BAB II

LANDASAN TEORI

A. Kajian Pustaka

1. Pengertian Aplikasi

Aplikasi merupakan program yang berisikan perintah-perintah untuk melakukan pengolahan data. Jadi aplikasi secara umum adalah suatu proses dari cara manual yang ditransformasikan ke komputer dengan membuat sistem atau program agar data diolah lebih berdaya guna secara optimal. (Jogiyanto,2004)

Perangkat lunak/aplikasi adalah suatu subkelas perangkat lunak komputer yang memanfaatkan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pengguna. Biasanya dibandingkan dengan perangkat lunak sistem yang mengintegrasikan berbagai kemampuan komputer, tapi tidak secara langsung menerapkan kemampuan tersebut untuk mengerjakan suatu tugas yang menguntungkan pengguna.

Aplikasi adalah software atau perangkat lunak yang dibuat untuk mengerjakan menyelesaikan masalah-masalah khusus. (Daryanto,2004).

Dari uraian diatas dapat disimpulkan bahwa aplikasi adalah sebuah perangkat lunak yang berisi perintah untuk menyelesaikan masalah dan pengolahan data.

2. Smartphone

Telepon pintar (*smartphone*) adalah telepon genggam yang mempunyai kemampuan tingkat tinggi, kadang-kadang dengan fungsi yang menyerupai komputer. Belum ada standar pabrik yang menentukan arti telepon pintar. (Elcom, 2011)

Bagi beberapa orang, telepon pintar merupakan telepon yang bekerja menggunakan seluruh perangkat lunak sistem operasi yang

menyediakan hubungan standar dan mendasar bagi pengembang aplikasi. Bagi yang lainnya, telepon cerdas hanyalah merupakan sebuah telepon yang menyajikan fitur canggih seperti surel (surat elektronik), internet dan kemampuan membaca buku elektronik (e-book) atau terdapat papan ketik (baik sebagaimana jadi maupun dihubung keluar) dan penyambung VGA. Dengan kata lain, telepon cerdas merupakan komputer kecil yang mempunyai kemampuan sebuah telepon.

3. Sistem Android

Sistem operasi Android sendiri merupakan sebuah sistem operasi open source yang dikembangkan dan diluncurkan oleh Google inc, yang dikhususkan untuk diaplikasikan pada teknologi smartphone. Akan tetapi dengan perannya sebagai sebuah open source maka Android sendiri telah banyak berkembang pesat hingga merambah ke penggunaan pada sebuah komputer.

Sistem Android adalah sebuah sistem operasi berbasis linux yang ditulis menggunakan bahasa pemrograman java. Sehingga dapat dikatakan bahwa komponen dasar penyusun sistem android tidak jauh berbeda dengan komponen dasar penyusun sistem operasi linux. (Nazruddin Safaat, 2011)

4. Data Recovery

Berdasarkan data dari www.recoverydata.us, yang diakses pertanggal 21 November 2015, bahwa kasus kehilangan data yang paling banyak terjadi umumnya adalah kegagalan logis, yaitu ketika sistem operasi gagal untuk mengenali sistem file, baik disk, partisi atau karena sistem operasinya yang rusak. (Imam,R,2018).

Kasus yang juga umum menyebabkan kehilangan data adalah kesalahan penghapusan file secara tidak sengaja dari harddisk dan dari recycle bin. Apapun penyebabnya, tujuan dari data recovery adalah mengembalikan file yang sudah hilang tersebut kemudian

memindahkannya ke tempat yang aman dengan cara menyalin atau meng-copy. Kemudian proses setelah recovery data bisa ditindaklanjuti dengan pemartisian ulang harddisk dan memindahkan data-data yang berharga ke tempat lain secara terus menerus. Terutama dipisahkan dari tempat sistem operasi berada.

Tipe kerusakan kedua adalah kegagalan di level disk. Misalnya sistem file yang tidak konsisten, partisi yang error atau hard disk yang rusak. Jenis kerusakan tipe kedua ini memungkinkan data sulit untuk dibaca. Dengan tingkat kerusakan yang bervariasi, solusi untuk data recovery bisa beragam dari mulai memperbaiki sistem file, partisi, MBR (master boot record), atau recovery dari sisi hardware. Jika yang rusak adalah hardware-nya maka perbaikan harus digunakan oleh mereka yang kompeten dan menggunakan peralatan yang khusus. Karena fungsinya untuk mengembalikan data yang hilang maka proses data recovery ini bisa digunakan dalam konteks komputer forensik atau untuk mata-mata.

5. Mobiledit Forensik

MOBILedit Forensik adalah suatu software yang berfungsi untuk penyelidikan atau pengambilan data pada smartphone. Software ini dapat membaca pesan, catatan panggilan, membaca SIM card dan lain sebagainya. Versi lite MOBILedit dapat didownload dari internet. Instalasi MOBILedit tidaklah terlampau sulit. Seperti juga Oxygen, MOBILedit membutuhkan kondisi USB debugging mode enabled di ponsel. (Ahmad,L2016).

Ponsel dapat terkoneksi baik menggunakan kabel langsung maupun menggunakan koneksi wireless. Hal ini memberikan keuntungan untuk jenis ponsel yang tidak dapat didetekesi menggunakan software ini dapat diutilisasi menggunakan koneksi wireless. MOBILedit akan menginstal aplikasi kecil di ponsel untuk menarik data.

6. Autopsy

The Autopsy Forensic Browser merupakan tool analisis investigasi digital dengan command line The Sleuth Kit. Mereka dapat menganalisis disk dan filesistem Windows dan UNIX (NTFS, FAT, UFS1/2, Ext2/3). The Sleuth Kit dan Autopsy bersifat Open Source. Autopsy berbasis HTML, hal ini memungkinkan pengguna untuk melakukan koneksi ke server Autopsy dari sembarang platform dengan menggunakan browser HTML.

Analisis offline terjadi ketika digunakan sistem analisis khusus untuk memeriksa data dari sistem tersangka. Autopsy dan The Sleuth Kit dijalankan dalam lingkungan terpercaya, biasanya dalam sebuah laboratorium.

Analisis hidup (live analysis), terjadi ketika sistem tersangka dianalis ketika sedang berjalan. Dalam hal ini Autopsy dan The Sleuth Kit dijalankan dari sebuah CD (SLAX4) dalam lingkungan yang tidak terpercaya Hal ini sering dilakukan selama proses incident response ketika insiden sedang dikonfirmasi. Setelah ia dikonfirmasi, sistem dapat diambil dan dilakuka analisis offline.

7. FTK Imager

FTK imager merupakan sebuah acquisition tool digital forensik yang dibuat oleh AccessData. FTK Imager dapat digunakan untuk membuat image sebuah drive (physical imaging), membuat image isi sebuah folder, maupun membuat custom image yang terdiri atas file-file yang dipilih saja. Masing-masing opsi sangat berguna di dalam kondisi lapangan yang berbeda-beda dan jenis evidence yang dicari.

8. Hashmyfile

Verifikasi file adalah proses menggunakan algoritme untuk memverifikasi integritas file komputer. Ini dapat dilakukan dengan membandingkan dua file sedikit demi sedikit, tetapi memerlukan dua salinan dari file yang sama, dan mungkin melewatkan kerusakan sistematis yang mungkin terjadi pada kedua file. Pendekatan yang lebih populer adalah membuat hash dari file yang disalin dan membandingkannya dengan hash dari file asli.

Integritas file dapat dikompromikan, biasanya disebut sebagai file yang rusak. File dapat rusak karena berbagai cara: media penyimpanan yang salah, kesalahan pengiriman, kesalahan penulisan selama menyalin atau memindahkan, bug perangkat lunak, dan sebagainya.

Verifikasi berbasis hash memastikan bahwa file tidak rusak dengan membandingkan nilai hash file dengan nilai yang dihitung sebelumnya. Jika nilai ini cocok, file tersebut dianggap tidak dimodifikasi. Karena sifat dari fungsi hash, tabrakan hash dapat menghasilkan positif palsu, tetapi kemungkinan tabrakan sering diabaikan dengan korupsi acak.

B. Penlitian Terdahulu

Pada penelitian yang telah dilakukan sebelumnya yaitu Akuisisi Data Forensik *Google Drive* Pada Android Dengan Metode *National Institute of Justice (NIJ).* Hasil dari penelitian mengurutkan tahapan forensic digital dengan mulai dari *identification, collection, examination, analysis,* dan *reporting* dengan sangat baik. Metode ini banyak digunakan dalam menangani kasus kejahatan digital. Hasil akuisisi kemudian akan di analisa dengan cara menerjemahkan kode-kode *hexsa* hasil akuisisi sehingga menghasilkan barang bukti yang yang bisa di mengerti oleh hakim nantinya. Yudhana, Anton., et al (2016).

Menurut Imam Riadi,2019 pada penelitiannya tentang *Review Proses Forensik Optical Drive Menggunakan Metode National Institute of Justice (NIJ)* Bahwasanya dari jurnal tersebut dapat diambil kesimpulan penelitian menggunkana simulasi investigator akan melakukan proses cloning pada DVD-R yang terlah diformat untuk menghindari perubahan secara fisik dan digital pada barang bukti digital agar tetap autentik. DVD-R yang menjadi objek penelitian dalam sudah diformat sehingga investigator harus menggunakan tools forensik untuk melakukan akuisisi pada DVD-R agar dapat mengambil filefile yang akan dijadikan barang bukti digital lalu akan dijadikan bukti pelaporan pada tahapan akhir metode yang digunakan dan dilakuan hanya satu kali format dilakukan.

Menurut Rusidi Umar,2018 penelitiannya yang berjudul *Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Of Institute Of Justice (NIJ)* 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 analisa 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% yang diperoleh dari 85 file yang disiapkan untuk implementasi dan pengujian dan hasil file dari eksaminasi dan yang berhasil direstorasi hanya 25 file.

Dalam penelitian lain yang dilakukan Syahib, et al. (2018) disebutkan bahwa penelitian ini *volume* ancaman *siber* meningkat, keamanan dalam komputasi awan masih berlangsung area penelitian. Meskipun *cloud computing* sudah menjadi bidang yang menarik bagi penjahat *cyber*, tidak ada penelitian

menyelidiki dampak pada keamanan forensik *cloud*. Artikel ini telah diperkenalkan dan dibandingkan topik komputasi awan dan forensik digital, untuk menggambarkan tumpang tindih mereka. Akhirnya, dampak dari kesiapan forensik cloud pada tingkat keamanan adalah dibahas dan bagaimana kesiapan cloud forensik dapat meningkatkan keamanan *cloud*. Untuk mengurangi kesenjangan antara keamanan dan forensik di lingkungan *cloud*, lebih lanjut perlu dilakukan studi kesiapan persyaratan dan faktor- faktor yang mempengaruhi kesiapan.

Dalam penelitian lain yang dilakukan Yudhana, et al. (2016) disebutkan bahwa penggunaan metode *National Institute of Justice (NIJ)* mengurutkan tahapan forensic digital dengan mulai dari *identification, collection, examination, analysis, dan reporting* dengan sangat baik. Metode ini banyak digunakan dalam menangani kasus kejahatan digital. Hasil akuisisi kemudian akan di analisis dengan cara menerjemahkan kode-kode hexsa hasil akuisisi sehingga menghasilkan barang bukti yang yang bisa di mengerti oleh hakim nantinya.

Dalam penelitian lain yang dilakukan Bhatt, Pranshant., et al. (2016) disebutkan bahwa *Cloud based Storage Drive Forensics* Tahap awal adalah Identifikasi Layanan Cloud dan detail akun pengguna. Ini akan membantu simpatisan untuk memeriksa dan mengidentifikasi lokasi data dan merespons untuk mengamankan data. Pemeriksaan akun *Google Drive* dengan mengambil beberapa kata kunci dan lokasi file umum untuk menemukan informasi yang bermanfaat. Penulis juga dapat menentukan nama pengguna dan Kata Sandi *Google Drive* dari gambar forensik yang simpan. Sungguh luar biasa bahwa *Google Drive Password* beberapa contoh ditemukan sebagai Plaintext di I.E. *(Internet Explorer)* dan beberapa Browser lama lainnya. Tetapi sekarang, hal seperti ditambal oleh Browser tersebut. Baru-baru ini, Penulis hanya dapat menemukan URL Google Drive dan file mana yang mereka akses dan Kata

Sandi tetap dalam Formulir terenkripsi. Di Future Work, Penulis akan menyiapkan Script yang secara langsung mengekstrak URL Spesifik dari Sistem. Ini membantu Penyelidik untuk mengatasi Kelemahan Sistem yang Ada Pengakuan. Merek dagang, nama produk, nama Perusahaan, Cuplikan layar yang direferensikan dalam makalah ini diakui oleh pemiliknya masing-masing.

Dalam penelitian lain yang dilakukan Chang, Ming Sang (2016) disebutkan bahwa *Forensic Investigation of Google Drive on Android* Saat menyelidiki penggunaan penyimpanan cloud, file tahap awal meliputi identifikasi *cloud* akun layanan dan pengguna. Ini memungkinkan peneliti untuk mengidentifikasi lokasi data. Di dalam penelitian, menemukan bahwa penyelidik dapat mengidentifikasi Penggunaan akun *Google Drive* dengan melakukan kata kunci pencarian. Sisa-sisa aktivitas cloud dapat ditemukan di smartphone. Ini bisa berharga bagi forensik penguji. Menemukan sisa-sisa di dalamnya percobaan. Nama pengguna, file cache, dan log aktivitas yang membantu memulihkan file yang dihapus dan data. Mengidentifikasi akun, nama file, konten, dan jejak waktu untuk menentukan detail pengguna dan informasi penyimpanan cloud terkait penggunaan *Google Drive* dalam penelitian. Dengan menentukan sisa-sisa data pada perangkat klien, berusaha untuk meningkatkan efisiensi forensik digital dan investigasi kejahatan.

Dalam penelitian lain yang dilakukan R. Umar. (2018) pada penelitian *"Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)"*, Penelitian ini menggunakan metode "DFRWS yang terdiri dari tahap-tahap sebagai berikut: *Identification, Preservation, Collection, Examinition, Analysis dan Presentation.* Langkah selanjutnya adlaah menjalankan perangkat lunak (FTK Imager) sebagai bahan pendukung untuk mengetahui keamanan pada aplikasi Twitter. Dalam meyakinkan bahwa akun media sosial menjadi nilai yang

merepresentasikan string asli atau akun asli dilakukan dengan analisis data pada direktori laptop. Berdasarkan beberapa hasil dari tahapan-tahapan metode yang telah dilakukan, proses analisis mengenai data pada media sosial Twitter dapat dikatakan bahwa bukti digital berupa barang bukti data yang valid Berdasarkan pada analisa dan perbandingan bukti forensik aplikasi media sosial Facebook dan Twitter pada *Smartphone Android,* Hasil dari penelitian ini menunjukkan bahwa semua bukti forensik pada aplikasi media sosial Facebook berhasil ditemukan semua. Untuk aplikasi media social Twitter hanya berhasil ditemukan berupa nama akun, data lokasi, *photo profile*, *cover photo*, *posting* berupa teks dan posting berupa gambar.