CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 3, No. 2, November 2020, hlm. 12-21

INVESTIGASI FORENSIK TERHADAP BUKTI DIGITAL DALAM MENGUNGKAP *CYBERCRIME*

Moh. Riskiyadi
Program Studi Magister Akuntansi
Universitas Trunojoyo Madura
mohriskiyadi@gmail.com

(Naskah masuk: 13 Oktober 2020, diterima untuk diterbitkan: 31 November 2020)

Abstak

Teknologi yang berkembang pesat sejalan dengan tindakan *cybercrime* yang meningkat drastis, sehingga teknik dan modus baru *cybercrime* sulit untuk dideteksi dan dipecahkan oleh para investigator forensik digital. Tujuan dari penelitian ini adalah memberikan referensi terkait dengan kehandalan *tools digital forensic* dalam mengungkap *cybercrime* agar diperoleh bukti digital yang berintegritas, handal dan legal dalam proses ligitasi. Penelitian ini menggunakan metode *static forensic* dengan *framework* dari *National Institute of Justice* (NIJ) dengan skenario kasus *cybercrime* berupa *carding* dengan bukti elektronik *flash disk* menggunakan *tools digital forensic FTK Imager* dan *Autospy*. Hasil penelitian ini menunjukkan penggunaan *FTK Imager* dan *Autospy* mampu mengakuisisi dan menganalisis file yang dihapus permanen maupun file yang tersimpan sebelum *flash disk* diformat ulang. Sedangkan penghapusan permanen dan penggunaan *password* pada *flash disk* dengan *tools BitLocker Drive Encryption*, kedua *tools* tersebut tidak dapat mengakuisisi dan menganalisis file yang dihapus permanen ataupun diformat ulang. Batasan penelitian ini termuat pada penentuan metode *static forensic* dengan *framework* dari *National Institute of Justice* (NIJ) serta penentuan objek bukti elektronik *flash disk* dan *tools FTK Imager* dan *Autospy*. Untuk menunjang hasil penelitian ini diperlukan penelitian lanjutan tentang metode atau *tools digital forensic* lain yang lebih handal, sehingga pengungkapan bukti digital atas tindakan *cybercrime* serupa dapat diselesaikan. Penelitian ini benar dilakukan oleh peneliti dengan pengembangan literatur dan penelitian terdahulu sebagai desain penelitian.

Kata kunci: *cybercrime, tools digital forensic, static forensic, flash disk, bukti digital*.

FORENSIC INVESTIGATION OF DIGITAL EVIDENCE TO REVEALING CYBERCRIME

Abstract

Technology that is developing rapidly in line with cybercrime actions is increasing dramatically, so that the techniques and new modes of cybercrime are difficult to detect and solve by digital forensic investigators. The purpose of this study is to provide references related to the reliability of digital forensic tools in revealing cybercrime in order to obtain digital evidence of integrity, reliability and legal in the litigation process. This study uses a static forensic method with a framework from the National Institute of Justice (NIJ) with cybercrime case scenarios in the form of carding with flash disk electronic evidence using digital forensic tools FTK Imager and Autospy. The results of this study indicate the use of FTK Imager and Autospy is able to acquire and analyze files that are permanently deleted or files that are stored before the flash disk is reformatted. While the permanent deletion and use of passwords on a flash disk with BitLocker Drive Encryption tools, the two tools cannot acquire and analyze files that are permanently deleted or reformatted. The limitation of this research is the determination of the static forensic method with the framework of the National Institute of Justice (NIJ) as well as the determination of electronic flash disk evidence objects and FTK Imager and Autospy tools. To support the results of this study, further research is needed on methods or other digital forensic tools that are more reliable, so that the disclosure of digital evidence of similar cybercrime actions can be completed. This research was actually carried out by researchers with the development of literature and previous research as a research design.

Keywords*: cybercrime, digital forensic tools, static forensic, flash disk, digital evidence.*

1. PENDAHULUAN

Teknologi yang meningkat pesat memberikan manfaat dan dampak yang sama besar bergantung dari pengguna dari teknologi tersebut. Manfaat positif yang dapat diperoleh dari teknologi adalah memudahkan individu atau kelompok dalam melakukan aktifitasnya, sedangkan dampak negatif timbul karena penyalahgunaan teknologi oleh individu atau kelompok untuk tindakan kejahatan dunia maya (*cybercrime*) yang dapat merugikan orang lain (Akbar and Riadi, 2019; Gani, 2018; dan Hasa, Yudhana and Fadlil, 2019). Kemajuan teknologi yang semakin pesat juga diiringi dengan sistem keamanan yang semakin meningkat sebagai respon dari tindakan *cybercrime* yang semakin meningkat drastis. Akibatnya pelaku *cybercrime* selalu lebih aktif dan cepat membuat terobosan baru terhadap sistem keamanan yang dibentuk oleh anti *cybercrime*. Kondisi yang sangat menghawatirkan terjadi apabila pelaku *cybercrime* adalah ahli juga dalam tindakan anti *cybercrime*, sehingga modus baru *cybercrime* sulit untuk dideteksi dan dipecahkan oleh para investigator forensik digital.

Guna memberikan payung hukum dalam mengantisipasi ancaman kejahatan *cybercrime* di Indonesia telah diberlakukan regulasi yang mengatur yaitu UU 11/2008 tentang Informasi dan Transaksi Elektronik (ITE) yang telah diubah dengan UU 19/2016 (Rifauddin and Halida, 2018). Kehadiran regulasi te juga sebagai solusi dan pengakuan bahwa alat bukti elektronik dapat dijadikan sebagai alat bukti yang sah dalam proses ligitasi sebagaimana tertuang dalam Pasal 54 Ayat (1) dan legalitas dari alat bukti tersebut tertuang dalam Pasal 44 dan Pasal 5, yang mana sebelum regulasi ini terbit, KUHAP belum mengatur secara tegas berkenaan dengan alat bukti elektronik. Mengacu pada ketentuan pembuktian sebagaimana diatur dalam KUHAP, harus ada alat penguji yang handal dan memadai atas alat bukti elektronik, sehingga alat bukti tersebut dapat diakui secara sah dalam proses ligitasi sama halnya dengan alat bukti lainnya, yaitu persyaratan formil dan materiil harus dipenuhi (Handoko, 2016; Jayantari and Sugama, 2019; dan Pribadi, 2018).

Cybercrime pada umumnya meninggalkan jejak (*history*) dari aktivitas kejahatan yang dilakukan sehingga dapat dijadikan sebagai barang bukti (Rosalina, Suhendarsah & Natsir, 2016). Barang bukti dalam kasus *cybercrime* terbagi menjadi dua kriteria, yaitu barang bukti elektronik dan barang bukti digital. Barang bukti elektronik adalah barang bukti yang berbentuk fisik dari suatu perangkat elektronik atau perangkat penyimpanan *(storage device)*. Barang bukti digital adalah barang bukti berupa *file* dokumen, *file history*, atau *file log* yang berisi data terkait dengan suatu kasus *cybercrime* yang diperoleh dari ekstraksi *file* pada barang bukti elektronik (Riadi, Umar & Nasrulloh, 2018).

Barang bukti dari kasus *cybercrime* berbeda dengan kejahatan konvensional, dimana penanganan atas bukti elektonik maupun bukti digital yang termuat didalamnya rentan mengalami perubahan atau kontaminasi, sehingga bukti elektronik harus dipacking dan disimpan dengan baik di tempat yang aman (Ivanović, 2018). Dalam mengatasi kondisi tersebut penanganan atas bukti digital diperlakukan khusus dibandingkan dengan bukti fisik pada kejahatan konvensional yang lebih dikenal dengan *chain of custody* (Prayudi, 2014; dan Prayudi, Luthfi and Pratama, 2014). Meskipun demikian sampai saat ini belum tersedia alat (*tools*) atau *software* yang mampu secara komprehensif dan menyeluruh dapat mengimplementasikan konsep dari *digital chain of custody* (Jain & Kalbande, 2015). *Tools* yang ada umumnya hanya mampu menangani bagian tertentu dari investigasi bukti digital, tetapi tidak berorientasi pada konsep investigasi forensik digital secara keseluruhan. Sehingga untuk menerapkan konsep *digital chain of custody* agar diperoleh bukti digital yang potensial dan kuat serta mampu dipertahankan dalam proses ligitasi, harus dipilih *tools* yang handal di setiap tahapan dari *digital chain of custody* (Kao et al., 2018; dan Masvosvere and Venter, 2016).

Disamping metode penanganan bukti digital dengan *tools* yang telah tersedia berdasarkan konsep *digital chain of custody*, hal penting lainnya adalah dengan hadirnya lembaga yang menaungi segala aktifitas investigasi kriminal dunia maya (*cybercrime*). Peranan dari lembaga ini adalah menganalisis konsep, proyek terkait investigasi forensik digital, *tools* dan dukungan hukum di bidang *cybercrime* dalam rangka merepresentasikan bukti digital yang berintegritas sehingga dapat diterima dalam proses ligitasi (Granja & Rafael, 2015).

Berbagai penelitian tentang *cybercrime* yang berhubungan dengan prosedur investigasi forensik digital telah banyak dibahas dan memberikan banyak pilihan metode yang dapat diterapkan. Selanjutnya prosedur investigasi dapat diperbandingkan terkait dengan kompatibilitas prosedur investigasi tradisional, analisis perilaku *cybercrime*, prosedur investigasi forensik terhadap bukti, analisis dan verifikasi kasus, metode pengumpulan dan analisis bukti serta prosedur yuridis peradilannya (Sun, Shih & Hwang, 2015). Berkaitan dengan prosedur atau metode investigasi yang dipilih, legalitas dan proses penguasaan bukti elektonik, penggunaan *tools*, aspek hukum di setiap tahapan dari prosedur yang ditetapkan dan investigator yang terlibat dalam menangani bukti digital menjadi kunci utama dalam keberhasilan investigasi forensik digital. Seluruh persyaratan tersebut harus terpenuhi secara komprehensif agar bukti digital yang diperoleh handal dalam proses ligitasi (Hoolachan & Glisson, 2010).

Penelitian tentang teknik investigasi forensik digital yang meliputi *static forensic* dan *live forensic* berhubungan dengan kasus yang lebih spesifik terkait dengan alat atau media yang digunakan pelaku dalam melakukan tindakan *cybercrime*, jenis investigasi

forensik dapat berupa *computer forensic, network forensic, mobile forensic, database forensic, multimedia forensic* dan sebagainya telah banyak dilakukaan di Indonesia (Iman, Susanto & Inggi, 2020). Diantaranya penelitian (Hikmatyar & Sugiantoro, 2019) terkait dengan investigasi *computer forensic* atas bukti eletronik yang digunakan dalam tindakan *cybercrime*, penelitian (Handrizal, 2017) tentang teknik investigasi *static forensic* dengan memperbandingkan kinerja dari beberapa *tools digital forensic* dalam mengembalikan data yang yang sengaja dihapus oleh pelaku. Selanjutnya penelitian (Aziz, Riadi & Umar, 2018) dengan teknik atau metode investigasi *live forensic* menggunakan *framework* dari *National Institute of Justice* (NIJ) diperoleh lokasi file *log, cache* dan gambar sebagai bukti digital. Penelitian (Ramadhan, Prayudi & Sugiantoro, 2017) dengan teknik *static forensic* pada *SSD* yang mengaktifkan (*enable*) fitur TRIM menggunakan tools *Autospy* tidak dapat merecovery file. Hasil penelitian tersebut didukung oleh penelitian (Riadi, Umar & Nasrulloh, 2018) dengan teknik investigasi *static forensic* dan perlakuan berbeda pada *Solid State Drive Non-volatile Memory Express* (SSD NVMe) dengan mengaktifkan (*enable*) dan tidak fitur TRIM menggunakan *tools FTK Imager, Recover My File* dan *Autospy* diperoleh hasil bahwa saat fitur TRIM aktif tidak dapat dilakukan *recovery* data atas file yang dihapus permanen (*shift + delete*). Penelitian sejenis (Albanna & Riadi, 2017) menggunakan metode *static forensic* pada *hard drive* (*hard disk*) yang dibekukan dengan *tools Deepfreeze* menggunakan tools *Autopsy, Winhex, Photorec* dan *Foremost* untuk mengembalikan (*recovery*) file sebelum sistem komputer dimatikan, diperoleh hasil dengan *tools Winhex* mampu merecovery file gambar, file dokumen dan file *log*. Penelitian (Hasa, Yudhana & Fadlil, 2019) dengan metode atau teknik *static forensic* pada *Secure Digital Card (SD Card)* menggunakan *tools FTK Imager* dan *Autopsy* dengan perlakuan hapus permanen (*shift + delete*) dan *wipe* data diperoleh hasil bahwa dengan perlakuan *wipe* data, tidak dapat dilakukan *recovery* data yang telah dihapus. Menurut penelitian (Akbar & Riadi, 2019) dengan metode atau teknik investigasi *static forensic* menggunakan *framework Generic Computer Forensic Investigation Model* (GCFIM) pada *flash disk* dengan memanfaatkan *tools Winhex* untuk proses *cloning* atau *imaging* dan *tools Autospy* untuk menganalisa hasil *cloning* data dari *flash disk*.

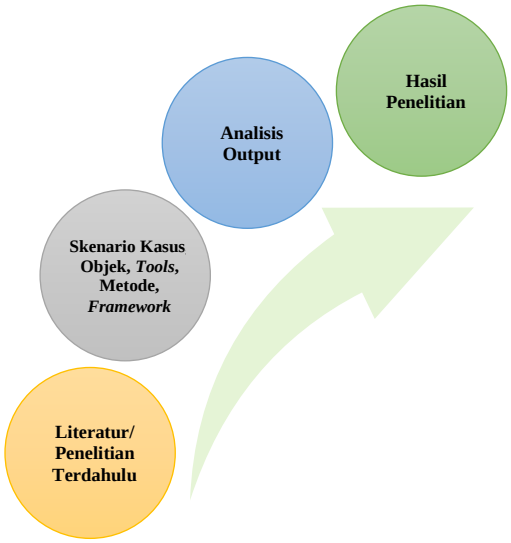
Berdasarkan permasalahan tersebut dan hasil penelitian terdahulu sebagaimana telah diuraikan di atas, penting dilakukan penelitian tentang investigasi forensik bukti digital menggunakan metode *static forensic* dengan *framework National Institute of Justice* (NIJ). Pelaku tindakan *cybercrime* selama ini masih banyak menggunakan *tools* dan komputer dalam melakukan aksinya. *Tools* atau *software* yang digunakan pelaku umumnya disimpan dalam *drive* komputer ataupun media penyimpanan eksternal seperti *flash disk*. Objek yang dipilih dalam penelitian ini adalah bukti elektronik *flash disk* karena fleksibelitas dari *flash disk* yang mudah dibawa serta umum digunakan para pelaku *cybercrime*. Alasan berikutnya adalah objek *flask disk* dapat merepresentasikan media penyimpanan lainnya seperti SD *card*, SSD, HDD komputer dengan ruang penyimpanan yang lebih besar, sehingga menggunakan *flash disk* dengan ruang penyimpanan yang lebih rendah dapat menghemat waktu analisis data dari objek penelitian.

Pembaharuan pada penelitian ini adalah penentuan *tools, framework* dan skenario atau perlakuan pada objek yang berbeda dengan penelitian (Akbar & Riadi, 2019), perbedaan objek, perlakuan pada objek dan *tools* yang digunakan dari penelitian (Albanna & Riadi, 2017; Aziz, Riadi & Umar, 2018; Handrizal, 2017; Hasa, Yudhana & Fadlil, 2019; Ramadhan, Prayudi & Sugiantoro, 2017; dan Riadi, Umar & Nasrulloh, 2018). Dengan pembaharuan ini diharapkan dapat menambah referensi *tools* yang relevan dalam melakukan investigasi forensik digital sesuai dengan kasus *cybercrime* yang terjadi dan mampu mengisi gap riset terdahulu sebagaimana telah dipaparkan sebelumnya. Sehingga pada akhirnya diperoleh bukti digital yang berintegritas, legal dan diterima dalam proses ligitasi.

Tujuan penelitian ini untuk memberikan referensi agar dilakukan pengembangan *tools digital forensic* dan metode investigasi forensik digital ada agar senantiasa memberikan solusi yang tepat dalam pengungkapan bukti digital dari kasus *cybercrime*.

2. METODE PENELITIAN

Desain penelitian ini berasal dari literatur dan hasil penelitian terdahulu, selanjutnya dilakukan inventarisasi atas *gap* penelitian tersebut dengan didukung literatur yang telah ada. Memetakan pembaharuan yang dapat dikembangkan dari hasil penelitian tersebut. Selanjutnya berdasarkan *gap* penelitian terdahulu ditetapkan skenario kasus, objek, metode dan *tools* yang sesuai atas pengembangan penelitian ini. Berikutnya dilakukan analisis atas output *tools* dari objek yang telah ditentukan serta langkah terakhir merepresentasikan hasil analisis tersebut dalam hasil penelitian sebagaimana alur proses pada gambar 1 berikut:



Gambar 1. Alur desain penelitian

Setelah desain penelitian terbentuk, dilakukan pengumpulan dan pemetaan atas literatur dan penelitian terdahulu terkait dengan penelitian investigasi forensik digital sehingga fokus untuk menetapkan metode yang tepat dan sesuai. Adapun metode yang dipilih dalam penelitian ini adalah *static forensic* dengan *framework National Institute of Justice* (NIJ). Penentuan skenario kasus *cybercrime* dihubungkan dengan salah satu bentuk pelanggaran atas UU ITE berupa *cading*. Selanjutnya untuk penentuan bahan dan peralatan serta metode yang digunakan dalam penelitian ini diuraikan sebagai berikut.

2.1. Bahan dan Peralatan

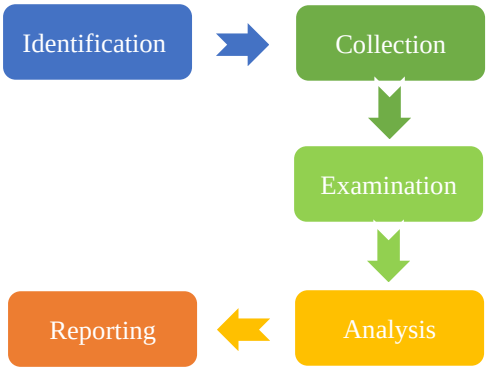
Bahan dan alat yang digunakan yaitu berupa perangkat *hardware* dan *software*, desain skenario kasus dan bukti yang diperoleh, serta pengimplementasian investigasi forensik digital atas kasus dan bukti yang diperoleh dari skenario kasus dimaksud. *Hardware* dan *software* yang digunakan dalam penelitian ini sebagaimana table 1 berikut:

Tabel 1. Tabel *hardware* dan *software* penelitian

No	Hardware/ Software	Spesifikasi/ Keterangan
1	Laptop	Sony Vaio SVF142C1WW Core i3-3217U 1,8Ghz, DDR3 6GB, Windows 10 Home Single Language 64 Bit
2	Flash Disk	SanDisk Cruzer Blade 8GB SDC250-008B B1180724954B
3	BitLoker Encryption	Tools default Windows 10
4	AccsesData FTK Imager	FTK Imager for Windows Versi 4.3.0.18
5	Sleuth Kit Autopsy	Autopsy for Windows Versi 4.14.0

2.2. Metode

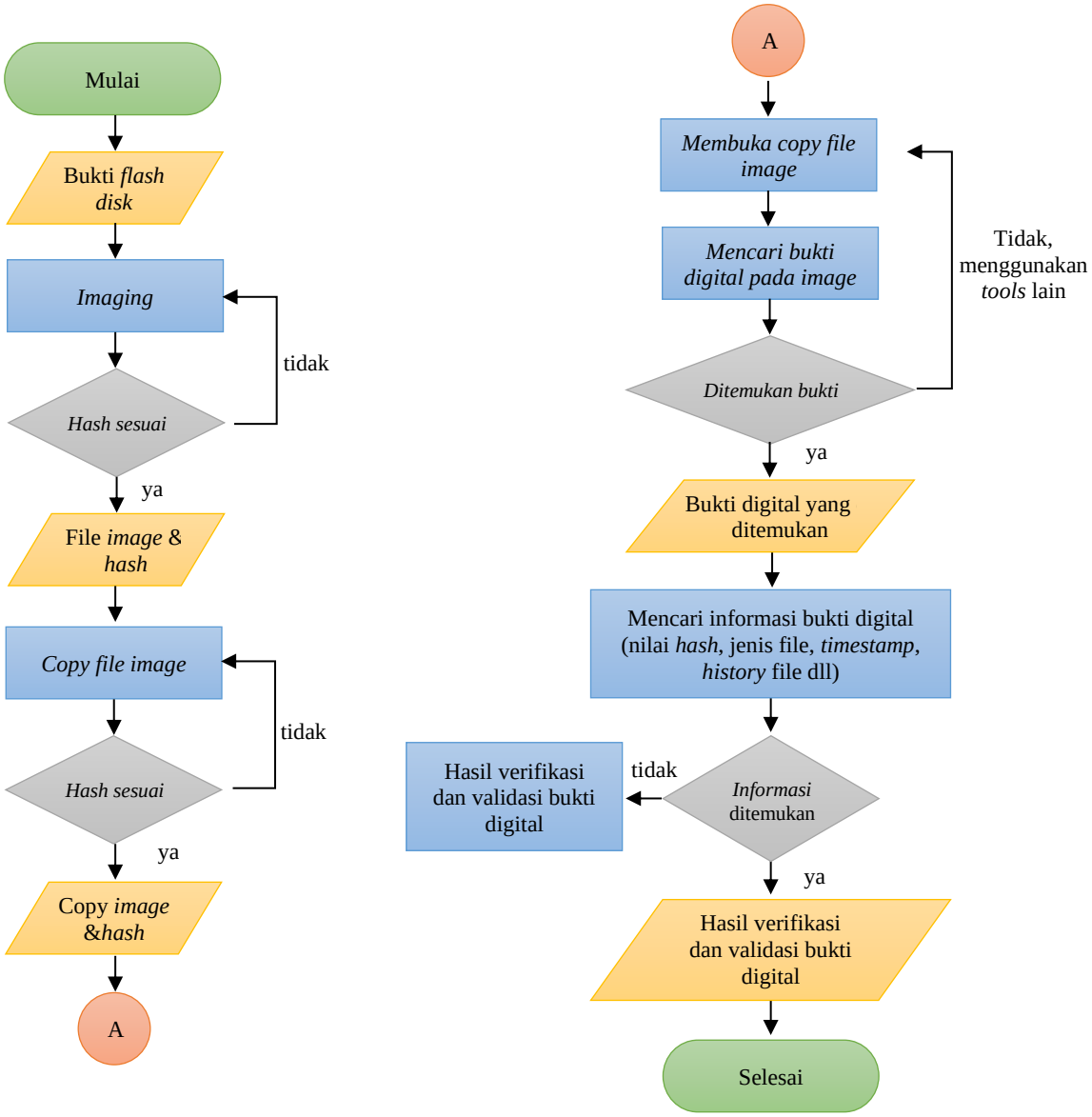
Penelitian ini menggunakan metode *static forensic* dengan menggunakan *framework* NIJ (Aziz, Riadi & Umar, 2018; Hasa, Yudhana & Fadlil, 2019; Riadi, Umar & Nasrulloh, 2018; dan Riadi & Hadi, 2019), dimana metode *forensic static* diproses secara *bit by bit image* dalam proses forensik digital atas barang bukti eletronik pada saat *system running off* atau sistem dalam keadaan tidak beroperasi atau tidak aktif (Ramadhan, Prayudi & Sugiantoro, 2017). Dalam proses penelitian ini dilakukan dengan 5 (lima) tahapan proses forensik, sebagaimana Gambar 2 berikut:



Gambar 2. Tahapan proses *static forensic* dengan *framework* NIJ

Identification adalah proses memilah barang bukti fisik oleh investigator dari tindak kejahatan komputer untuk dijadikan bukti otentik saat proses penyidikan. Proses *identification* berupa pelabelan dan perekaman untuk keutuhan barang bukti fisik. *Collection* adalah proses duplikasi dari barang bukti fisik yang otentik ke bukti digital untuk menjaga integritas barang bukti dari perubahan atau kontaminasi. Proses penjagaan barang bukti fisik dan membuat duplikasi menjadi file *image* ini disebut dengan akuisisi. *Examination* atau pemeriksaan adalah proses ekstraksi hasil *image* sehingga data digital yang ada didalamnya sama dengan barang bukti fisik. Tahapan ini memastikan data yang didapat asli dan akan dicek validasinya dengan menggunakan *hashing*. *Analysis* adalah proses pengecekan barang bukti digital yang telah didapat dari proses eksaminasi, barang bukti digital diproses secara detail sesuai pelaporan tindak kejahatan untuk mengungkap kasus tindak kejahatan dengan metode yang benar secara ilmiah dan dapat dipertanggungjawabkan secara sah menurut hukum. *Reporting* adalah proses pembuatan laporan, hasil laporan analisis menggambarkan tindakan yang dilakukan oleh pelaku kriminal, penjelasan *tools* yang dipakai dan metode yang digunakan (Hasa, Yudhana

& Fadlil, 2019). Tahapan *indetification*, *collection*, *examination*, *analysis* dan *reporting* digambarkan dalam flowchat sebagaimana gambar 3 berikut.



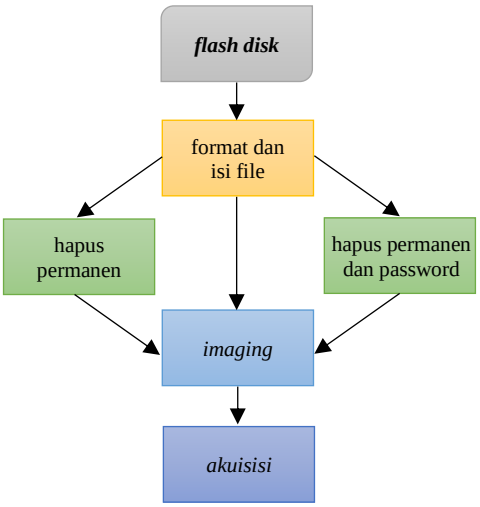
Gambar 3. Flowchat *indetification*, *collection*, *examination*, *analysis* dan *reporting* dari *framework NIJ*

Objek yang menjadi fokus pada penelitian ini yaitu *USB flash drive (flash disk).* Penentuan objek penelitian menggunakan *flash disk* karena media penyimpanan tersebut masih menjadi pilihan utama pengguna media elektronik dalam melakukan penyimpanan data atau file yang dikelolalnya. Disamping itu, barang bukti elektronik tersebut merupakan barang bukti yang sangat potensial dalam kasus *cybercrime* yang memuat informasi seperti file catatan, dokumen, gambar atau foto, pesan email, riwayat internet, catatan obrolan dan daftar teman, database, catatan peristiwa dan sebagainya yang dapat dijadikan bukti digital dalam investigasi atau penuntutan forensik digital.

Dalam penelitian ini dibuat suatu skenario tindakan *cybercrime* berupa *carding*, yaitu tindakan menggunakan nomor dan identitas kartu kredit milik orang lain yang diperoleh secara ilegal dan pada umumnya diperoleh dengan mencuri data pemilik kartu kredit di internet. Tindakan *carding* yang diskenariokan dalam penelitian ini adalah pelaku yang memperoleh data kartu kredit dari pihak lain dan tidak melakukan *phising* sendiri. Tindakan *cybercrime* yang demikian melanggar ketentuan Pasal 32 Ayat (1) UU 11/2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan UU 19/2016 yang pada intinya pelaku yang sengaja dan tidak miliki hak atau tindakan melanggar hukum dengan cara apapun melakukan perubahan baik penambahan maupun pengurangan, menghilangkan, menyembunyikan, pemindahan atau transmisi, pengrusakan atas suatu informasi elektronik atau dokumen elektronik yang dimiliki orang lain atau publik.

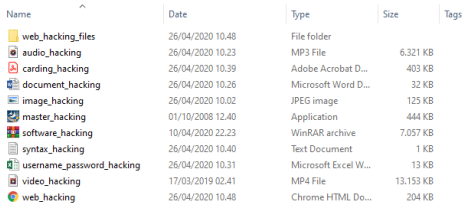
Berdasarkan tindakan *cybercrime* tersebut telah dilakukan penyitaan alat bukti eletronik diantaranya berupa *flash disk*, yang selanjutanya dijadikan simulasi dalam penelitian ini. Pelaku tindakan *cybercrime* pada umumnya dalam melakukan aksinya mempassword (enkripsi) media penyimpanan yang digunakan serta melakukan penghapusan permanen atas file yang digunakan dalam melakukan tindakannya dengan tujuan untuk menghilangkan jejak kejahatan.

Software yang digunakan sebagai *tools digital forensic* pada penelitian ini adalah *FTK Imager* dan *Autopsy* sebagai *tools* untuk mengembalikan data (*recovery data*), adapun penggunaan *software* ini dipilih karena merupakan software yang handal dalam melakukan analisis forensik digital serta gratis untuk digunakan. *Software FTK Imager* digunakan untuk melakukan *imaging* data serta membandingkan *hashing* file *imange* dengan bukti elektronik *flash disk* dan *Autopsy* digunakan untuk menganalisis hasil *imaging* dari *flash disk*. Skenario atas objek bukti elektronik *flash disk* ditunjukkan gambar 4 berikut:



Gambar 4. Skema simulasi perlakuan atas *flash disk* sesuai skenario

Flash disk sebagai simulai dalam penelitian ini sebelumnya dilakukan *quick format* menggunakan *file system* FAT32, selanjutnya *flash disk* diisi dengan beberapa file berekstensi docx, xlsx, pdf, jpg, mp3, mp4, rar, txt, exe, html dan forlder dari hasil penyimpanan dari *website*. File yang disalin kedalam *flash disk* sebagaimana gambar 5 berikut:



Gambar 5. File simulasi dalam *flash disk*

Selanjutnya dilakukan tiga perlakuan berbeda atas *flash disk* tersebut, yaitu seluruh file dilakukan penyalinan (*copy* + *paste*) ke *flash disk*, selanjutnya dilakukan *imaging* data secara *physical drive* dari *flash disk* yang menjadi target menggunakan *FTK Imager*. Proses *imaging* data secara *physical drive* dipilih agar seluruh informasi dari *flash disk* dapat termuat dalam hasil *imaging*. Selanjutnya dilakukan analisa atas hasil *imaging* data tersebut.

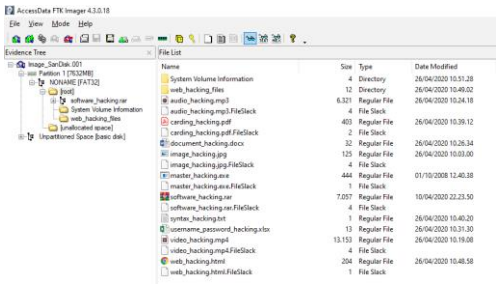
Perlakuan berikutnya adalah dilakukan penghapusan permanen (*shift* + *delete*) seluruh file yang tersimpan dalam *flash disk* dan dilakukan hal serupa berupa imaging data dan analisis data.

Perlakuan terakhir atas *flash disk* adalah dilakukan *password* (enkripsi) atas *flash disk* dengan memanfaatkan *tools BitLocker Drive Encryption* yang merupakan *tools default* dari Windows 10. Selanjutnya dilakukan proses *imaging* data secara *phical drive* dan dilakukan analisis data.

3. HASIL DAN PEMBAHASAN

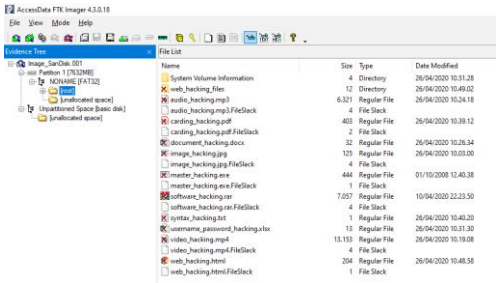
Tahap awal dalam penelitian ini adalah proses *acquisition* yaitu proses *imaging* dengan menggunakan *software FTK Imager*. Proses ini dilakukan untuk mengakuisisi data dan file yang tersimpan dalam barang bukti elektronik atau media penyimpanan *flash disk* sebagaimana skenario kasus yang telah ditentukan. Proses dilakukan dengan menghubungkan *flash disk* melalui port USB pada laptop, selanjutnya menjalankan *software FTK Imager* untuk memulai proses *imaging* data dari *flash disk.*

Proses *imaging* data secara *physical drive* dengan *FTK Imager* pada *flash disk* sebagaimana perlakuan pertama. Hasil dari proses *imaging* data pada *flash disk* dapat dilihat pada gambar 6 berikut ini:



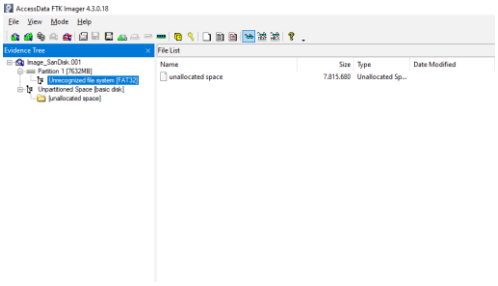
Gambar 6. Hasil *imaging* data secara *physical drive* dengan perlakuan pertama

Proses *imaging* data secara *physical drive* dengan *FTK Imager* pada *flash disk* dengan cara menghapus permanen (*shift + delete*) seluruh data dapat dilihat pada gambar 7 berikut ini:



Gambar 7. Hasil *imaging* data secara *physical drive* dengan perlakuan kedua.

Proses *imaging* data secara *physical drive* dengan *FTK Imager* pada *flash disk* dengan cara menghapus permanen (*shift + delete*) seluruh data serta dilakukan enkripsi (*password*) atas *flash disk* menggunakan *BitLocker Drive Encryption* dapat dilihat pada gambar 8 berikut ini:

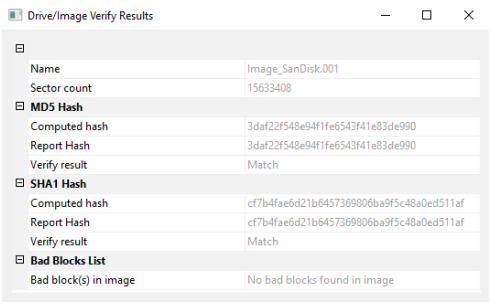


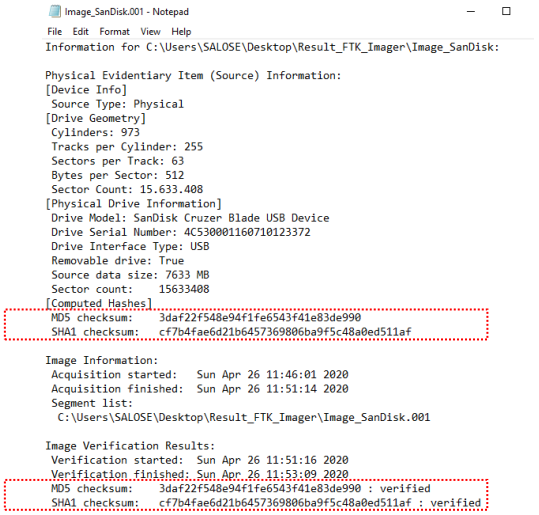
Gambar 8. Hasil *imaging* data secara *physical drive* dengan perlakuan ketiga

Berdasarkan tiga perlakuan sebagaimana hasil *imaging* dengan *FTK Imager*, seluruh file yang dihapus permanen menggunakan perlakuan kedua masih dapat diakusisi yang terletak di folder [root], sedangkan dengan perlakuan ketiga yaitu menghapus permanen seluruh file serta *password flash disk* dengan *BitLocker Drive Encryption* tidak dapat mengakuisisi satu file pun dan folder [root] tidak ada.

Proses berikutnya adalah *examination* yang bertujuan untuk mengungkap dengan melakukan analisis atas hasil dari tahap *acquisition* untuk memperoleh data yang diharapkan sebagai bukti digital. Proses *examination* diproses dengan *software FTK Imager* berdasarkan file *image.* Proses dilakukan dengan mencari data atau *file* yang tersembunyi atau dihapus pada *flash disk* oleh pelaku. Selanjutnya dilakukan dokumentasi terhadap data atau *file* yang telah ditemukan.

Proses *examination* data menggunakan *FTK Imager* atas *file image* dengan perlakuan pertama diperoleh seluruh jenis file dan *metadata file*, serta diperoleh *hash* yang sesuai, sebagaimana gambar 9 berikut ini:





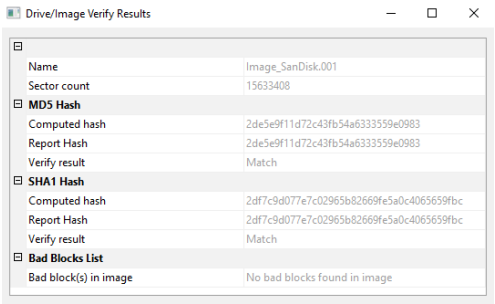
Image_SanDisk.001 - Notepad

File Edit Format View Help

```
Information for C:\Users\SALOSE\Desktop\Result_FTK_Imager\Image_SanDisk:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 973
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.633.408
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Blade USB Device
 Drive Serial Number: 4C530001160710123372
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7633 MB
 Sector count:    15633408
[Computed Hashes]
 MD5 checksum:    3daf22f548e94f1fe6543f41e83de990
 SHA1 checksum:   cf7b4fae6d21b6457369806ba9f5c48a0ed511af

Image Information:
 Acquisition started:   Sun Apr 26 11:46:01 2020
 Acquisition finished:  Sun Apr 26 11:51:14 2020
 Segment list:
  C:\Users\SALOSE\Desktop\Result_FTK_Imager\Image_SanDisk.001

Image Verification Results:
 Verification started:  Sun Apr 26 11:51:16 2020
 Verification finished: Sun Apr 26 11:53:09 2020
 MD5 checksum:    3daf22f548e94f1fe6543f41e83de990 : verified
 SHA1 checksum:   cf7b4fae6d21b6457369806ba9f5c48a0ed511af : verified
```

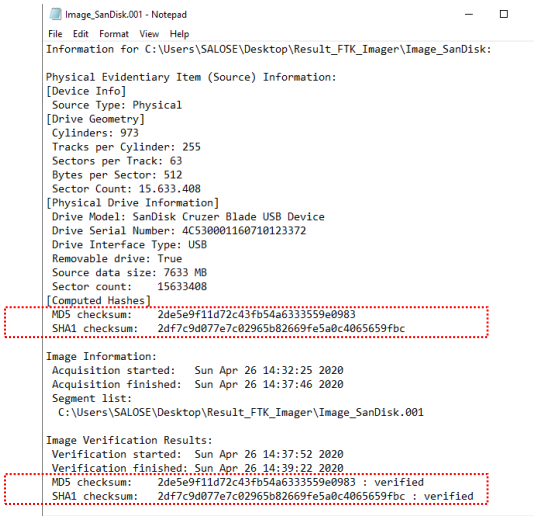
Gambar 9. Hasil *examination* dengan *FTK Imager* pada perlakuan pertama

Hasil *examination* dengan *FTK Imager* atas file *image* dengan perlakuan kedua diperoleh seluruh jenis file dan *metadata file* serta diperoleh *hash* yang sesuai, sebagaimana gambar 10 berikut ini:



Drive/Image Verify Results

Name	Image_SanDisk.001
Sector count	15633408
MD5 Hash	
Computed hash	2de5e9f11d72c43fb54a6333559e0983
Report Hash	2de5e9f11d72c43fb54a6333559e0983
Verify result	Match
SHA1 Hash	
Computed hash	2df7c9d077e7c02965b82669fe5a0c4065659fbc
Report Hash	2df7c9d077e7c02965b82669fe5a0c4065659fbc
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image



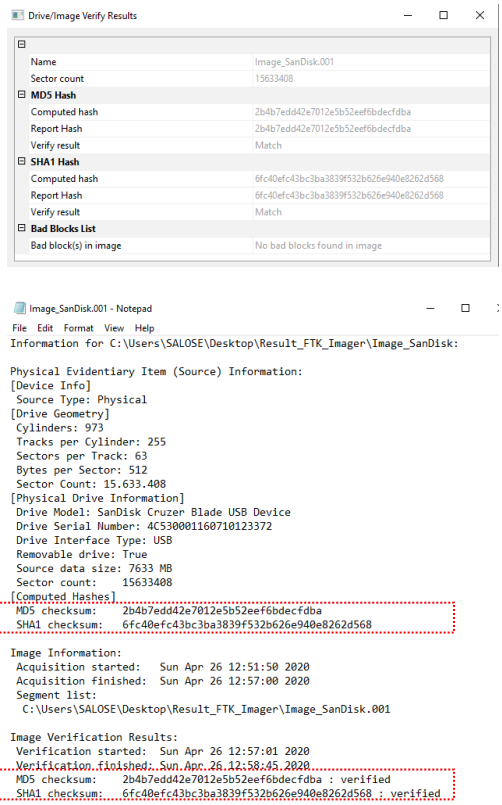
Image_SanDisk.001 - Notepad

File Edit Format View Help

```
Information for C:\Users\SALOSE\Desktop\Result_FTK_Imager\Image_SanDisk:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 973
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.633.408
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Blade USB Device
 Drive Serial Number: 4C530001160710123372
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7633 MB
 Sector count:    15633408
[Computed Hashes]
 MD5 checksum:    2de5e9f11d72c43fb54a6333559e0983
 SHA1 checksum:   2df7c9d077e7c02965b82669fe5a0c4065659fbc

Image Information:
 Acquisition started:   Sun Apr 26 14:32:25 2020
 Acquisition finished:  Sun Apr 26 14:37:46 2020
 Segment list:
  C:\Users\SALOSE\Desktop\Result_FTK_Imager\Image_SanDisk.001

Image Verification Results:
 Verification started:  Sun Apr 26 14:37:52 2020
 Verification finished: Sun Apr 26 14:39:22 2020
 MD5 checksum:    2de5e9f11d72c43fb54a6333559e0983 : verified
 SHA1 checksum:   2df7c9d077e7c02965b82669fe5a0c4065659fbc : verified
```

Gambar 10. Hasil *examination* dengan *FTK Imager* dengan perlakuan kedua

Hasil *examination* dengan *FTK Imager* atas file *image* dengan perlakuan ketiga tidak diperoleh satupun file yang dihapus permanen serta diperoleh *hash* yang sesuai, sebagaimana gambar 11 berikut ini:



Drive/Image Verify Results

Name	Image_SanDisk.001
Sector count	15633408
MD5 Hash	
Computed hash	2b4b7edd42e7012e5b52eef6bdecfdba
Report Hash	2b4b7edd42e7012e5b52eef6bdecfdba
Verify result	Match
SHA1 Hash	
Computed hash	6fc40efc43bc3ba3839f532b626e940e8262d568
Report Hash	6fc40efc43bc3ba3839f532b626e940e8262d568
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

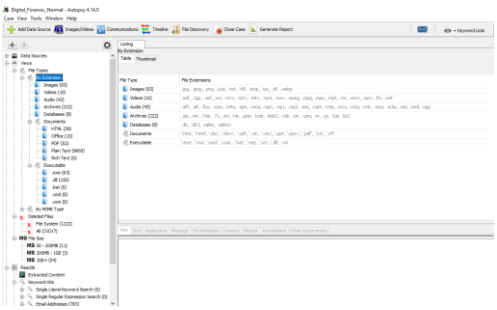
Image_SanDisk.001 - Notepad

File Edit Format View Help

```
Information for C:\Users\SALOSE\Desktop\Result_FTK_Imager\Image_SanDisk:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 973
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15.633.408
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Blade USB Device
 Drive Serial Number: 4C530001160710123372
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7633 MB
 Sector count:    15633408
[Computed Hashes]
 MD5 checksum:    2b4b7edd42e7012e5b52eef6bdecfdba
 SHA1 checksum:   6fc40efc43bc3ba3839f532b626e940e8262d568

Image Information:
 Acquisition started:   Sun Apr 26 12:51:50 2020
 Acquisition finished:  Sun Apr 26 12:57:00 2020
 Segment list:
  C:\Users\SALOSE\Desktop\Result_FTK_Imager\Image_SanDisk.001

Image Verification Results:
 Verification started:  Sun Apr 26 12:57:01 2020
 Verification finished: Sun Apr 26 12:58:45 2020
 MD5 checksum:    2b4b7edd42e7012e5b52eef6bdecfdba : verified
 SHA1 checksum:   6fc40efc43bc3ba3839f532b626e940e8262d568 : verified
```

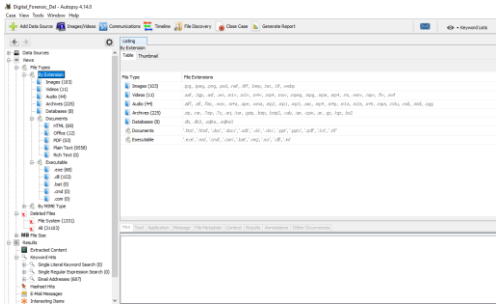
Gambar 11. Hasil *examination* dengan *FTK Imager* dengan perlakuan ketiga

Proses *analysis* dari file *image* yang telah dilakukan *examination* dengan *tools Autopsy* untuk perlakuan yang pertama diperoleh hasil seluruh file untuk selanjutnya dapat dijadikan bukti digital dalam proses ligitasi sebagaimana gambar 12 berikut:



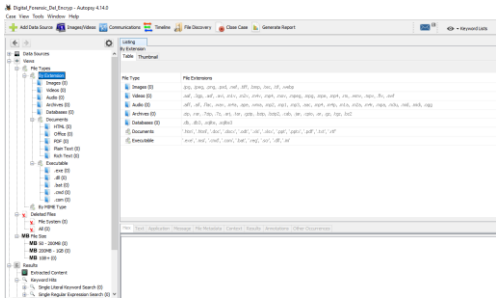
Gambar 12. Hasil *analysis* dengan *Autospy* dengan perlakuan pertama

Proses *analysis* dari file *image* yang telah dilakukan *examination* dengan *tools Autopsy* untuk perlakuan yang kedua diperoleh hasil seluruh file untuk selanjutnya dapat dijadikan bukti digital dalam proses ligitasi sebagaimana gambar 13 berikut:



Gambar 13. Hasil *analysis* dengan *Autospy* dengan perlakuan kedua

Proses *analysis* dari file *image* yang telah dilakukan *examination* dengan *tools Autopsy* untuk perlakuan yang ketiga tidak diperoleh hasil satu file pun, sebagaimana gambar 14 berikut:



Gambar 14. Hasil *analysis* dengan *Autospy* dengan perlakuan ketiga

Berdasarkan hasil *analysis* menggunakan *Autospy* atas file *image* dengan *FTK Imager* pada *flash disk*, berikut perbandingan hasil temuan file untuk masing-masing perlakuan:

1. Perlakuan pertama yaitu tanpa dilakukan penghapusan atas file-file simulasi, diperoleh hasil seluruh file simulasi terdeteksi, sekaligus dengan file-file yang pernah ada dalam *flash disk* sebelum dilakukan format ulang, adapun file simulasi tersebut adalah: masing-masing 1 file untuk file berekstensi (docx, xlsx, pdf, jpg, mp3, mp4, rar, txt, exe, html) dan 1 forlder memuat (9 css, 11 html, 22 js.download, 4 *non extention*, 1 gif, 2 jpeg, 7 jpg. 1 php, 8 png dan 9 txt).
2. Perlakuan kedua yaitu menghapus pemanen (*shift* + *delete*) seluruh file simulasi, diperoleh hasil seluruh file simulasi terdeteksi, sekaligus dengan file-file yang pernah ada dalam *flash disk* sebelum dilakukan format ulang, adapun file simulasi tersebut adalah: masing-masing 1 file untuk file berekstensi (docx, xlsx, pdf, jpg, mp3, mp4, rar, txt, exe, html) dan 1 forlder memuat (9 css, 11 html, 22 js.download, 4 *non extention*, 1 gif, 2 jpeg, 7 jpg. 1 php, 8 png dan 9 txt).
3. Perlakuan ketiga, yaitu dengan menghapus pemanen (*shift* + *delete*) seluruh file serta mengpassword *flash disk* dengan *tools* bawaan Windows 10 *BitLocker Drive Encryption*, tidak terdeteksi file apapun.

4. KESIMPULAN

Berdasarkan hasil penelitian dari proses investigasi forensik bukti digital dari bukti elektronik *flash disk*, perbedaan perlakuan pada *flash disk* memberikan hasil yang berbeda, yang ditunjukkan dengan nilai *hash* yang berbeda dari masing-masing perlakuan. Hasil analisis file untuk perlakuan yang pertama dan kedua, seluruh file simulasi serta file-file lainnya yang pernah disimpan dalam *flash disk* sebelum dilakukan format ulang dapat terdeteksi atau terecovery, sedangkan dengan perlakuan ketiga tidak ditemukan jenis file apapun. *Tools FTK Imager* dan *Autopsy* masih belum mampu melakukan akuisisi dan analisis data dengan perlakuan penghapusan permanen dan enkripsi (*password*) pada *flash disk* menggunakan *tools* bawaan *Windows 10* yaitu *BitLocker Drive Encryption.*

Saran untuk penelitian selanjutnya adalah memetakan skenario lain yang mungkin dilakukan oleh pelaku *cybercrime* pada bukti elektronik dan bukti digital serta penggunaan *tools digital forensic* lain untuk mengatasi permasalahan penanganan bukti digital dalam penelitian ini. Bukti elektronik dan bukti digital harus ditangani sesuai dengan prosedur yang tepat dan legal agar bukti yang dihasilkan dari hasil investigasi forensik digital dapat dijadikan bukti digital yang handal dan legal dalam proses ligitasi *cybercrime.*

DAFTAR PUSTAKA

AKBAR, M.H. & RIADI, I., 2019. Analisis Bukti Digital pada Flash Disk Drive Menggunakan Metode Generic Computer Forensic Investigation Model (GCFIM). *Seminar Nasional Teknologi Fakultas Teknik Universitas Krisnadwipayana*, pp.715–723.

ALBANNA, F. & RIADI, I., 2017. Forensic Analysis of Frozen Hard Drive Using Static Forensics Method. *International Journal of Computer Science and Information Security (IJCSIS)*, 15(1), pp.173–178.

AZIZ, M.A., RIADI, I. & UMAR, R., 2018. Analisis Forensik Line Messenger Berbasis Web Menggunakan Framework National Institute of Justice. *Seminar Nasional Informatika 2018 (semnasIF 2018)*, 1(1), pp.51–57.

GANI, A.G., 2018. Cybercrime (Kejahatan Berbasis Komputer). *JSI (Jurnal sistem Informasi) Universitas Suryadarma*, 5(1), pp.16–29.

GRANJA, F.M. & RAFAEL, G.D.R., 2015. Preservation of Digital Evidence: Application in Criminal Investigation. In: *2015 Science and Information Conference (SAI)*. [online] 2015 Science and Information Conference (SAI). London, United Kingdom: IEEE.pp.1284–1292. Available at:

<http://ieeexplore.ieee.org/document/7237309/> [Accessed 22 Apr. 2020].

HANDOKO, C., 2016. Kedudukan Alat Bukti Digital dalam Pembuktian Cybercrime di Pengadilan. *Jurisprudence*, 6(1), pp.1–15.

HANDRIZAL, H., 2017. Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete Dan Recuva Data Recovery Untuk Digital Forensik. *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, 1(1), p.84.

HASA, M.F., YUDHANA, A. & FADLIL, A., 2019. Analisis Bukti Digital pada Storage Secure Digital Card Menggunakan Metode Static Forensic. *Jurnal Mobile and Forensics (MF)*, 1(2), pp.22–30.

HIKMATYAR, F.G. & SUGIANTORO, B., 2019. Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases. *IJID (International Journal on Informatics for Development)*, 7(2), p.19.

HOOLACHAN, S.A. & GLISSON, W.B., 2010. Organizational Handling of Digital Evidence. *ADFSL Conference on Digital Forensics, Security and Law*, pp.33–44.

IMAN, N., SUSANTO, A. & INGGI, R., 2020. Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review). *Jurnal Telekomunikasi dan Komputer*, 9(3), p.186.

IVANOVIĆ, A., 2018. The Way of Handling Evidence of Criminal Offences of Computer Crime. *Criminal Justice and Security in Central and Eastern Europe*.

JAIN, N. & KALBANDE, D.R., 2015. Computer Forensic Tool Using History and Feedback Approach. In: *2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions)*. [online] 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions). Noida, India: IEEE.pp.1–5. Available at: <http://ieeexplore.ieee.org/document/7359315/> [Accessed 26 Apr. 2020].

JAYANTARI, I.G.A.S. & SUGAMA, I.D.G.D., 2019. Kekuatan Alat Bukti Dokumen Elektronik dalam Tindak Pidana Berbasis Teknologi dan Informasi (Cyber Crime). *e-Jurnal Ilmu Hukum Kertha Wicara*, 8(6), pp.1–16.

KAO, D.-Y., CHAO, Y.-T., TSAI, F., & HUANG, C.-Y., 2018. Digital Evidence Analytics Applied in Cybercrime Investigations. In: *2018 IEEE Conference on Application, Information and Network Security (AINS)*. [online] 2018 IEEE Conference on Application, Information and Network Security (AINS). Langkawi, Malaysia: IEEE.pp.111–116. Available at: <https://ieeexplore.ieee.org/document/8631403/> [Accessed 17 Apr. 2020].

MASVOSVERE, D.J.E., & VENTER, H.S., 2016. Using a Standard Approach to the Design of Next Generation e-Supply Chain Digital Forensic Readiness Systems. *SAIEE Africa Research Journal*, 107(2), pp.104–120.

PRAYUDI, Y., 2014. Problema dan Solusi Digital Chain of Custody Dalam Proses Investigasi Cybercrime. *Senasti - Seminar Nasional Sains dan Teknologi Informasi*, p.8.

PRAYUDI, Y., LUTHFI, A. & PRATAMA, A.M.R., 2014. Pendekatan Model Ontologi Untuk Merepresentasikan Body of Knowledge Digital Chain of Custody. 2(2), p.8.

PRIBADI, I., 2018. Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana. *Jurnal Lex Renaissance*, [online] 3(1). Available at: <https://journal.uii.ac.id/Lex-Renaissance/article/view/12736/pdf> [Accessed 22 Apr. 2020].

RAMADHAN, R.A., PRAYUDI, Y. & SUGIANTORO, B., 2017. Implementasi dan Analisis Forensika Digital pada Fitur TRIM Solid State Drive. *TEKNOMATIKA*, 9(2), p.13.

RIADI, I. & HADI, A., 2019. Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics. p.9.

RIADI, I., UMAR, R. & NASRULLOH, I.M., 2018. Analisis Forensik Digital pada Frozen Solid State Drive dengan Metode National Institute Of Justice (NIJ). *Elinvo (Electronics, Informatics, and Vocational Education)*, 3(1), pp.70–82.

RIFAUDDIN, M. & HALIDA, A.N., 2018. Waspada Cybercrime dan Informasi Hoax pada Media Sosial Facebook. *Khizanah al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, 6(2), pp.98–111.

ROSALINA, V., SUHENDARSAH, A. & NATSIR, M., 2016. Analisis Data Recovery Menggunakan Software Forensic: Winhex and X-Ways Forensic. *Jurnal Pengembangan Riset dan Observasi Sistem Komputer (PROSISKO)*, 3(1), pp.51–55.

SUN, J.-R., SHIH, M.-L. & HWANG, M.-S., 2015. A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure. *International Journal of Network Security*, 17(4), pp.497–509.