BAB II
TINJAUAN PUSTAKA

A. PENELITIAN TERDAHULU

Dalam penelitian lain yang dilakukan Riadi, *et al*. (2018) Hasil pada tahap implementasi dan pengujian yang dilakukan sesuai desain skenario, dengan tujuan untuk mendapatkan bukti digital seperti pada kasus kejahatan komputer yang sebenarnya maka dibuat skenario: Melakukan aktifitas internet membuka laman web dan mengunduh beberapa file .doc, .pdf, dan .mp3, membuka, melakukan pengeditan, dan menyimpan file pada *drive SSD* yang dibekukan dengan *software utility* pembeku *drive Shadow Defender*, file yang digunakan pengujian, Menyalin file pada *drive SSD* yang dibekukan melalui *flashdisk* dan begitu juga sebaliknya, guna membuktikan validitas file yang dibuat terhadap hasil analisa forensik dan *recovery* file maka dilakukan hashing pada setiap file yang dibuat dan disalin pada *drive SSD* yang dibekukan. disebutkan bahwa berdasarkan hasil dari penelitian yang telah dilakukan pada implementasi salah satu *software* pembeku *drive* yaitu *Shadow Defender* yang dapat membekukan suatu *drive SSD* (*frozen solid state drive*) dan terbukti berpengaruh terhadap praktik eksaminasi dan analisis forensik terhadap didapatkannya buktibukti digital. Tidak semua file dapat direstorasi dengan baik karena struktur file dan data sudah rusak, serta catatan pengguna komputer (*recent activity*) dan sejarah internet (*history* internet) tercatat ketika fitur pembeku *drive* diaktifkan. Jika dilakukan perhitungan tingkat prosentase keberhasilannya hanya memiliki nilai 28,7% yang diperoleh dari 85 file yang disiapkan untuk implementasi dan pengujian dan hasil file dari eksaminasi dan yang berhasil direstorasi hanya 25 file. Sehingga dapat menjadi hambatan

dalam proses forensik digital (digital forensik) oleh penyidik dan hasil dari penyidikan masih sangat sedikit informasi yang didapatkan dari barang bukti digital.

Kemudian penelitian yang dilakukan Albanna & Riadi, (2017) Dalam tulisan ini, kami telah menyebutkan bahwa teknik Forensik akuisisi statis yang dapat bekerja pada *hard drive* beku komputer yang telah dimatikan. Investigasi adalah dilakukan pada data statis file dokumen digital, diperoleh gambar, log riwayat internet, dan log terbuka baru-baru ini di beku *hard drive* ditemukan di ruang yang tidak terisi. Semua perangkat lunak memang ditemukan pada *hard drive* beku.

Pada penelitian yang telah dilakukan sebelumnya yaitu. Penerapan *toolkit* Puran file *recovery*, *Glary Undelete* dan *Recuva* data *recovery* dilakukan pada sistem operasi windows 7. Ketiga *toolkit* ini adalah *software* yang bisa di*download* secara gratis. Setelah ketiga *software* tersebut di*download* kemudian di*install*, tampilan awal untuk *toolkit* Puran file *recovery*. pengujian ketiga *toolkit* ini dilakukan untuk mengetahui bagaimana kinerja *toolkit* dalam pencarian data yang sudah dihapus didalam sebuah *flash drive* Dalam pengujian ini akan dilihat hasilnya berdasarkan banyaknya jumlah data yang dapat di*scan* dan jumlah data yang dapat dipulihkan. Tahap pertama pengujian akan dilakukan dengan menggunakan *toolki*t Puran file *recovery*. Kemudian pengujian dilanjutkan dengan *toolkit Glary Undelete* dan terakhir dengan Recuva data recovery Handrizal, (2017).

Implementasi atau aplikasi *OSforensik, GetDataBack, Disk Genius* dan *Diskdigger* telah dilakukan pada Sistem Operasi *Windows* 8. Keempat aplikasi ini adalah perangkat lunak *freeware* / dapat diunduh secara gratis. Setelah empat perangkat lunak diunduh dan kemudian di*instal*. Setelah terinstal di tahap terakhir menguji empat aplikasi pemulihan data. Perlu diketahui pengujian keempat aplikasi ini dilakukan untuk mengetahui bagaimana kinerja aplikasi dalam data pencarian yang telah dihapus dalam *flash drive*. Dalam tes ini akan terlihat hasil berdasarkan jumlah data yang dapat dipindai dan jumlah data yang dapat dipulihkan. Tahap pertama pengujian akan dilakukan dengan

menggunakan aplikasi *OSforensik*. Pengujian lebih lanjut dilanjutkan dengan aplikasi *GetDataBack*, kemudian dengan aplikasi pengujian *Disk Genius* dan terakhir dengan *Diskdigger*. Tahapan pengujian untuk setiap aplikasi adalah sebagai berikut: 1) Hapus *flash drive*, 2) Salin dua puluh file dari *drive* D: / ke *flash drive*, 3) Hapus semua data dalam *flash drive*, 4) Kosongkan *recycle bin*, 5) Mengoperasikan Pemulihan Aplikasi . Hidayat, *et al*. (2019).

Analisis forensik menyediakan domain untuk mendefinisikan dampak kehilangan data atau pencurian data. Sekarang, ini bisa menjadi terobosan penting jika orang dibuat sadar akan semua pro dan kontra forensik digital dan terutama ketika datang ke domain perspektif keamanan data. Kedua, hard drive, drive USB, dan perangkat penyimpanan digital lainnya menyediakan jalur untuk mengakses dan mengambil data, tetapi juga dapat terbukti menjadi bencana ketika kehilangan bagian terpenting dari sistem atau ruang kerja. Menentukan alat untuk menerapkan forensik digital di suatu organisasi, penyelidikan kriminal atau tingkat individu dikembangkan, di mana beberapa adalah pemilik dan beberapa GPL. Berbagai cabang forensik digital juga mendefinisikan kami sebagai solusi untuk menjaga integritas di berbagai tingkat pengembangan perangkat lunak. Berbagai tahap forensik digital juga menentukan hubungan dan saling ketergantungan skenario pengambilan data atau ekstraksi melalui penerapannya yang efektif dan aman. Semua layanan yang disediakan oleh Digital forensic dievaluasi dan cukup membantu untuk mengakses berbagai domain data atau kehilangan properti individu terkait dengan data dan kejahatan dunia maya, yang entah bagaimana mencakup analisis forensik. (Pansari, 2019)

B. LANDASAN TEORI

1. Digital Forensik

Menurut Al-Azhar, (2012) komputer atau digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (*pro justice)*, yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau *computer crime*

secara ilmiah (*scientific)* hingga bisa mendapatkan bukti-bukti digitak yang dapat digunakan untuk menjerat pelaku kejahatan tersebut.

Hal yang perlu di pahami seorang ahli forensik digital adalah prinsip dasarnya, dalam hal ini ACPO (*Association Of Chief Police Officiers)* England Wales dan Nireland adalah suatu lembaga hukum di United Kingdom (UK) bidang penegakan hukum menyatakan bahwa prinsip-prinsip dasar sebagai berikut:

1. *No action taken by law enforcement agencies or their agents should change data held on a computer storage media which may subsequenctly be relied upon court.*
2. *In circumstances where a person finds it necessary to access original data held on a computer or an storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their action.*
3. *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.*
4. *The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.*

2. *Flashdisk*

Flashdisk adalah perangkat penyimpan data yang terdiri dari memori flash dan terintegrasi dengan antarmuka USB (*Universal Serial Bus*). *Flashdisk* memiliki sifat dapat dibaca dan ditulis oleh komputer dan akan mempertahankan informasi yang telah ditulis di dalamnya walaupun tanpa adanya arus listrik. Dengan demikian, data yang ada di dalam flashdisk akan tetap tersimpan di memori flash walaupun tanpa menggunakan baterai Lahagu, (2017).

3. Bukti *Digital*

Riadi, *et al*. (2018) menyatakan bahwa bukti digital adalah informasi yang disimpan atau di kirim dalam bentuk *biner* yang dapat diandalkan di Pengadilan. Khusus untuk bukti digital berhubungan dengan mobile seperti *smartphone* dapat ditemukan di *call history, phonebook, SMS dan MMS, Photo, Audio, Video* dan lainlainnya. Bukti digital umumnya terkait dengan kejahatan digital seperti kejahatan yang memanfaatkan sosial media sebagai tempat melakukan kejahatan, sehingga Bukti digital digunakan untuk membantu dalam mengadili semua jenis kejahatan digital . Bukti digital sangat rentan akan perubahan sehingga dapat mempengaruhi keasliannya jika tidak ditangani dengan benar. Semua jenis perubahan yang mengandung bukti digital akan mengarah pada kesimpulan salah, atau bukti tidak akan berguna.

4. *Digital Forensics Research Workshop (DFRWS)*

   Model investigasi DFRWS ini meliputi enam tahapan dengan tahap pertama yaitu identifikasi. Tahap ini untuk melakukan penentuan kebutuhan yang akan diperlukan untuk penyelidikan dan pencarian bukti digital. Tahap kedua Pemeliharaan yaitu untuk menjaga bukti bukti dan memastikan keaslian atau integritas barang bukti sehingga bukti benar-benar valid/sah. Tahap ketiga yaitu tahap pengumpulan, merupakan tahap untuk identifikasi mengumpulkan sumber bukti yang berpotensi menjadi bukti yang kuat. Tahap keempat adalah tahap pemerikasaan yaitu tahapan untuk menentukan apa saja yang akan dianalisa atau lebih dikenal dengan filterisasi data, sehingga investigator dapat lebih fokus dalam melakukan tahapan selanjutnya. Tahap kelima adalah analisis yaitu tahap untuk mencari dan mengolah data termasuk data diperoleh dari mana, siapa yang membuuat dan bagaimana data tersebut dihasilkan. Tahap terakhir adalah tahap presentasi yaitu tahap dimana melaporkan dan mempresentasikan hasil analisa sehingga dapat dipahami oleh publik. (Nur Faiz. et al 2018)