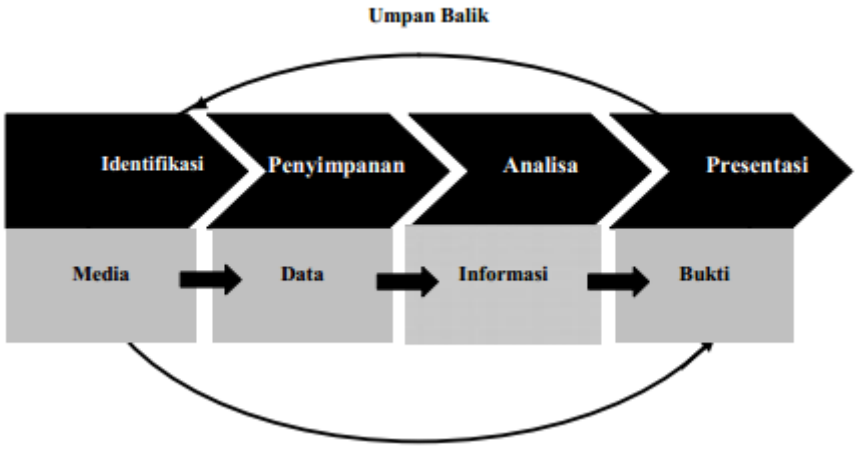
Manusia yang diperlukan dalam komputer forensik merupakan pelaku yang tentunya mempunyai kualifikasi tertentu untuk mencapai kualitas yang diinginkan. Ada tiga kelompok sebagai pelaku digital fornsik, yaitu collection specialist, examiner dan investigator. Collection specialist bertugas mengumpulkan barang bukti berupa *digital evidence. Examiner* bertugas sebagai penguji terhadap media dan mengekstrak data sedangkan investigator bertugas sebagai penyidik.

Secara garis besar perangkat untuk kepentingan digital forensik dapat dibedakan menjadi dua kategori yaitu *hardware* dan *software*. Jjenis perangkat hardware yang digunakan pada implementasi digital forensik yaitu mulai dari yang sederhana dengan komponen *single-purpose* seperti *write blocker* yang fungsinya hampir sama dengan *“writeprotect”* pada disket, pada optical media dan hardisk fungsi seperti ini tidak ada yang memastikan bahwa data tidak akan berubah manakala diakses, sampai pada sistem komputer lengkap dengan kemampuan server seperti F.R.E.D (*Forensic Recovery of Evidence Device).* Sedangkan perangkat software dikelompokkan kedalam dua kelompok yaitu aplikasi berbasis *command line* dan aplikasi berbasis GUI *(Graphical User Interface).* Aturan merupakan komponen yang paling penting dalam pemodelan digital forensik, didalamnya mencakup prosedur dalam mendapatkan, menggali, menganalisa barang bukti dan akhirnya bagaimana menyajikan hasil penyelidikan dalam laporan.

Ada beberapa tahapan dalam proses implementasi digital forensik. Secara garis besar dapat di klasifikasikan menjadi empat tahapan yaitu:

1. Identifikasi bukti digital
2. Penyimpanan bukti digital
3. Analisa bukti digital
4. Presentasi

Keempat tahapan ini dapat digambarkan pada gambar berikut:



Berikut hasil dari resume kasus video yang berjudul ***Mobile Digital Forensic for the Military*** ***(*** **https://www.youtube.com/watch?v=O8DPr6UgFiA**):

Di era digital yang serba cepat saat ini militer dan badan intelijen harus mengatasi tantangan global. Operasi militer harus berkomitmen dan membutuhkan intelijen. Intelijen tim harus menggunakan beberapa metode analisis untuk memberikan arahan dan bimbingan kepada para militer di lapangan termasuk forensic digital. Eksploitasi situs menyediakan informasi dalam gambaran ruang pertempuran militer tersebut. Eksploitasi situs forensik digital mungkin terjadi pemulihan data dengan menggunakan alat digital forensik serta waktu yang sangat efektif. Intelijen ditindaklanjuti dengan tingginya nilai target dengan cepat dan efektif. Tim intelijen spector dells seluler forensic merupakan solusi untuk mendapatkan informasi digital sebagai bagian dari situs tersebut. Misi eksploitasi tim tersebut tiba di titik yang ditunjuk dengan cepat untuk menetapkan perimeter keamanan lokal di lokasi sasaran yang telah diidentifikasi dan tim mulai beroperasai onsite serta mengarahkan segala yang dibutuhkan untuk mengeksploitasi digital dalam kasus tersebut. Satelit phone dan penyimpanan digital lainnya dapat diproses dengan cepat dan efisien untuk mengidentifikasi beberapa profil dan dapat digunakan secara bersamaan untuk menangkap semua sasaran perangkat termasuk mengcapture sistem yang sedang berjalan yang sudah dirancang. Kecepatan dan ketepatan pada sasaran sangat efektif diterapkan sehingga waktu pada target bisa sesingkat mungkin. Dalam satu pendekatan, memungkinkan removable media sel dan telepon satelit untuk di proses dengan mengurangi peralatan beban operator. Intelijen harus

diproses dengan cepat dan remote akses yang baik untuk kemampuan yang memungkinkan data yang akan dibuat aman tersedia untuk jarak jauh.

Kesimpulan :

Kasus video ***Mobile Digital Forensic for the Military*** digital forensik diatas dapat diselesaikan melalui 4 tahapan sebagai berikut:

1. *Identifikasi Bukti Digital,* Pada tahap ini segala bukti-bukti yang mendukung penyelidikan dikumpulkan. Penyelidikan dimulai dari identifikasi dimana bukti itu berada, dimana disimpan, dan bagaimana penyimpanannya untuk mempermudah penyelidikan. Media digital yang bisa dijadikan sebagai barang bukti mencakup sebuah sistem komputer, media penyimpanan (seperti flash disk, pen drive, hard disk, atau CD-ROM), PDA, handphone, smart card, sms, e-mail, cookies, source code, windows registry, web browser bookmark, chat log, dokumen, log file, atau bahkan sederetan paket yang berpindah dalam jaringan komputer. Tahapan ini merupakan tahapan yang sangat menentukan karena bukti-bukti yang didapatkan akan sangat mendukung penyelidikan untuk mengajukan seseorang ke pengadilan.

2. *Penyimpanan Bukti Digital,* Tahapan ini mencakup penyimpanan dan penyiapan bukti-bukti yang ada, termasuk melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu. Bukti harus benar-benar steril artinya belum mengalami proses apapun ketika diserahkan kepada ahli digital forensik untuk diteliti. Karena bukti digital bersifat sementara *(volatile),* mudah rusak, berubah dan hilang, maka pengetahuan yang mendalam dari seorang ahli digital forensik mutlak diperlukan. Kesalahan kecil pada penanganan bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan. Bahkan menghidupkan dan mematikan komputer dengan tidak hati-hati bisa saja merusak atau merubah barang bukti tersebut.

3. *Analisa Bukti Digital,* Tahapan ini dilaksanakan dengan melakukan analisa secara mendalam terhadap bukti-bukti yang ada. Bukti yang telah didapatkan perlu di-explore kembali kedalam sejumlah skenario yang berhubungan dengan tindak pengusutan, seperti siapa yang telah melakukan, apa yang telah dilakukan, apa saja software yang digunakan hasil proses apa yang dihasilkan serta waktu melakukan.

4. *Presentasi,* Presentasi dilakukan dengan menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggung jawabkan secara hukum di pengadilan. Laporan yang disajikan harus di *cross-check* langsung dengan saksi yang ada, baik saksi yang terlibat langsung maupun tidak langsung. Hasil laporan akan sangat menentukan dalam menetapkan seseorang bersalah atau tidak sehingga harus dipastikan bahwa laporan yang disajikan benar-benar akurat, teruji, dan terbukti.