ELINVO(Electronics, Informatics, and Vocational Education), May 2018,3(1), 70-82
ISSN 2580-6424 (printed), ISSN 2477-2399 (online), DOI:10.21831/elinvo.v3i1.19308

ANALISIS FORENSIK DIGITAL PADA *FROZEN SOLID STATE DRIVE* DENGAN METODE *NATIONAL INSTITUTE OF JUSTICE (NIJ)*

Imam Riadi[1], Rusydi Umar[2]& Imam Mahfudl Nasrulloh[3]
[1,2,3]Universitas Ahmad Dahlan Yogyakarta
E-mail: mahfudz.mail@gmail.com

ABSTRACT

Computer crime has evidence of digital crime and needs to be analyzed. The rapid development of computer technology has brought changes in the field of hardware. In hardware today there is a Solid State Drive (SSD) as the primary storage of the computer, because the SSD technology has fast data access speed. The use of drive freezing software on computers is often done by computer technicians, as it can save on maintenance costs. This software is used to protect the computer from unwanted changes, computer systems that use frozen drive software are not stored on storage media after the computer is shut down. When this happens, what digital forensic investigators must do. This study discusses the comparison of related forensic tools used for the examination and analysis process. The collection of digital evidence is carried out by static forensic methods, while the research and analysis stage adjusts and implements forensic methods from the National Institute of Justice (NIJ) to obtain digital evidence. Drive freezing software such as Shadow Defender has been shown to influence the practice of digital forensic examination on the acquisition of digital evidence, with a successful file restoration percentage of only 28.7% so that it can become an obstacle in the digital forensic process.

***Keywords**: Forensic, Digital, Evidence, SSD, NIJ*

ABSTRAK

Kejahatan komputer memiliki bukti *digital* dari tindak kejahatan dan perlu dilakukan analisa. Perkembangan teknologi komputer yang demikian pesat telah membawa perubahan pada bidang perangkat keras. Pada perangkat keras saat ini terdapat *Solid State Drive (SSD)* sebagai media penyimpanan utama komputer, karena teknologi *SSD* memiliki kecepatan akses data yang cepat. Penggunaan *software* pembeku *drive* pada komputer sering dilakukan oleh teknisi komputer, karena dapat menghemat biaya perawatan. *Software* tersebut digunakan untuk melindungi komputer dari perubahan yang tidak dikehendaki, sistem komputer yang tanam software tersebut menjadikan perubahan yang terjadi pada sistem komputer tidak disimpan pada media penyimpanan setelah komputer dimatikan. Ketika hal ini terjadi apa yang harus dilakukan oleh penyidik forensik digital. Penelitian ini membahas perbandingan terkait tool Forensik yang digunakan untuk proses eksaminasi dan analisa. Pengambilan salinan bukti digital dilakukan dengan metode forensik statik, sedangkan tahapan penelitian dan analisa mengadaptasi dan mengimplementasikan metode forensik dari National Institute of Justice (NIJ) untuk mendapatkan bukti digital. Software pembeku drive seperti Shadow Defender terbukti berpengaruh terhadap praktik eksaminasi forensik digital terhadap didapatkannya bukti-bukti *digital*, dengan kondisi tersebut prosentase keberhasilannya merestorasi *file* hanya 28,7% sehingga dapat menjadi hambatan dalam proses forensik digital.

Kata kunci: Forensik, Bukti, Digital, SSD, NIJ

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang demikian pesat telah membawa perubahan pada bidang perangkat lunak *(software)*, perangkat keras *(hardware)*, dan budaya masyarakat *(brainware)*. Aktivitas penggunaan teknologi informasi dan komunikasi yang pada mulanya menuntut peralatan-peralatan pemrosesan data yang sangat besar dan rumit, kini digantikan oleh perangkat otomasi digital dan perangkat jinjing *(portable)*. Aktifitas manusia saat ini sebagian besar berhubungan dengan data, informasi, dan komunikasi, serta dalam kegiatannya secara langsung maupun tidak langsung akan berhubungan dengan perangkat teknologi komputer. Penggunaan teknologi komputer sehari-hari pada dasarnya memiliki manfaat

yang sangat besar, sebagai dampak penggunaan dari komputer memiliki manfaat positif dan ada dampak negatif. Manfaat secara positif dari teknologi komputer yang ditimbulkan sangat bermanfaat, sehingga dapat membantu proses dari pekerjaan yang sulit menjadi mudah dan membantu aktivitas manusia menjadi lebih mudah, cepat, serta efisien. Adapun dampak teknologi komputer secara negatif yaitu adanya penyalahgunaan terhadap teknologi komputer itu sendiri yang digunakan untuk tindak kejahatan, sehingga dapat menimbulkan kerugian perseorangan, golongan, instansi, lembaga, atau bahkan negara.

Kejahatan komputer atau disebut *computer crime* merupakan kejahatan yang melibatkan teknologi komputer yang ada didalamnya [(1)]. Kejahatan komputer memiliki bukti elektronik dan *digital* dari tindak kejahatan berupa jejak aktivitas kejahatannya dan perlu dilakukan analisa terhadap bukti *digital* yang didapatkan dengan ilmu dan metode forensik. Pada bidang teknologi, analisa forensik terhadap barang bukti *digital* atau elektronik disebut dengan sebutan komputer forensik atau *digital forensic* [(2)]. *Digital forensic* itu sendiri merupakan tindakan memperoleh, mengambil, melestarikan, dan menyajikan data sesuai dengan metode dan *tool* forensik.

Pada suatu kasus kejahatan teknologi komputer yang terjadi pada umumnya akan meninggalkan jejak aktivitas kejahatan. Jejak aktivitas *(history)* yang terkait dengan tindak kejahatan tersebut dapat dijadikan sebagai barang bukti. Barang bukti kejahatan komputer dapat berupa barang bukti elektronik dan barang bukti *digital*. Barang bukti elektronik dapat berupa bentuk fisik dari perangkat elektronik tersebut atau dapat berupa media simpan *(storage device)*, sedangkan barang bukti digital dapat berupa *file* dokumen, *file history*, atau *file log* yang berisikan data-data terkait yang dapat dijadikan sebagai informasi pendukung pengambil keputusan. Barang bukti elektronik dan barang bukti *digital* menjadi hal terpenting dalam suatu kasus kejahatan komputer, karena aktivitas tindak kejahatan komputer yang dilakukan terekam oleh sistem komputer pada media penyimpanan utama *(primary storage)* perangkat komputer. Bukti digital dapat diketahui dan dilihat pada saat kejahatan dilakukan melalui metode *live forensics* atau setelah terjadi tindak kejahatan dengan metode *static forensics*. Analisa bukti *digital* perlu dilakukan sesuai dengan prosedur penanganan khusus, metode analisa forensik yang tepat, dan dengan mengkomparasikan berbagai *tool* forensik untuk mendapatkan bukti *digital* yang baik serta terjaga integritas datanya, sehingga dari bukti digital tersebut diperoleh barang bukti berupa informasi yang valid untuk mendukung putusan hukum suatu perkara tindak kejahatan komputer.

Media penyimpanan komputer pada dasarnya terdiri dari dua jenis media penyimpanan yaitu *non-volatile memory (NVM)* dan *volatile memory*. *Non-volatile memory* memungkinkan data yang tersimpan tidak akan hilang meskipun aliran listrik terputus atau tidak tergantung dengan catu daya listrik [(3)], seperti *Harddisk, Solid State Drive (SSD), Flashdisk, Memory Card, Zip Drive, Optical Drive,* dan *Nand Flash*, sedangkan media penyimpanan *Violatile Memory* akan kehilangan data ketika aliran listrik terputus atau tidak ada catu daya listrik, seperti pada *Random Access Memory (RAM), Dynamic Random-access Memory (DRAM),* dan *Static Random-access Memory (SRAM). Solid State Drive* atau *Solid State Disk* disingkat *SSD* adalah perangkat penyimpan data yang menggunakan serangkaian *integrated circuit* atau *IC* sebagai memori yang digunakan untuk menyimpan data atau informasi [(4)].

SSD merupakan salah satu media penyimpanan utama selain *Harddisk*. Teknologi *SSD* menggunakan *solid state memory* berbasis *NAND flash* atau *NOR flash* pada penyimpanan datanya. *SSD* menggunakan teknologi yang hampir mirip seperti *RAM (Random Access Memory)*, data dalam *SSD* berbasis flash biasanya disimpan dalam sel memori pada chip, terdapat dua macam jenis

sel memori yang umum digunakan, yaitu jenis *Multi Level Cell (MLC)* dan *Single Level Cell (SLC)*. Secara fisik yang membedakan *SSD dengan harddisk (HDD)* adalah pada *SSD* menggunakan semikonduktor atau *integrated circuit (IC)*, sedangkan pada *harddisk* menggunakan platter magnetis yang berputar. Meskipun secara teknis bukan sebuah *disk* tetapi bentuk atau dimensi *SSD* sama dengan *Harddisk*, sehingga dapat digunakan pada komputer dan notebook (komputer jinjing). *SSD* juga menggunakan *interface* yang sama pada *harddisk* yaitu *Serial Advanced Technology Attachment (SATA)* atau *Integrated Drive Electronics (IDE)*. Saat ini *SSD* berangsur-angsur menggantikan posisi *harddisk* pada media penyimpanan utama komputer, karena teknologi *SSD* ini memiliki kecepatan akses data yang sangat tinggi.

Penelitian mengenai media penyimpanan komputer yang dilakukan Albana & Riadi [(5)] pada suatu kasus kejahatan komputer dengan sistem operasi *proprietary* menjadi permasalahan bagi penyidik untuk menemukan *file* dokumen, *history*, serta perubahan yang dilakukan oleh pelaku kejahatan ketika *drive* pada suatu *harddisk* dibekukan menggunakan aplikasi *software Deep Freeze*, karena jejak pengguna akan terhapus dari memori dan media penyimpanan secara otomatis setelah komputer itu dihidupkan ulang atau *restart*. Hal tersebut senada apa yang dikatakan oleh perusahaan pengembang *software Deep Freeze* pada websitenya deepfreeze.com.au, *software* untuk membekukan *drive* dapat mengurangi biaya pemeliharaan komputer sebesar 63%, sehingga untuk menghemat biaya pemeliharaan perkantoran, instansi, dan warnet di Indonesia mengadopsi perangkat lunak ini [(6)]. Tidak dipungkiri pengelola komputer dan internet publik seperti warung internet (warnet) dan *internet cafe* menggunakan aplikasi-aplikasi sejenis untuk menekan biaya perawatan dan pemeliharaan. Hal ini bisa menjadikan salah satu faktor mengapa kejahatan komputer di Indonesia pada umumnya pelaku kejahatan komputer *(computer crime)* dan kejahatan dunia maya *(cybercrime)* lebih cenderung mengakses komputer dan *internet* ditempat umum seperti warnet dan internet cafe.

Penggunaan *software utility* untuk membekukan sistem dan *drive* pada komputer juga sering dimanfaatkan oleh teknisi atau pranata komputer yang digunakan untuk melindungi komputer dari perubahan yang tidak dikehendaki. Beberapa *software* pembeku *drive* yang sering digunakan diantaranya *DeepFreeze, Shadow Defender, Windows Steady State, dan Toolwiz Time Freeze.* Pada *software* tersebut memiliki fitur *system restore* dan pembeku *drive* pada Harddisk, SSD, dan media simpan utama lainnya. Ketika pengaturan pada software tersebut diaktifkan maka perubahan yang terjadi pada sistem komputer tidak akan disimpan pada media penyimpanan. Sistem kerja *software* tersebut pada saat komputer dimatikan dan dihidupkan kembali maka keadaan sistem komputer seperti semula sebelum dilakukan perubahan, begitu juga jika melakukan proses penyimpanan *file* pada *drive* yang dibekukan, maka ketika komputer dimatikan dan dihidupkan kembali *drive* akan kembali seperti sebelum dilakukan penyimpanan file. Hal ini menjadikan tantangan investigator forensik komputer *(digital forensics)* dan bagaimana melakukan analisa bukti-bukti *digital* pada kondisi tersebut diatas jika terjadi pada media penyimpanan *Solid State Disk (SSD)* yang dibekukan *(frozen)*?

Kondisi drive SSD yang dibekukan atau *frozen solid state drive (SSD)* yang dimaksudkan disini adalah *SSD* tersebut dilakukan pembekuan *drive*, dimana sistem komputer tersebut terinstal *software utility* yang digunakan untuk melindungi komputer dari perubahan yang tidak dikehendaki. *Software utility* pembeku *drive* yang digunakan pada penelitian awal ini adalah *Shadow Defender*. Dikatakan pada website pengembang *software* Shadow Defender [(7)] aplikasi tersebut akan mengambil snapshot dari disk dan menjalankan setiap file dalam mode virtual, setelah pengguna keluar dari dimensi

paralel setiap perubahan pada sistem dan file pada disk akan dihapus. Kesimpulan dari penggunaan *software* tersebut adalah komputer tidak akan terpengaruh oleh perubahan apapun dan tidak ada file berbahaya yang akan ditulis ke komputer. Pada keadaan dan sistem komputer pada kondisi seperti inilah menjadi tantangan bagi investigator forensik *digital* sehingga perlu dilakukan analisis forensik bukti digital pada *frozen solid state drive (SSD)*.

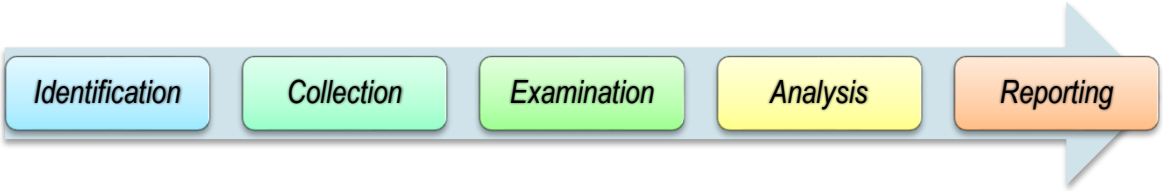
Pengumpulan bukti digital pada media penyimpan komputer atau *non-volatile memory (NVM)* atau *non-volatile evidence collection* melibatkan pengumpulan bukti dari media simpan komputer seperti *MMC Card, Compact Flash, Flash Disk, SD Card, Flash Memory, Harddisk, Solid State Disk,* dan yang sejenis [(1)]. Penelitian lainnya terhadap media simpan yang pernah dilakukan, yaitu penelitian terhadap *Harddisk* dan *SSD* dengan perlakuan yang sama, *file* yang sama, dilakukan penghapusan *file* dan format dengan interval yang sama kemudian dianalisis menggunakan *tool* FTK Toolkit, diperoleh hasil bahwa setelah dilakukan tindakan yang sama pada kedua *drive* tersebut hasil yang diperoleh tidak sama sehingga menimbulkan permasalahan bagi penyidik [(8)]. Hasil penelitian serupa pada forensik digital *SSD* menunjukkan hasil perolehan data pada *SSD* tidak dapat diprediksi dan bervariasi [(4)]. Hasil perolehan data pada *SSD* ada pengaruh dari fitur TRIM, TRIM terbukti berpengaruh terhadap praktek examinasi dan analisis forensika digital pada *SSD* [(9)]. *SSD* dalam posisi fitur TRIM dalam keadaan non-aktif (disable) sebagian besar data yang terhapus data di-recovery kembali seperti halnya melakukan recovery data pada Harddisk konvensional. Namun, berbeda dengan SSD dalam posisi fitur TRIM dalam keadaan aktif (enable), sebagian besar data yang terhapus tidak dapat di-recovery kembali. TRIM merupakan sebuah perintah yang langsung ditujukan kepada kepada firmware dari SSD.

Selain itu *tool* forensik yang sesuai diperlukan untuk mengumpulkan bukti dan memastikan diterimanya bukti digital dan integritas dari keaslian bukti digital yang didapatkan dan juga perlu dipastikan melalui mekanisme seperti *hashing* atau menerapkan *write protection* untuk menjaga integritas data dan mencegah adanya perubahan data atau file yang mengakibatkan tidak diterimanya sebagai bukti *digital*. Perbedaan penggunaan *tool* forensik juga akan mempengaruhi bukti *digital* yang didapat. Pada penelitian Rosalina et al [(10)] melakukan analisa forensik menggunakan *tool* forensik yaitu *X-Ways Forensics* dan *WinHex* dari kedua *tool* tersebut dapat digunakan untuk mekanisme pengembalian data atau *file* secara otomatis maupun pengembalian secara manual, dan dapat digunakan pada media penyimpanan termasuk SSD. Selain obyek forensik dan *tool* forensik adalah metode analisa forensik, menurut Argawal [(1)] pemilihan model, metode, atau sistematika investigasi digital forensik diantaranya harus memenuhi individualitas *(individuality)*, keterulangan *(repeatability)*, kehandalan *(reliability)*, kinerja *(performance)*, kemampuan uji *(testability)*, skalabilitas *(scalability)*, dan standar kualitas *(quality standards)*. Pada analisa forensik dapat mengacu dan menggunakan metode dari *National Institute of Justice (NIJ)* dengan alur *identification, collection, examination, analysis,* dan *reporting* [(11)], atau dapat menggunakan metode dari *National Institute of Standards and Technology (NIST)* dengan rangkaian forensik *collection, examination, analysis,* dan *reporting* [(12)].

METODE

Pada penelitian ini mengadaptasi dan mengimplementasikan metode analisa forensik dari *National Institute of Justice (NIJ)*. Metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada. Menurut Anggara [(11)] disebutkan melakukan teknik forensik dan analisa

forensik berdasarkan metode yang benar akan memiliki keberhasilan hampir 100% dalam mengumpulkan data forensik. Tahapan pada penelitian ini dapat digambarkan seperti pada Gambar 1.



Gambar 1. Metode *National Institute of Justice (NIJ)*

Tahapan metode dari *National Institute of Justice (NIJ)* ini terbagi menjadi lima tahapan yakni *identification, collection, examination, analysis,* dan *reporting* [(11)], secara lengkap dipaparkan sebagai berikut:

Tahap *identification* atau tahap identifikasi merupakan kegiatan pemilahan barang bukti tindak kejahatan digital dan pemilahan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan *digital*. Pada tahap ini didalamnya terdapat proses identifikasi, pelabelan, perekaman, untuk menjaga keutuhan barang bukti.

Tahap *collection* atau tahap pengumpulan merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan *digital*. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari perubahan.

Tahap *examination* atau tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara forensik baik secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa *file* tersebut asli sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, untuk itu pada *file* digital perlu dilakukan identifikasi dan validasi *file* dengan teknik *hashing*.

Tahap *analysis* atau tahap meneliti ini dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dan komprehensif dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut. Hasil analisis terhadap data digital selanjutnya disebut digunakan sebagai barang bukti digital serta dapat dipertanggungjawabkan secara ilmiah dan secara hukum.

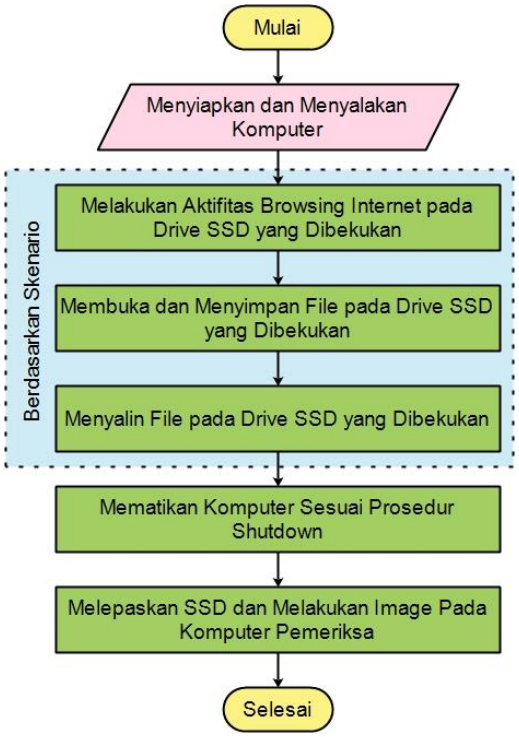
Tahap *reporting* atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai *tool*, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, *tool*, atau aspek pendukung lainnya pada proses tindakan *digital* forensik. Adapun tahapan penelitian yang dilalui pada penelitian ini mengacu pada 5 (lima) tahap dari *National Institute of Justice (NIJ)* dan langkah dari penelitian ini dibagi menjadi 3 (tiga) tahapan utama seperti pada Gambar 2.

Gambar 2. Tahapan Penelitian

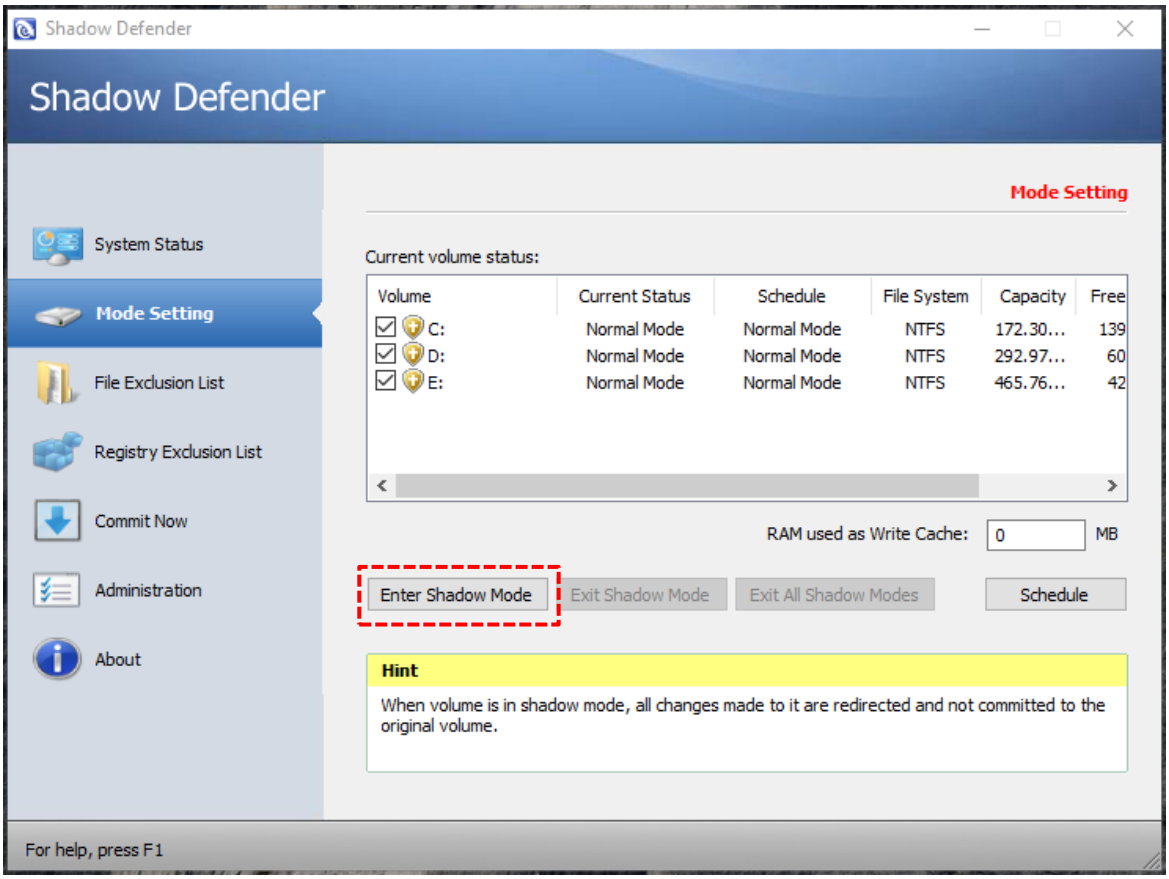
Pada penelitian ini bukti digital yang digunakan tidak didapatkan pada lingkungan yang sebenarnya atau barang bukti tidak didapatkan dari hasil tindak kejahatan komputer yang sebenarnya, melainkan bukti

digital dibuat dan peroleh dari hasil skenario pada tahap implementasi dan pengujian yang akan dibahas pada bagian sub-bab tersendiri. Tahap implementasi dan pengujian forensik bukti *digital* pada *SSD* yang dibekukan *(frozen solid state drive)* ditunjukkan pada alur Gambar 3.

Implementasi dan pengujian dilakukan dengan desain skenario, dengan tujuan untuk mendapatkan bukti digital seperti pada kasus kejahatan komputer yang sebenarnya. Alur pada tahapan sesuai Gambar 3 merupakan implementasi dan pengujian forensik bukti *digital* pada *frozen solid state drive* (SSD). Pada tahap ini dilakukan praktek fungsi *frozen* (pembekuan) pada *drive* SSD, yaitu mengaktifkan fitur *frozen* pada *software* Shadow Defender. Tampilan *software* Shadow Defender seperti pada Gambar 4 untuk mengaktifkan pembekuan *drive (frozen drive)* dengan mengaktifkan Shadow Mode.



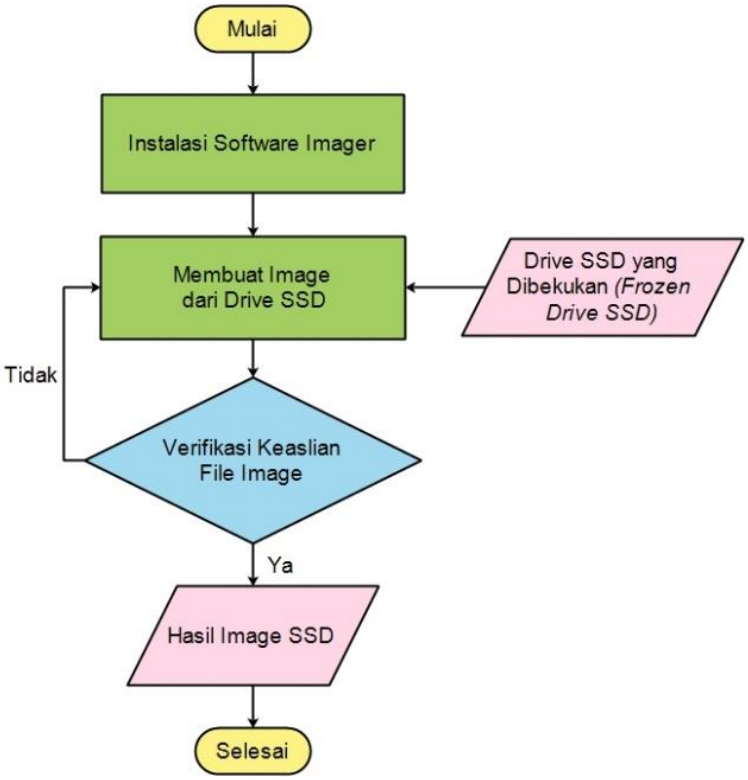
Gambar 3. Tahapan Implementasi dan Pengujian



Gambar 4. Tampilan Shadow Defender

Implementasi yang dilakukan terhadap fungsi *frozen* (pembekuan) pada *drive* SSD yaitu melakukan aktifitas menggunakan komputer secara normal dan seolah-olah digunakan untuk tindak kejahatan dengan membuat dan menyalin berbagai macam *file* dokumen *(.doc, .xls, .ppt, .pdf)*, *file* gambar *(.jpg, .png)*, *file* aplikasi *(.exe)*, *file* multimedia *(.mp3, .mp4)*, dan melakukan aktifitas browsing internet. Setelah dimelakukan sekenario penggunaan komputer seolah-olah digunakan kejahatan tahap berikutnya adalah melakukan akuisisi atau membuat salinan terhadap *drive SSD* yang dibekukan dengan membuat *image drive* menggunakan *software* OSForensics untuk menganalisis *file-file* apa saja yang dapat dikembalikan atau direstorasi setelah komputer dimatikan dalam kondisi *drive* dibekukan *(frozen drive)* pada SSD. *Tools* yang digunakan dalam praktek analisis adalah OSForensics, Autopsy dan WinHex guna kebutuhan analisis serta FTK Imager guna membuat *image* dari SSD.

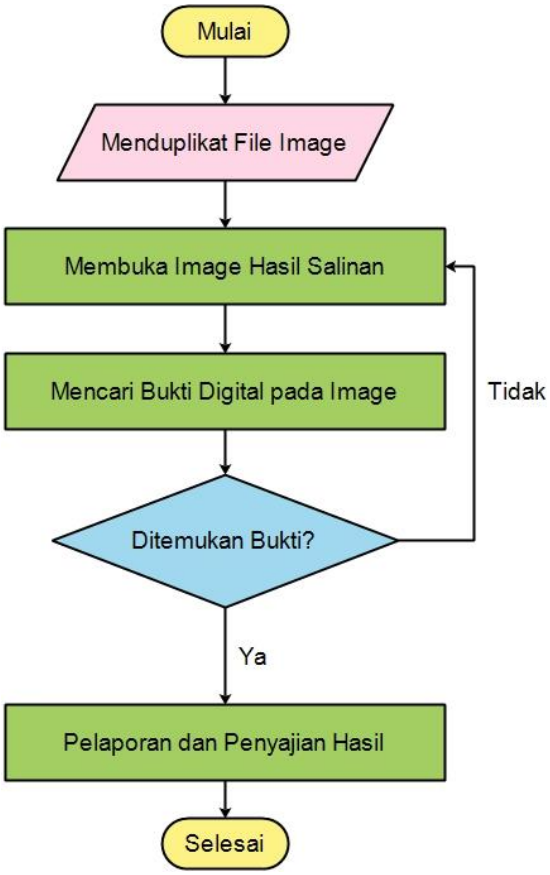
Pengambilan bukti digital mengacu pada metode *static forensic* atau disebut juga metode akuisisi secara tradisional, hal ini berfokus pada memeriksa salinan duplikat [(14)]. Pengambilan salinan bukti *digital* harus tetap dipastikan konsisten dengan aslinya, sehingga hasil yang didapat pada kondisi baik [(15)]. Pada umumnya ketika menjalankan *tool* forensik baik dalam analisis metode *static* atau *live* untuk memperoleh data, proses tersebut dapat menimpa struktur data dari data sebelumnya yang dapat menyebabkan inkonsistensi data. Tahapan pengambilan salinan pada penelitian ini menerapkan metode statis yaitu pengambilan bukti digital dilakukan pada komputer dalam keadaan mati *(off)*, alur pengambilan salinan bukti digital seperti pada Gambar 5.



Gambar 5. Tahapan Pengambilan Salinan

Tahapan diatas dilalui agar bukti salinan berupa *image drive* memiliki kesamaan dengan *drive* aslinya, dan memiliki struktur data dan file yang sama. Pada tahapan analisa forensik bukti *digital* pada *SSD* yang dibekukan *(frozen solid state drive)* secara garis besar mengimplementasikan metode forensik dari *National Institute of Justice*

(NIJ). Hasil salinan atau *image* dilakukan duplikasi dan dianalisa menggunakan *tool software* OSForensics, Autopsy, dan Winhex untuk menemukan bukti digital. Bukti digital yang diharapkan ditemukan adalah *file* dokumen *(.doc, .xls, .ppt, .pdf)*, *file* gambar *(.jpg, .png)*, *file* aplikasi *(.exe)*, *file* multimedia *(.mp3, .mp4) history* internet, dan catatan terbaru penggunaan komputer. Tahapan analisis forensik digambarkan pada Gambar 6.

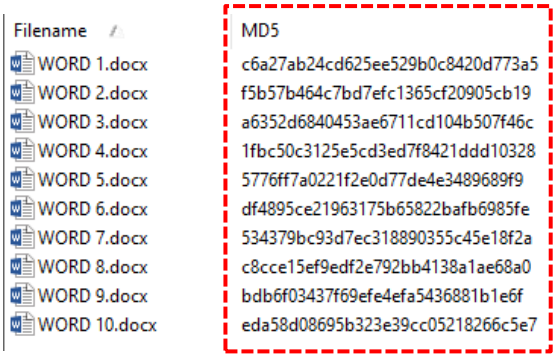


Gambar 6. Tahapan Analisa Forensik

Melalui tahapan analisa forensik yang dilalui diperoleh bukti-bukti *digital* file-file yang terkait dengan kejahatan tersebut, kemudian disajikan dalam bentuk laporan hasil. Sehingga laporan dari analisa tersebut dapat mendukung informasi berupa siapa, kapan, dan dimana kejahatan komputer tersebut dilakukan, yang kemudian dilanjutkan dengan proses hukum sesuai dengan prosedur yang ada.

HASIL DAN PEMBAHASAN

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 sealiknya, 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 seperti pada Gambar 7.



Filename	MD5
WORD 1.docx	c6a27ab24cd625ee529b0c8420d773a5
WORD 2.docx	f5b57b464c7bd7efc1365cf20905cb19
WORD 3.docx	a6352d6840453ae6711cd104b507f46c
WORD 4.docx	1fbc50c3125e5cd3ed7f8421ddd10328
WORD 5.docx	5776ff7a0221f2e0d77de4e3489689f9
WORD 6.docx	df4895ce21963175b65822bafb6985fe
WORD 7.docx	534379bc93d7ec318890355c45e18f2a
WORD 8.docx	c8cce15ef9edf2e792bb4138a1ae68a0
WORD 9.docx	bdb6f03437f69efe4efa5436881b1e6f
WORD 10.docx	eda58d08695b323e39cc05218266c5e7

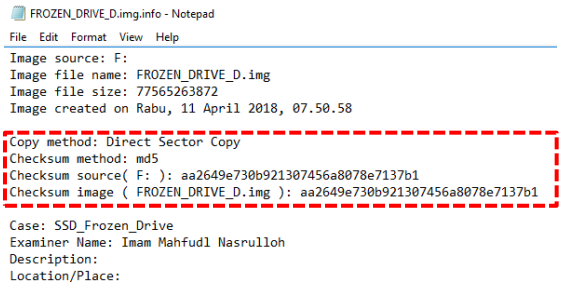
Gambar 7. Nilai Hashing pada *File*

Kemudian mematikan komputer seolah-olah komputer tersebut telah dipakai, dan langkah selanjutnya melakukan pembuatan salinan pada komputer pemeriksa.

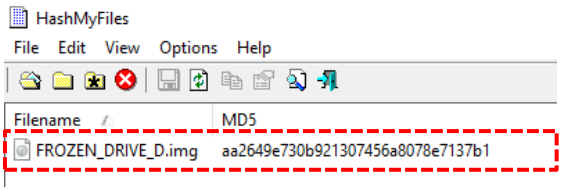
Hasil dari tahap implementasi dan pengujian yang dilakukan sesuai desain skenario selanjutnya dilakukan akuisisi atau membuat salinan *drive solid state drive (SSD)*, yaitu dengan membuat *image* menggunakan *tool* forensik FTK Imager atau OSForensic. Hal ini dimaksudkan barang bukti yang diperoleh yaitu *solid state drive (SSD)* tidak

rusak dan tidak berubah baik struktur direktori, struktur file, dan struktur datanya ketika dilakukan proses eksaminasi dan analisa forensik, karena jika data atau file tersebut berubah maka dianggap ada perubahan barang bukti. Barang bukti tersebut setelah dibuat salinan akan disimpan dan dibuka kembali pada saat dipengadilan jika diperlukan.

Hasil *imaging* dari *drive* SSD Samsung 850 Evo 120GB menunjukan 2 partisi, partisi pertama memiliki ukuran 77565263872 *bytes* dan partisi kedua memiliki ukuran 41941991424 *bytes*. Setelah dibuat file salinan berupa *image drive* untuk memastikan hasil salinan dan integritas salinan barang bukti digital maka dilakukan *hashing* dan mengkomparasikan dengan nilai *hash (checksum)* yang dimiliki oleh file aslinya seperti pada Gambar 8 dan Gambar 9 memiliki kesamaan nilai *hash (checksum)*.



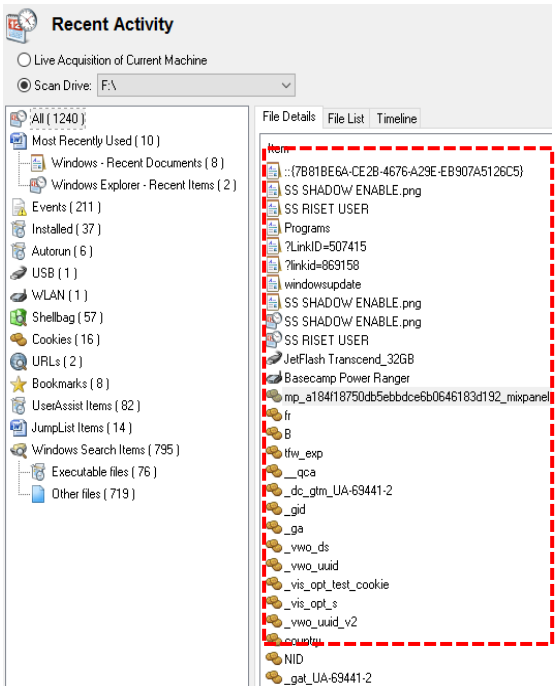
Gambar 8. Nilai Hash Hasil *Image*



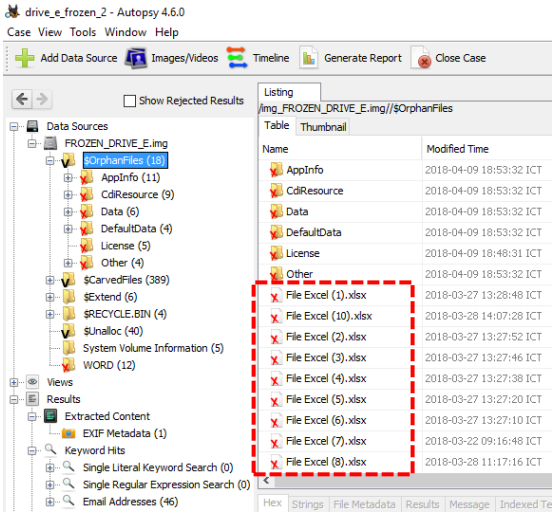
Gambar 9. Nilai Hash Salinan *Image*

Setelah melakukan pengecekan keotentikan kedua file baik *image* asli dan *image* salinan maka tahapan selanjutnya adalah melakukan examinasi dan analisis data pada hasil salinan *drive*.untuk mendapatkan bukti-bukti atau bukti *digital* terkait dengan kejahatan digital. Pada bagian ini menjelaskan hasil dari penelitian terhadap analisa forensik bukti *digital* pada *frozen solid state drive (SSD)*. Setelah pengimplementasian fitur *frozen* pada SSD dan membuat salinan *drive* dari aslinya selanjutnya dilakukan analisa forensik. Pada tahap ini *tool* yang digunakan untuk menganalisa yaitu *OSForensics*, Autopsy dan WinHex. Secara prinsip dari ketiga tool tersebut sama digunakan untuk membuka struktur direktori dan struktur data yang ada pada image salinan.

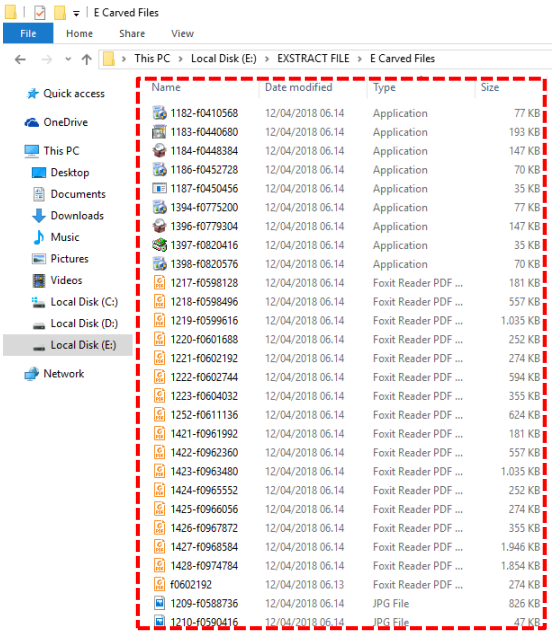
Hasil eksaminasi pada *drive* SSD yang dibekukan *(frozen drive)*, *file* yang telah terhapus oleh *software* Shadow Defender secara otomatis ketika komputer dimatikan dan *file* yang dihapus secara manual oleh pengguna hasil eksaminasi dan analisa dengan OSForensics versi 3.3 menunjukan struktur direktori dapat dilihat, namun hanya dapat dilihat catatan terakhir komputer saat digunakan *(recent activity)*, sedangkan file-file dan data yang terkait pada tahap skenario dan implementasi pengujian tidak ada, sehingga terkait dengan file yang dibuat pada tahap awal tidak dapat dapat direstorasi, tampilan hasil analisa dengan menggunakan OSForensics seperti yang ditunjukkan pada kotak bergaris Gambar 10 dibawah ini.



Gambar 10. Eksaminasi pada OSForensics



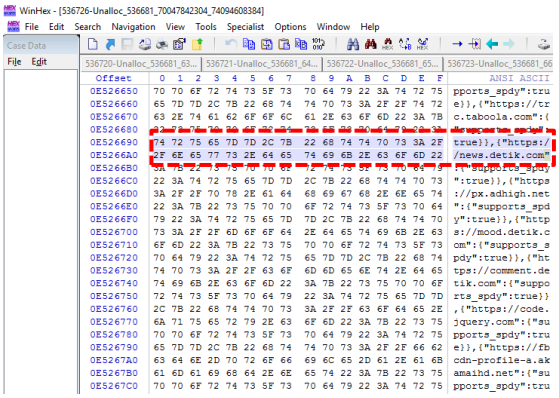
Gambar 11. Eksaminasi pada Autopsy



Gambar 12. Hasil Ekstraksi dari Autopsy

Guna membandingkan hasil yang didapat saat analisa maka dilakukan eksaminasi dan pengamatan dengan *tool* forensik yang kedua, yaitu dengan Autopsy versi 4.6.0. Pada *file* yang telah terhapus oleh software Shadow Defender secara otomatis ketika komputer dimatikan dan *file* yang dihapus secara manual oleh pengguna hasil eksaminasi dan pengamatan dengan Autopsy mendapatkan hasil dan *file* dapat diketemukan, namun file tidak berada pada direktori aslinya melainkan ada pada direktori $OrphanFiles, $CarvedFiles, dan $Unalloc, serta hasil eksaminasi sebagian dapat direstorasi dan dikem'balikan meskipun nama *file* tidak sama dengan aslinya kondisi file dapat dibuka dengan baik tidak ada kerusakan pada struktur data. Informasi yang menunjukkan catatan terakhir pengguna *(recent activity)* dapat ditampilkan. Hasil eksaminasi dari Autopsy ditunjukkan pada kotak bergaris Gambar 11 dan hasil ekstraksi seperti pada Gambar 12.

Dari kedua *tool* forensik, OSForensics dan Autopsy belum dapat menampilkan sejarah internet *(history internet)* maka dilakukan took ketiga untuk eksaminasi dan analisa menggunakan WinHex versi 19.6. Hasil yang didapat menggunakan WinHex, catatan sejarah internet *(history internet)* dapat diketemukan, ditunjukan pada Gambar 13.



Gambar 13. Eksaminasi pada WinHex

Pada hasil analisa menggunakan WinHex sejarah internet *(history)* dapat dilihat. Alamat website yang terlihat diduga masih dalam catatn baru *(recent activity)*. Data tersebut tercatat pada direktori $Unalloc dengan ekstensi file tidak dikenali namun dengan *tool* WinHex dapat dibaca dan ditampilkan dalam data Hexadesimal atau sistem bilangan basis 16. Website yang tercatat pada file tersebut diantaranya: https://youtube.com, https://kompas. com, https://news.detik.com, hal ini menunjukan bahwa dengan *tool* WinHex dapat mengambil informasi sejarah internet *(history internet)*.

Dari hasil eksaminasi dan analisis ketiga *tool* forensik yang digunakan pada *frozen solid state drive* (SSD), *file* yang telah terhapus oleh *software* Shadow Defender secara otomatis ketika komputer dimatikan dan *file* yang

dihapus secara manual oleh pengguna sebagian dapat restorasi kembali. Berikut secara rinci ekstensi *file* yang dapat direstorasi seperti pada Tabel 1.

Tabel 1. Daftar File yang Dapat Direstorasi Pada Kondisi Drive Dibekukan

Jenis File	Tool Software		
	OSForensics	Autopsy	Winhex
File Dokumen			
.doc	Tidak	Ya	Tidak
.xls	Tidak	Ya	Tidak
.ppt	Tidak	Sebagian	Tidak
.pdf	Tidak	Sebagian	Tidak
File Gambar			
.jpg	Tidak	Sebagian	Sebagian
.png	Tidak	Sebagian	Sebagian
File Multimedia			
.mp3	Tidak	Sebagian	Tidak
.mp4	Tidak	Sebagian	Tidak
File Aplikasi			
.exe	Tidak	Sebagian	Tidak
File Log			
History Internet	Tidak	Tidak	Sebagian
Catatan terakhir	Ya	Ya	Tidak

Dari hasil eksaminasi dan analisa forensik didapatkan informasi berupa *file* dan informasi pendukung lainnya. *File* yang didapat dapat direstorasi, namun untuk melihat keaslian dari *file* tersebut maka dilakukan teknik *hashing*, diasumsikan bahwa jika dari kedua file, baik file asli dan file hasil restorasi memiliki nilai hash yang sama dapat dikatakan *file* tersebut identik dan sama. Pada Tabel 2 secara detail dapat dijelaskan.

Tabel 2. Hasil Verifikasi dan Validasi Keaslian File dengan Hashing

Nama File Asli	Nilai Hashing MD5 File Asli	Nama File Hasil Restorasi	Nilai Hashing MD5 File Restorasi
WORD 1.docx	c6a27ab24cd625ee529b0c8420d773a5	1443-f1130576.docx	c6a27ab24cd625ee529b0c8420d773a5
WORD 2.docx	f5b57b464c7bd7efc1365cf20905cb19	1447-f1133456.docx	f5b57b464c7bd7efc1365cf20905cb19
WORD 3.docx	a6352d6840453ae6711cd104b507f46c	1449-f1133480.docx	a6352d6840453ae6711cd104b507f46c
WORD 4.docx	1fbc50c3125e5cd3ed7f8421ddd10328	1451-f1133504.docx	1fbc50c3125e5cd3ed7f8421ddd10328
WORD 5.docx	5776ff7a0221f2e0d77de4e3489689f9	1453-f1133704.docx	5776ff7a0221f2e0d77de4e3489689f9
WORD 6.docx	df4895ce21963175b65822bafb6985fe	1455-f1133792.docx	df4895ce21963175b65822bafb6985fe
WORD 7.docx	534379bc93d7ec318890355c45e18f2a	1190-f0493896.docx	534379bc93d7ec318890355c45e18f2a
WORD 8.docx	c8cce15ef9edf2e792bb4138a1ae68a0	1457-f1133824.docx	c8cce15ef9edf2e792bb4138a1ae68a0
WORD 9.docx	bdb6f03437f69efe4efa5436881b1e6f	1459-f1133856.docx	bdb6f03437f69efe4efa5436881b1e6f
WORD 10.docx	eda58d08695b323e39cc05218266c5e7	1445-f1130600.docx	eda58d08695b323e39cc05218266c5e7
File Excel (10).xlsx	71c6f8181fcb01ea752fc8ffcb11a5b6	1201-f0575840.xlsx	71c6f8181fcb01ea752fc8ffcb11a5b6
File Excel (6).xlsx	31514f08b4ccf357fc0c1c855060a03f	1202-f0581472.xlsx	31514f08b4ccf357fc0c1c855060a03f
KEAMANAN JARINGAN.ppt	ceb6417758b290b1b894573164072fd8	1258-f0620072.pptx	ceb6417758b290b1b894573164072fd8
File PDF (1).pdf	4d1518c91c53da625ae800cfdd06ff90	1421-f0961992.pdf	4d1518c91c53da625ae800cfdd06ff90
File PDF (3).pdf	603469708cd301eeea39fe67c31e3497	1220-f0601688.pdf	603469708cd301eeea39fe67c31e3497
File PDF (4).pdf	255d57ee06444c64c43962f6b9103b64	1221-f0602192.pdf	255d57ee06444c64c43962f6b9103b64
File PDF (5).pdf	144422c1d272faa42c141d9b46617c78	1222-f0602744.pdf	144422c1d272faa42c141d9b46617c78
File PDF (6).pdf	9c4fc8c6a25fd9c301ec07ff62ace8e0	1223-f0604032.pdf	9c4fc8c6a25fd9c301ec07ff62ace8e0
File PDF (7).pdf	eaec6c18efcef9bc57abee93159475de	1427-f0968584.pdf	eaec6c18efcef9bc57abee93159475de
File PDF (9).pdf	6b81c90596254a134bad89e9ebe30adb	1252-f0611136.pdf	6b81c90596254a134bad89e9ebe30adb
File PDF (10).pdf	b4791406338db847ae817c5e1bf3e58e	1218-f0598496.pdf	b4791406338db847ae817c5e1bf3e58e
01GAC Suara.mp3	82ed964902bfb852677397d338bb551e	1188-f0468488.mp3	82ed964902bfb852677397d338bb551e
01Sheila On 7.mp3	d74be8fe1a62e0a76f7d8ede2b109228	1194-f0501856.mp3	d74be8fe1a62e0a76f7d8ede2b109228
01Virgoun Bukti.mp3	3db73258697a62f5b53b66086018f014	1195-f0508952.mp3	3db73258697a62f5b53b66086018f014
Vigroun.mp4	93b42b0d7a8dccc435ba75118e8393e7	1441-f1102808.mp4	93b42b0d7a8dccc435ba75118e8393e7

Berdasarkan informasi yang didapatkan baik dari pengamatan, eksperimen dan beberapa literatur ujukan yang diimplementasikan pada penelitian ini, membuktikan bahwa mekanisme *frozen solid state drive (SSD)* atau pembekuan terhadap *drive* pada *SSD* dapat menghambat penyelidikan forensik digital. Ketika diaktifkan efek dari mekanisme *software* pembeku *drive* memiliki pengaruh pada sitem operasi yang sedang berjalan dan pada *drive* penyimpanan.

SIMPULAN

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 bukti-bukti *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.

REFERENSI

[1] Agarwal, Ankit, Gupta, Megha and Gupta, Saurabh. *Systematic Digital Forensic Investigation Model.* 2011, International Journal of Computer Science and Security (IJCSS), 5(1), 118-131.

[2] Ridho, Faizin, Yudhana, Anton and Riadi, Imam. *Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time.* 2016. Prosiding Annual Research Seminar 2016. 2(1), 111-116. ISBN: 979-587-626-0.

[3] Silberschatz, Abraham, Galvin, Peter Baer and Gagne, Greg. *Operating Systeme Concepts: Ninth Edition.* United States of America: 2013.

[4] Geier, Florian. *The Differences Between SSD And HDD Technology Regarding Forensic Investigations. Computer Science.* Degree of Computer Science. Linnaeus University. Swedia. 2015.

[5] *Forensic Analysis of Frozen Hard Drive Using Static Forensics Method.* Albanna, Faiz and Riadi, Imam. 2017, International Journal of Computer Science and Information Security (IJCSIS), 15(1), 173-178.

[6] Deepfreeze. How Deep Freeze Works (Online). [Cited: November 23, 2017.] http://deepfreeze.com.au/.

[7] Shadowdefender. What is Shadow Defender ? (Online).[Cited:November 25, 2017] http://www.shadowdefender.com/.

[8] Marupudi, Shiva Sai Ram. *Solid State Drive: New Challenge for Forensic Investigation.* 2017 : Culminating Projects in Information Assurance. 30.

[9] Ramadhan, Rizdqi Akbar, Prayudi, Yudi and Sugiantoro, Bambang.*Implementasi Dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive.* 2017, TEKNOMATIKA, 9(2), 1-13.

[10] Rosalina, Vidila, Suhendarsah, Andri and Natsir, M. *Analisis Data Recovery Menggunakan Software Forensic: Winhex And X-Ways Forensic.* 2016, PROSISKO, 3(1), 51-55.

[11] Faiz, Muhammad Nur, Umar, Rusydi and Yudhana, Anton.*Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email.* 2017, JISKA, 1(3), 108-114.

[12] Riadi, Imam, Umar, Rusydi and Firdonsyah, Arizona. *Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method*. 2017, International Journal of Computer Science and Information Security (IJCSIS), 15(5), 155-160.

[13] Anggara Putra, Roni, Fadlil, Abdul and Riadi, Imam.*Forensik Mobile Pada Smartwatch Berbasis Android*. 2017, JURTI, 1(1), 41-47.

[14] Riadi, Imam, Umar, Rusydi and Sukarno, Wasito.*Analisis Forensik Serangan SQL Injection Menggunakan Metode Statis Forensik.* Program Pascasarjana Universitas Muhammadiyah Yogyakarta (PPs UMY). Prosiding Interdisciplinary Postgraduate Student Conference 1st. 102-103.

[15] Rafique, Mamoona and Khan, M.N.A.*Exploring Static and Live Digital Forensics: Methods, Practices and Tools.* 2013, International Journal of Scientific & Engineering Research, 4(10), 1048-1056.