Jurnal Ilmu Teknik dan Komputer
Vol. 4 No. 2 Juli 2020
ISSN 2548-740X
E-ISSN 2621-1491

ANALISIS FORENSIK KOMPUTER PADA *HARD FORMAT SOLID STATE DRIVE* MENGGUNAKAN METODE *DIGITAL FORENSICS RESEARCH WORKSHOP*

Ardiansyah[*], Marza Ihsan Marzuki[**]

[*]Teknik Elektro, Fakultas Pascasarjana, Universitas Mercu Buana
Jl. Raya Meruya Selatan No. 1, Kembangan, Jakarta Barat 11650
odon.sukses@gmail.com

[**]Teknik Elektro, Fakultas Pascasarjana, Universitas Mercu Buana
Jl. Raya Meruya Selatan No. 1, Kembangan, Jakarta Barat 11650
marza.ihsan@mercubuana.ac.id

ABSTRACT

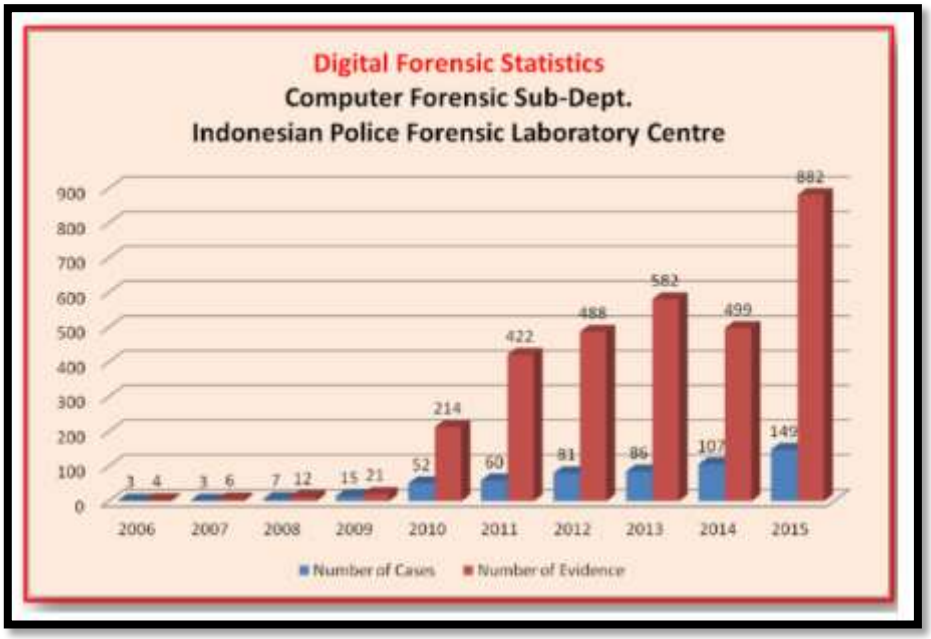
Kasus cybercrime di Indonesia tiap tahunnya mengalami peningkatan 15% atau rata – rata mengalami peningkatan 56 kasus pertahun, menurut Digital Laboratorium Forensik Mabes Polri. Investigasi digital forensics memiliki cara yang berbeda untuk mendapatkan bukti digital seperti komputer forensics, mobile forensics, network forensics dan database forensics. Investigasi komputer forensics pada media penyimpanan solid state drive yang di hard format untuk mendapatkan bukti digital berkaitan dengan file recovery, yaitu suatu metode untuk mengambil logical file atau memunculkan kembali file yang sudah terhapus maupun hilang karena tidak tecatat lagi di file system NTFS (New Technology File System) pada operation system Windows. Penelitian ini menggunakan metode digital forensics research workshop untuk mendapatkan bukti digital. Aktifnya fitur trim pada solid state drive terbukti berpengaruh terhadap praktik examination dan recovery pada proses investigasi komputer forensics. Dengan kondisi fitur trim aktif yang berhasil di-recovery hanya 5 file dari 17 file yang disiapkan untuk pengujian, dengan persentase 29%. Sedangkan fitur trim nonaktif hanya 15 file dari 17 file dengan persentase 88% yang berhasil di-recovery.

Kata Kunci : cybercrime, solid state drive, digital forensics research workshop, forensik komputer, hard format

PENDAHULUAN

LATAR BELAKANG

Di Indonesia, menurut Laboratorium Forensik Mabes Polri pada tahun 2006 hingga 2015, seperti yang terihat pada gambar 1. Kejahatan *cybercrime* tiap tahunnya mengalami peningkatan yang signifikan pada tahun 2015 terdapat 149 kasus *cycbercrime* dengan jumlah barang bukti sebanyak 882 unit. Statistik ini menunjukkan bahwa kejahatan komputer adalah masalah serius di era *digital*. Penanganan bukti *digital* mencakup setiap dan semua *data digital* yang dapat menjadi bukti penetapan bahwa kejahatan telah dilakukan atau dapat memberikan *link* antara kejahatan dan korbannya atau kejahatan dan pelakunya.



Gambar 1. Statistik Kejahatan Komputer di Indonesia (Albana, 2017).

Analisa bukti *digital* dilakukan sesuai dengan prosedur penanganan khusus, metode *analysis forensics* yang tepat, dan dengan mengkomparasikan berbagai *tools forensics* 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. Proses investigasi *digital forensics* dilakukan untuk mendapatkan bukti *digital* yang *valid.* (Alharbi, 2011).

RUMUSAN MASALAH

Dari latar belakang diatas dapat ditarik permasalahan untuk dijadikan perumusan masalah antara lain :

1) Bagaimana bukti *digital* pada media penyimpanan *solid state drive* yang di *hard format* ?
2) Bagaimana mekanisme *digital forensics research workshop* untuk mendapatkan bukti *digital* dari *solid state drive* yang di *hard format* ?

TUJUAN PENELITIAN

Berdasarkan rumusan yang dibuat maka dapat diambil tujuan dari penelitian ini adalah :

1) Menggali informasi yang bisa digunakan sebagai bukti *digital* pada media penyimpanan *solid state drive* mengunakan *digital forensics research workshop*.
2) Mensimulasikan proses investigasi yang efektif yang dapat dipergunakan dalam peroses investigasi komputer *forensics* pada media penyimpanan *solid state drive* yang di *hard format* untuk keperluan *forensics.*

BATASAN PENELITIAN

Untuk lebih fokus dan terarahnya penelitian yang dilakukan dan berdasarkan rumusan masalah yang telah dipaparkan sebelumnya maka diberikan batasan dalam penelitian ini sebagai berikut :

1) Fokus penelitian ini pada laptop yang menggunakan media penyimpanan *solid state drive* dengan *operation system* Windows 10 Home 64 bit.

2) Kegiatan penelitian ini dilakukan menggunakan metode *digital forensics research workshop* dan *tools forensics* seperti Autopsy, OSForensics, dan RecoverMyFiles untuk melakukam analisis pada media penyimpanan *solid state drive* yang di *hard format*.

STUDI LITERATUR

DIGITAL FORENSICS

Digital forensics dapat didefinisikan sebagai proses pengumpulan, memeriksa, menganalisis, dan melaporkan bukti *digital* tanpa kerusakan. (Dogan, 2017). *Digital forensics* adalah cabang ilmu *forensics* yang bersangkutan dengan penggunaan informasi *digital* yang dihasilkan, disimpan dan ditransmisikan oleh komputer sebagai sumber bukti dalam investigasi dan proses hukum. (Rahaditya, 2016).

KOMPUTER *FORENSICS*

Komputer *forensics* adalah ilmu yang menjelaskan keadaan saat ini di artefak digital yang berkaitan dengan bukti legal yang ditemui pada komputer dan media penyimpanan digital. (Promila, 2015). Pemeriksaan terhadap jenis barang bukti ini biasanya berkaitan dengan *files recovery*, yaitu suatu metode untuk mengambil *file logical* atau memunculkan kembali *file* yang sudah dihapus maupun hilang karena tidak tecatat lagi di *file system*. Komputer *forensics* dapat menangani berbagai informasi, mulai dari *log* (seperti *history internet*) melalui *file* yang sebenarnya berada pada media penyimpanan seperti *harddisk* atau *solid state drive.*

SOLID STATE DRIVE

Solid state drive adalah media penyimpanan data yang menggunakan *nonvolatile memory* sebagai media, dan tidak menggunakan disk magnetis seperti media penyimpanan eksternal konvensional. *Solid State Drive* adalah perangkat penyimpan data yang menggunakan serangkaian IC sebagai memori yang digunakan untuk menyimpan data atau informasi. *Solid state drive* memiliki fitur yang bernama trim, trim merupakan sebuah perintah yang langsung ditujukan kepada *firmware* dari *solid state drive*. Perintah *trim* sebenarnya adalah perintah SATA (*Serial Advanced Technology Attachment*) yang dibuat oleh *host operation system* yang kemudian diakui oleh solid state drive controller. (Rizdqi, 2017)

PENELITIAN TERDAHULU

Penelitian mengenai media penyimpanan komputer *solid state drive* juga dilakukan oleh (Riadi, 2018). hasil dari penelitiannya adalah bahwa *frozen solid state drive* terbukti berpengaruh terhadap praktik eksaminasi dan analisa *forensics* terhadap didapatkannya bukti - bukti *digital*. Jika dilakukan perhitungan tingkat presentase keberhasilan untuk *recovery file* dengan mengunakan beberapa *tools forensics* untuk RecoverMyFile yang berhasil di-*recovery* sebanyak 76,38%, Autopsy sebanyak sebanyak 75,27%, FTK sebanyak 0%, Encase sebanyak 0%, dan OSForensics sebanyak 0% dari 360 *file* yang disiapkan untuk implementasi dan pengujian. Terbukti bahwa mekanisme *solid state drive frozen* dapat menjadi hambatan dalam proses *digital forensics* oleh penyidik dan hasil dari penyidikan masih sangat sedikit informasi yang didapatkan dari barang bukti *digital*.

Penelitian mengenai invetigasi *mobile forensics* menggunakan model investigasi *digital forensics research workshop* terkait penanganan kasus perjudian togel di Indonesia dengan SMS yang dilakukan (Rahaditya, 2016). Dalam jurnal tersebut dijelaskan dalam membuat aplikasi untuk membantu pencarian pesan teks sebagai bukti dalam kejahatan yang menggunakan SMS sebagai media komunikasi. Dengan

menggunakan *digital forensics research workshop* sebagai pedoman *tools* SMS *forensics* telah berhasil melakukan penanganan kasus pidana yang melibatkan pesan SMS sebagai media komunikasi, dalam hal ini *tools* SMS *forensics* diterapkan untuk penanganan "perjudian Togel SMS". Dengan cara melakukan penyalinan dan penyaringan bukti SMS serta mencocokkan nilai hash awal kemudian memeriksa antara pesan SMS yang ada di *database* dengan pesan SMS yang dicetak dalam dokumen, nilai pesan menggunakan *hash* SHA256 dan menghasilkan *file output* bukti pelaporan SMS dalam bentuk *file* seperti dokumen PDF, dokumen Word, atau Excel.

METHODOLOGI

BAHAN PENELITIAN

Persiapan untuk menunjang implementasi dalam penelitian. Adapun beberapa perangkat keras dan perangkat lunak yang dibutuhkan untuk melakukan uji simulasi dari skenario yang dibuat, serta instalisasi beberapa *tools forensics* yang diperlukan dalam melakukan simulasi. Berikut ini beberapa alat dan bahan yang dipakai dalam melakukan penelitian.

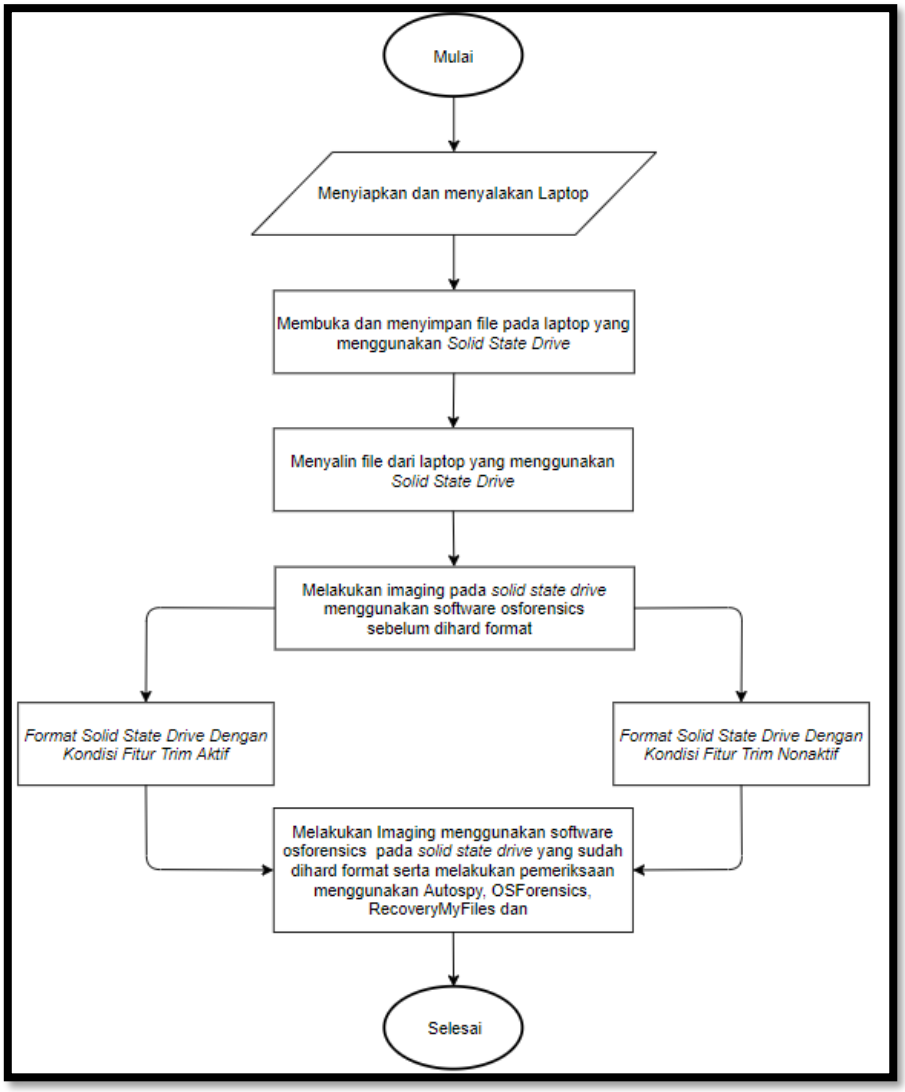
Tabel 1 Persiapan Alat dan Bahan Penelitian

No	*Hardware* Dan *Software (Tools)*	Keterangan
1	1 Unit Laptop	Sebagai komputer untuk melakukan penarikan data dan analisa
2	Autopsy, OSForensics, RecoverMyFiles – Profesional Edition	*Tools forensics* yang digunakan untuk menganalisa dan mendapatkan bukti *digital*
3	.doc, .docx, .xlsx, .pptx, .pdf, .txt, .jpg	Bukti *digital* dokumen dan gambar sebanyak 17 *file*

SKENARIO PENELITIAN

Penelitian ini mengimplementasikan metode *digital forensics research workshop*. 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. 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.

Jurnal Ilmu Teknik dan Komputer
Vol. 4 No. 2 Juli 2020
ISSN 2548-740X
E-ISSN 2621-1491



Gambar 2. Alur Skenario

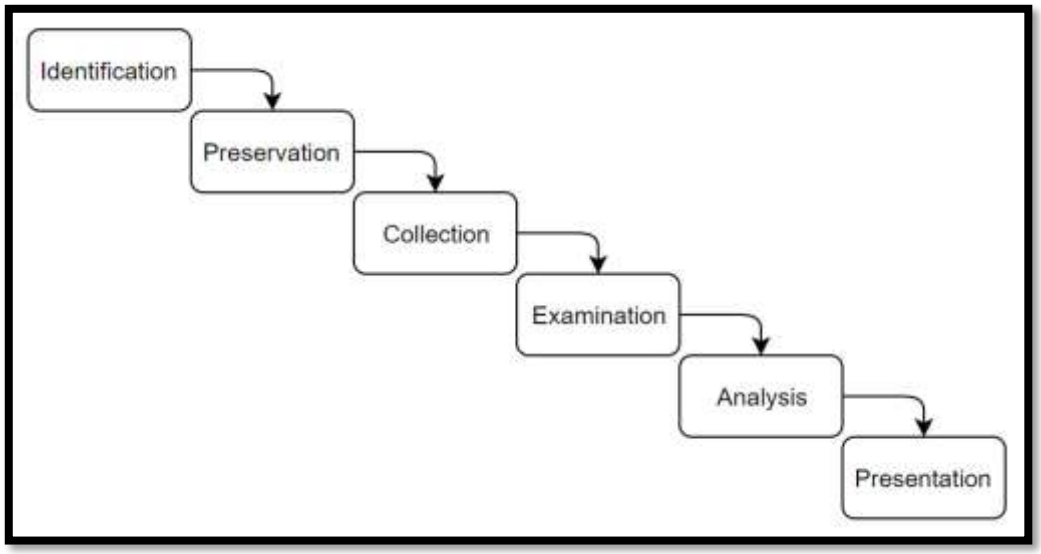
Hard format yang dilakukan pada penelitian ini adalah dengan mem-*format* direktori disk D yang ada pada *solid state drive* sedang direktori disk C tidak dilakukan *format*. Setelah melakukan skenario tahap berikutnya adalah melakukan akuisisi atau membuat salinan terhadap *solid state drive* yang telah di *hard format* dengan membuat *image* menggunakan *software* OSForensics untuk menganalisa *files* apa saja yang dapat di-*recovery* pada *solid state drive*. *Tools* yang digunakan dalam praktek analisis adalah OSForensics, RecoverMyFiles, Autopsy. Alur pada skenario dapat dilihat pada gambar 3. dibagi menjadi 2 kondisi saat melakukan *hard format* dengan kondisi mengaktifkan fitur *trim* dan menonaktifkan fitur *trim* pada laptop.

Gambar 3. Kondisi Mengaktifkan Fitur *Trim*

Gambar 4. Kondisi Menonaktifkan Fitur *Trim*

PROSES INVESTIGASI

Proses investigasi dan pengamanan terhadap barang bukti dilakukan supaya barang bukti yang didapat tidak terkontaminasi dari luar. Barang bukti yang didapat diambil gambarnya dengan kamera foto dan diberi label penamaan, pada saat melakukan investigasi *forensics* dan *analysis forensics* berdasarkan metode yang benar akan memiliki tingkat keberhasilan yang baik dalam mengumpulkan bukti digital. Tahapan investigasi pada penelitian ini menggunakan *digital forensics research workshop* (DFRWS) dapat digambarkan seperti pada gambar 5. (Palmer, 2001).



Gambar 5. Model Investigasi *Digital Forensics Research Workshop* (Palmer, 2001).

1) Tahap *identification* ini untuk melakukan penentuan kebutuhan yang akan diperlukan untuk penyelidikan dan pencarian bukti digital.
2) Tahap *preservation* ini untuk menjaga bukti - bukti dan memastikan keaslian atau integritas barang bukti sehingga bukti benar - benar *valid* / sah. Pada tahap ini didalamnya terdapat proses pelabelan, perekaman, untuk menjaga keutuhan barang bukti.
3) Tahap *collection* ini untuk identifikasi mengumpulkan sumber bukti yang berpotensi menjadi bukti yang kuat. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari perubahan.
4) Tahap *examination* ini untuk menentukan apa saja yang akan dianalisa atau lebih dikenal dengan filterisasi data, sehingga investigator

dapat lebih fokus dalam melakukan tahapan selanjutnya.

5) Tahap *analysis* ini untuk mencari dan mengolah data termasuk data diperoleh dari mana, siapa yang membuat dan bagaimana data tersebut dihasilkan. Hasil analisis terhadap data *digital* selanjutnya disebut digunakan sebagai barang bukti *digital* serta dapat dipertanggung jawabkan secara ilmiah dan secara hukum.
6) Tahap *presentation* untuk tahap ini dimana melaporkan dari hasil proses analisa sehingga dapat dipahami oleh publik.

HASIL DAN DISKUSI

Berdasarkan pada metode yang digunakan *digital forensics research workshop*, maka tahapan yang dilakukan untuk melakukan investigasi komputer *forensics* pada *solid state drive* yang di *hard format* adalah sebagai berikut :

TAHAP *IDENTIFICATION*

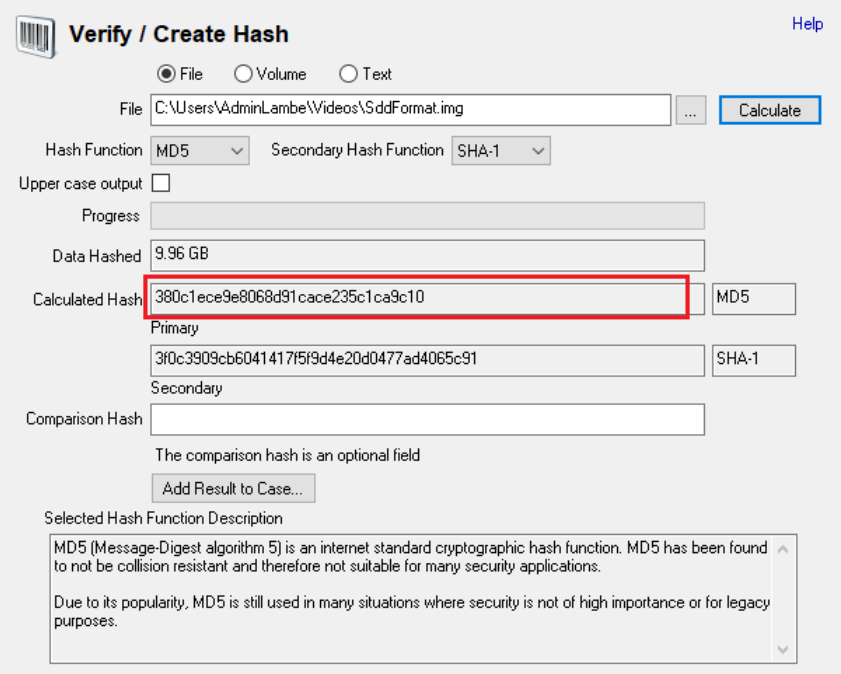
Identifikasi yang dilakukan merupakan tahapan awal untuk melakukan deteksi suatu kejadian atau kejahatan yang tersimpan pada *digital evidence* dengan mempelajari kasus-kasus sebelumnya yang berkaitan dengan pengungkapan kejahatan digital diantaranya penghapusan data dengan melakukan formating SSD.

TAHAP *PRESERVATION*

Tahap yang dilakukan adalah melakukan pengamanan pada barang bukti, dalam simulasi ini yaitu berupa 1 unit laptop asus dengan spesifikasi Processor Intel Core i-3 7th Gen, Memory Ram 4096 MB, VGA Nvidia GeForce MX 130, Samsung Solid State Drive 256 GB. Barang bukti yang didapat diamankan dari kontaminasi data sebelum dilakukan akusisi. Kemudian melakukan pencatatan terhadap barang bukti yang didapat untuk menjaga dan memelihara barang bukti.

TAHAP *COLLECTION*

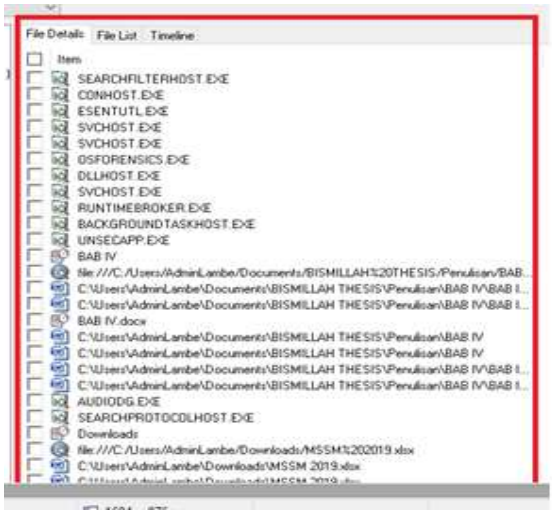
Sesuai dengan skenario, dibuat *file* salinan berupa *image* sebelum di *hard format* dan sesudah di *hard format* untuk memastikan hasil salinan dan integritas salinan barang bukti *digital* maka dilakukan *hashing* dengan mengkomparasikan nilai *hash*. Setelah melakukan pengecekan keotentikan kedua *file* baik *image* salinan asli dan *image solid state drive* yang telah di *hard format*, maka tahapan selanjutnya adalah melakukan *examination* dan *analysis*.



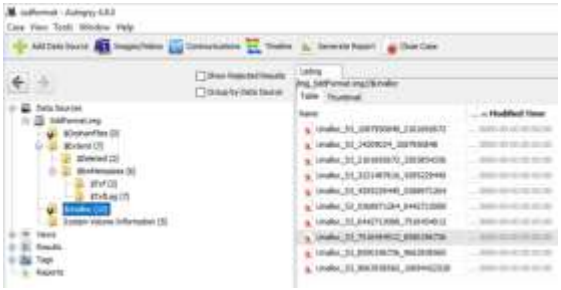
Gambar 9. Hasil Verifikasi Nilai *Hash Image*

TAHAP *EXAMINATION*

Hasil eksaminasi pada *solid state drive* yang di *hard format*, *file* yang telah terhapus karena di *hard format* dengan sengaja oleh pengguna mengunakan *tools* forensics seperti OSForensics, Autopsy dan RecoverMyFiles.

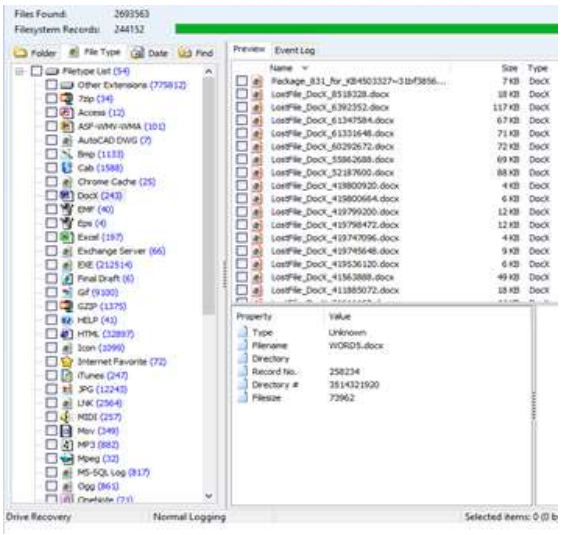


Gambar 10. Hasil Eksaminasi OSForensics



Gambar 11. Hasil Eksaminasi Autospy

Pada *file* yang telah terhapus karena di *hard format* 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 $Extend, $Unalloc, $Deleted, $Txflog, $Txf, dan $RmMetadata. Sedangkan menggunakan RecoverMyFiles kita menemukan *files* yang telah di *hard format*. Diantaranya dari extension *.docx terdapat 243 *file*, extension *.xlsx terdapat 324 *file*, extension *.jpg terdapat 12243 *file*, extension *.pdf terdapat 3230 *file*, extension *.txt terdapat 1132896 *file* dan untuk extension *.ppt terdapat 60 *file*.



Gambar 12. Hasil Eksaminasi RecoverMyFiles

Setelah melihat hasil eksaminasi dari 3 penggunaan *tools forensics, software* RecoverMyFiles merupakan hasil yang paling banyak dari proses *recovery*. Dengan banyak hasil yang didapat dari eksaminasi maka dari itu kita perlu memilih mana yang bisa dijadikan sebagai barang bukti *digital*, maka kita masuk ketahap selanjutnya yaitu *analysis.*

TAHAP *ANALYSIS*

Proses analisis melakukan pencarian informasi penting dari hasil eksaminasi data yang didapat dari *solid state drive* yang di *hard format* menggunakan *tools forensics* dapat dijadikan sebagai refrensi untuk analisa. Menggunakan OSForensics dapat dilihat aktivitas *user* pada penggunaan laptop, bahwa pada tanggal 8 Agustus 2019 merupakan aktivitas paling intens dibandingkan tanggal yang lain dibulan Agustus 2019 dapat dilihat pada gambar 13.

Dengan menggunakan fitur *delete file search* pada OSForensics kita dapat mengetahui bahwa telah terjadi *delete file* pada tanggal tersebut dan *user* yang digunakan untuk melakukan *delete file* pada laptop yang dijadikan barang bukti. Terjadi pada tanggal 8 Agustus 2019 menggunakan user AdminLambe.

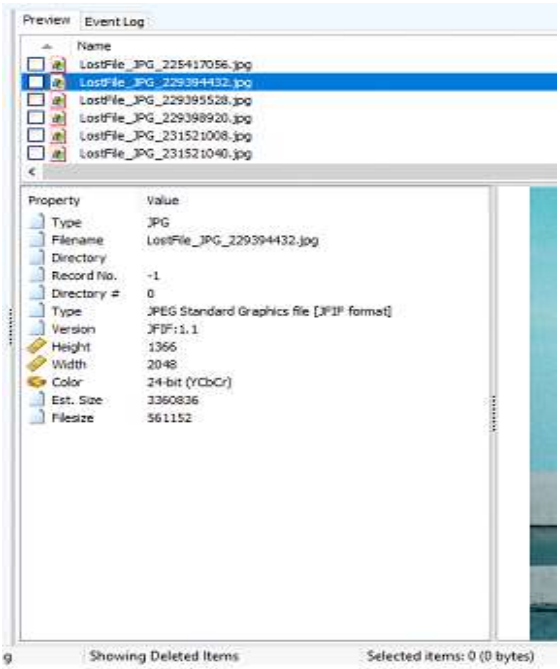
Gambar 13. Aktivitas *User* Pada Laptop

Gambar 14. *Hasil* Scaning Delete File Search

Gambar 15. Bukti *User* Yang Digunakan

Sesuai dengan skenario yang telah dibuat, saat melakukan *hard format* pada *solid state drive* kita mengkondisikan dengan mengaktifkan dan menonaktifkan fitur *trim* pada *solid state drive*. Hasil *recovery* dengan menggunakan RecoverMyFiles untuk *solid state drive* dengan kondisi mengaktifkan fitur *trim* dari *files* yang telah di *hard format* 5 *file* yang berhasil di-*recovery* dari 17 *file* yang dijadikan bahan simulasi. Meskipun *file* yang berhasil di-*recovery* dari kondisi fitur *trim* aktif namanya sudah tidak sesuai dengan *file* yang asli, *file* masih dalam keadaan baik

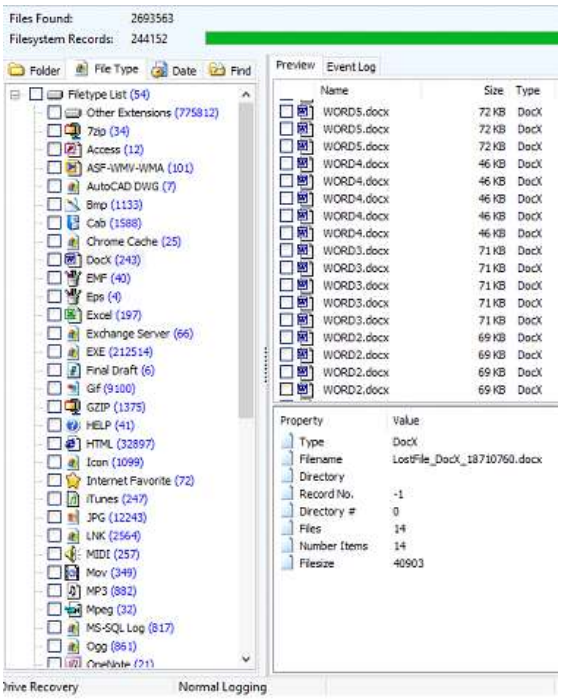
dan dapat dibuka kembali dapat dilihat pada gambar 16. Dengan melihat *size file* yang berhasil di-*recovery* memiliki nilai yang serupa dengan *size file* asli.



Gambar 16. Hasil *Recovery* Kondisi Fitur *Trim* Aktif

Sedangkan skenario dengan kondisi menonaktifkan fitur *trim* hasil dari *recovery* dengan menggunakan RecoverMyFiles lebih banyak yang berhasil di-*recovery* yaitu 15 *file* yang berhasil di-*recovery* dari 17 *file* Dapat dilihat pada gambar 17.

Dari temuan yang didapat saat proses *analysis* hasil *recovery* menggunakan *software* RecoveryMyFiles, *solid state drive* yang di *hard format* dengan 2 kondisi berbeda saat fitur *trim* aktif dan fitur *trim* nonaktif, memiliki hasil yang berbeda sehingga pada tahap *presentation* perlu dilakukan verifikasi dengan *file* aslinya berdasarkan nilai *hash* dan *size file*.



Gambar 17. Hasil *Recovery* Kondisi Fitur Trim Nonaktif

TAHAP *PRSENTATION*

Untuk melihat keaslian dari *file* tersebut maka dilakukan teknik *hashing* menggunakan OSfornesics guna membandingkan *file* yang berhasil di-*recovery* dengan *file* asli nya. Dari *file* yang berhasil di-*recovery* pada *solid state drive* yang di *hard format* dengan kondisi fitur *trim* aktif dan nonaktif memliki jumlah yang berbeda. Perbandingan *files* yang berhasil di-recovery dengan kondisi fitur *trim* aktif dan nonaktif sebagai berikut :

Tabel 2. Rincian Hasil *Recovery File* dengan kondisi fitur *trim* aktif dan nonaktif

Nama File	Hasil Recovery Fitur Trim Aktif	Hasil Recovery Fitur Trim Nonaktif
EXCEL1.XLSX	**Tidak**	**Ya**
EXCEL2.XLSX	**Tidak**	**Ya**
EXCEL3.XLSX	**Tidak**	**Ya**
JPG1.JPG	**Ya**	**Ya**
JPG2.JPG	**Ya**	**Ya**

JPG3.JPG	**Ya**	**Ya**
PDF1.PDF	**Tidak**	**Ya**
PDF2.PDF	**Ya**	**Ya**
PPT1.PPTX	**Tidak**	**Tidak**
PPT2.PPTX	**Tidak**	**Tidak**
TEXT1.TXT	**Tidak**	**Ya**
TEXT2.TXT	**Tidak**	**Ya**
WORD1.DOC	**Ya**	**Ya**
WORD2.DOCX	**Tidak**	**Ya**
WORD3.DOCX	**Tidak**	**Ya**
WORD4.DOCX	**Tidak**	**Ya**
WORD5.DOCX	**Tidak**	**Ya**

Sesuai dengan yang diasumsikan bahwa telah terjadi penghilangan atau perubahan *file* pada *solid state drive*. Dengan menggunakan teknik *hashing* kita mencocokan *file* asli dengan *file* hasil *recovery* untuk melihat keaslian dari *file* tersebut. Jika terdapat kesamaan atau identik nilai hash dari *file* asli dengan *file* hasil *recovery* dapat dikatakan bahwa *file* hasil *recovery* adalah *file* yang hilang dari *solid state drive* dengan cara di *hard format*.

Table 3. Hasil Verifikasi dan Validasi Keaslian *File* dengan *Hashing*

File Asli	*Recovery* Fitur *Trim* Aktif	*Recovery* Fitur Nonaktif
EXCEL1.XLSX 45b8a2562a8e8c442214ed25a29f20bbf		**EXCEL1.XLSX 45b8a2562a8e8c442214ed25a29f20bbf**
EXCEL2.XLSX 7252ac58b256325fe9c9b4c5258ecb55		**EXCEL2.XLSX 7252ac58b256325fe9c9b4c5258ecb55**
EXCEL3.XLSX 07771229b712f57974bc503daa8a3b0f		**EXCEL3.XLSX 07771229b712f57974bc503daa8a3b0f**
PDF1.PDF b14e9ea22c6f0b2797ca73f2e17ebcdd		**PDF1.PDF b14e9ea22c6f0b2797ca73f2e17ebcdd**
PDF2.PDF 5767885985c9a14cb51f6233aa968b19c	**LostFile_PDF_7569728.pdf 5767885985c9a14cb51f6233aa968b19c**	**PDF2.PDF 5767885985c9a14cb51f6233aa968b19c**
PPT1.PPTX 008a606a03e5e112da026d900a389761		
PPT2.PPTX e213e30f09ee82ee2e8909cbb974293a		
TEXT1.TXT 5306d858b71e76ae50b1617ffb4fd5cb		**TEXT1.TXT 5306d858b71e76ae50b1617ffb4fd5cb**
TEXT2.TXT a39b531ea2cc9576717ba003c5cbe82b		**TEXT2.TXT a39b531ea2cc9576717ba003c5cbe82b**

WORD1.DOC 9999100ce66f91255625f913e4b5119b	**LostFile_Word_2334432.doc 9999100ce66f91255625f913e4b5119b**	**WORD1.DOC 9999100ce66f91255625f913e4b5119b**
WORD2.DOCX ef6d1ede51add3c0380c4f8bc1884a2		**WORD2.DOCX 059024edf73c6a3fbe2d04938551885e**
WORD3.DOCX 63e9283a835bfe0ddbf8ea05a9790a36		**WORD3.DOCX 11b40a60d3a035f774a0e6bbbf13b286**
WORD4.DOCX be2be5509468f8f0dc57c7e5ab0869a9		**WORD4.DOCX be2be5509468f8f0dc57c7e5ab0869a9**
WORD5.DOCX 8270cf54ecccf8e89184b16d313a6637		**WORD5.DOCX d0b0e72d3955725f2cdf5e0aa9e4d779**

Lanjutan Table 4

File Asli	*Recovery* Fitur *Trim* Aktif	*Recovery* Fitur Nonaktif
JPG1.JPG 32bc68e49b2e8a22786db89a82066ff0	**LostFile_JPG_229394432.jpg 32bc68e49b2e8a22786db89a82066ff0**	**JPG1.JPG 32bc68e49b2e8a22786db89a82066ff0**
JPG2.JPG fd245d64ab8c4ecec49b733a14125bc7	**LostFile_JPG_229395528.jpg fd245d64ab8c4ecec49b733a14125bc7**	**JPG2.JPG fd245d64ab8c4ecec49b733a14125bc7**
JPG3.JPG 9a2baad48a060d8f7dc87f880f0a427f	**JPG3.JPG 9a2baad48a060d8f7dc87f880f0a427f**	**JPG3.JPG 9a2baad48a060d8f7dc87f880f0a427f**

Tercatat hasil verifikasi dan validasi dengan teknik *hashing file* asli dan *file* yang berhasil di-*recovery* dengan kondisi *solid state drive* fitur *trim* aktif dan fitur *trim* nonaktif. Terdapat perbedaan pada nama *file* dengan *file* yang asli akan tetapi memiliki nilai *hash* yang sama dengan *file* asli. Sedangkan dari beberapa *file* yang berhasil di-*recovery* dengan kondisi fitur *trim* nonaktif. Memiliki kesamaan pada nama *file* dengan *file* yang asli akan tetapi untuk *extension* *.docx terdapat beberapa *file* memiliki nilai *hash* yang berbeda dengan *file* asli, dikarenakan *file* nya telah rusak dan tidak dapat dibuka kembali. Jadi hasil dari *recovery solid state drive* yang di *hard format* dengan kondisi fitur *trim* aktif dan nonaktif dapat dijadikan sebagai bukti *digital.*

DISKUSI

Penelitian mengenai *solid state drive* yang dilakukan Abdulaziz, (2017). Pada suatu kasus kejahatan komputer pada *operation system open source* dengan menghapus *file* secara permanen pada *solid state drive*

dengan fitur *trim* aktif. Memiliki dampak penting untuk mencari dan menemukan barang bukti *digital*, karena hanya sebagian data yang dapat di-*recovery* kembali sebesar 56.7% yaitu 33.7 GB dari data awal sebesar 60.1 GB yang telah dihapus secara permanen. Sedangkan pada penelitian ini mengenai *solid state drive* yang di *hard format* pada *operation system* window 10 Home 64 bit. Hasil *recovery* dengan fitur *trim* aktif sebesar 29% dari 17 *file* hanya 5 *file* yang berhasil di-*recovery* dan beberapa *file* yang lainnya sudah tidak ada pada *solid state drive*. Disebabkan saat mengaktifkan fitur *trim* pada *solid state drive*, *host operation system* yang kemudian diakui oleh *solid state drive controller* yang sudah tersedia dari *firmware solid state drive*. Oleh karena itu ketika *file* dihapus dalam suatu *operation system*, perintah *trim* dikirim ke *disk controller* dengan LBA (*Logical Block Addresses*) untuk pengahapusan *file solid state drive* kemudian me-*reset blok - blok* yang menjadi ruang kosong tambahan. (Rizdqi, 2017). Dan untuk hasil recovery dengan kondisi fitur *trim* nonaktif sebesar 88% dari 17 f*ile* hanya 2 *file* yang tidak berhasil di-*recovery*.

Dapat kita lihat hasil *recovery solid state drive* pada *operation system* Windows 10 Home 64 bit dengan kondisi fitur *trim* aktif dan fitur *trim* nonaktif. Pada kondisi fitur *trim* aktif hasil dari *recovery* sangat sedikit dibandingkan dengan fitur *trim* nonaktif. Jika kita bandingkan dengan penelitian yang telah dibuat oleh (Abdulaziz, 2017) mengenai suatu kasus kejahatan komputer pada *operation system open source* dengan menghapus *file* secara permanen pada *solid state drive* dengan fitur *trim* aktif. Meskipun sama menggunakan media penyimpanan *solid state drive* dengan kondisi fitur *trim* aktif, penelitian tersebut dapat berhasil melakukan *recovery* sebesar 33.7 GB dari data awal sebesar 60.1 GB lebih dari setengahnya yang dapat berhasil di-*recovery*. Dikarenakan *file system* Ext4 yang ada pada *operation system open source* memiliki *batched discard* yang menciptakan skenario di mana fitur *trim* aktif pada *solid state drive* tidak segera menyadari telah terjadi penghapusan *file* sehingga tidak langsung dilakukan ekstarsi *file* melainkan menampungnya terlebih dahulu. Hal ini menunjukkan bahwa f*ile system NTFS (New Technology File System)* yang ada pada *operation system* Windows melakukan penghapusan *file* lebih agresif dibandingkan *file system* Ext4. Alastair, (2013). Maka dari itu pada penelitian ini dengan menggunakan *operation system* Windows yang berhasil di-*recovery* dengan kondisi fitur *trim* aktif pada *solid state drive* tidak mencapai setengahnya.

Berdasarkan informasi yang dikumpulkan dari literatur yang ada dan simulasi yang diimplementasikan pada penelitian ini, membuktikan bahwa meskipun menggunakan *operation system* yang berbeda fitur *trim* pada *solid state drive* memiliki pengaruh ketika diaktifkan. Karena tidak semua data yang telah dihilangkan tidak dapat di-*recovery* seluruhnya dan fitur *trim* aktif pada *solid state drive* menjadi tantangan untuk *digital forensics* dalam pencarian bukti *digital*.

KESIMPULAN

Berdasarkan hasil yang didapat pada proses implementasi, hasil dan pembahasan, maka pada penelitian studi dan analisis *digital forensics* pada *solid state drive* yang di *hard format* dengan investigasi menggunakan metode *digital forensics research workshop* dapat ditarik kesimpulan dan saran sebagai berikut :

1) Bukti *digital* yang diperoleh menggunakan RercoverMyFiles dari hasil *recovery solid state drive* yang di *hard format* dengan kondisi fitur *trim* aktif yang berhasil di-*recovery* hanya 5

file dari 17 *file* yang disiapkan untuk pengujian, dengan persentase 29%. Sedangkan fitur *trim* nonaktif hanya 15 *file* dari 17 *file* dengan persentase 88% yang berhasil di-*recovery*. Maka potensi kejahatan dengan memanfaatkan *solid state drive* dengan fitur *trim* yang aktif, sangat mungkin terjadi dan sulit untuk mendapatkan bukti *digital* terkait pemanfaatan fitur *trim* yang secara *default* dengan kondisi aktif.

2) Mekanisme untuk mendapatkan bukti *digital* pada laptop yang menggunakan media penyimpanan *solid state drive* yang di *hard format* dimana perangkat yang dijadikan barang bukti dalam keadaan mati. Sesuai dengan metode *digital forensics research workshop* dapat membantu proses investigasi *komputer forensics*.

DAFTAR PUSTAKA

Abdulaziz, A., Mohammad G. A., & Mohammad Y. U. (2017). Solid State Drive Data Recovery in Open Source Environment. *International Conference on Anti-Cyber Crimes (ICACC).*

Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A New Approach of Digital Forensics Model for Digital Forensics Investigation. *International Journal of Advance Computer Science and Applications (IJACSA)*, Vol. 2 No. 12, 175-178.

Agrawal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security(IJCSS)*, Vol. 5 No. 1, 118-131.

Alastair, N., Scott, L., & Matthew, R. (2013) A Forensic Analysis and Comparison of Solid State Drive Data Retention With Trim Enabled File Systems. *Proceedings of the 11th Australian Digital Forensics Conference*. Diadakan di Edith Cowan, Australia. Tanggal 2 - 4 Desember 2013.

Alharbi, S., Jahnke, J. W., & Traore, I. (2011). The Proactive and Reactive Digital Forensics Investigation Process : A Systematic Literature Review. *International Journal of Security and Its Applications (IJCSIA)*, Vol. 5 No. 4, 59-72.

Andri, L. S., Reza, A., & Nur, W. (2016). Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS). *Jurnal Edukasi dan Peneletian Informatika (JEPIN)*, Vol. 2, No. 2.

Ashar, N., Narasimha, S., & Umit, K. (2018). Forensic Analysis of Wear Levelling on Solid-State Media. *IEEE International Conference on Trust, Security and Privacy in Computing and Communications.*

Dezfoli, F., Dehghantanha**, A.,** Mahmoud**,** R., Fazlida, N., & Daryabar, F. (2014). Digital Forensic Trends and Future. *International journal of Cyber Security nad Digital Forensic (IJCSDF)* 2(2): 48-76.

Dogan, S., & Akbal, E. (2017). Analysis of Mobile Phones in Digital Forensics. *International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).*

Faiz, A., & Imam, R. (2017). Forensic Analysis of Frozen Hard Drive Using Static Forensics Method. *International Journal of Computer Science and Information Security (IJCSIS),* Vol. 15, No. 1.

Goel, A., Tyagi, A., & Agrawal, A. (2012). Smartphone Forensic Investigation Process Model. *International Journal of Computer Science & Security (IJCSS)*, Vol. 6 No. 5, 322-341.

Gulshan, S. (2016) Network Forensics: Methodical Literature Review. *3rd International Conference on Computing for Sustainable Global Development (INDIACom).*

Imam, R., Rusydi, U., & Imam, M. N. (2018). Analisis Forensik Digital Pada *Frozen Solid State Drive* dengan metode *National Institute Of Justice (NIJ). Electronic, Informatics and Vocational Education (ELINVO)*, Vol. 3 No.1.

Imam, R., Rusydi, U., & Imam, M. N. (2018). Experimental Investigation of Frozen Solid State Drive on Digital Evidance with Static Forensic Methods, *Lontar Komputer*, Vol. 9 No.3.

Joshua, S., & Bing Z. (2017). Forensic Database Reconstruction. *IEEE International Conference on Big Data (BIGDATA).*

Kalbande, D. & Jain, N. (2013). Comparative Digital Forensic Model. *International Journal of Innovative Research in Science, Engineering and Technology(IJIRSET)*, Vol. 2 No. 8.

Muhammad, N. F. (2018). Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal, *Journal of Informatics, Information System, Software Engineering and Applications*, Vol. 1, No. 1, PP.63-70.

Palmer. (2001). A Road Map for Digital Forensic Research. *Technical Report DTR-T0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).*

Promila, B., & Divakar, S. Y. (2015). Computer Forensics – Digitized Science. *SAI Intelligent Systems Conference 2015.*

Rahaditya, J., Arya, S., Gusti, M., Eka, P. (2016). Prototyping SMS Forensic Tool Application Based On Digital Forensic Research Workshop 2001 (DFRWS) Investigation Model Case Study **:** *SMS Togel* in Indonesia. *International Conference on Information Technology Systems and Innovation (ICITSI).*

Rizdqi, A. R., Yudi, P., & Bambang, S. (2017) Implementasi dan Analisis Foresika Digital Pada Fitur Trim Solid State Drive (SSD). *Jurnal TEKNOMATIKA***,** Vol. 9. No. 2.

Sammons, J. (2012). The Basic Of Digital Forensic, *The Primer For Getting Started in Digital Forensics*.

Software Autopsy. Tersedia https://www.autopsy.com/ (diakses pada tanggal 4 Maret 2019).

Software OSForensics. Tersedia https://www.osforensics.com/products.html (diakses pada tanggal 4 Maret 2019).

Software RecoverMyFiles - Profesional Edition. Tersedia http://www.recovermyfiles.com/ (diakses pada tanggal 20 Agustus 2019).