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

by Ardiansyah & Marza Ihsan Marzuki Seminar Nasional

Submission date: 10-Nov-2019 03:47PM (UTC+0700)
Submission ID: 1210624625
File name: 47_odon.sukses1573291051_full.pdf (1.03M)
Word count: 3695
Character count: 23041

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

Ardiansyah[1], Marza Ihsan Marzuki[2]

[1] Teknik Elektro, Universitas Mercu Buana
Email: odon.sukses@gmail.com

[2] Teknik Elektro, Universitas Mercu Buana
Email: marza.ihsan@mercubuana.ac.id

ABSTRAK

Kasus *cyber crime* 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 *files recovery*, yaitu suatu metode untuk mengambil *file logical* 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 investigasi *digital forensics* mendapatkan bukti *digital*. Aktifnya fitur *trim* pada *solid state drive* terbukti berpengaruh terhadap praktik *examination* dan *recovery*, dengan kondisi tersebut persentase keberhasilan me-*recovery file* hanya 29% dan 88% dengan fitur *trim* nonaktif.

Kata Kunci : *digital forensics, digital forensics research workshop, solid state drive*

ABSTRACT

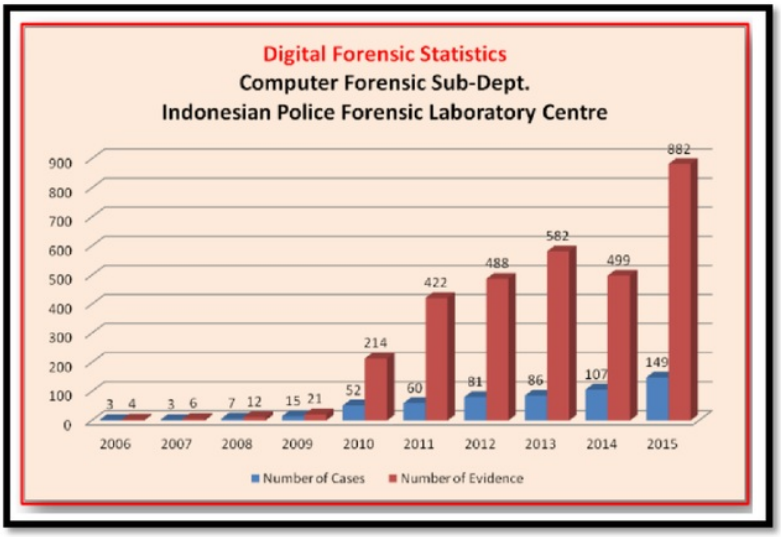
Cyber crime cases in Indonesia have increased by 15% each year or an average of 56 cases increase annually, according to the National Police Headquarters Forensic Laboratory. Digital forensics investigations have different ways to obtain digital evidence such as computer forensics, mobile forensics, network forensics and database forensics. Computer forensics investigation on solid state drive storage media in hard format to obtain digital evidence related to file recovery, which is a method for retrieving logical files or recovering files that have been deleted or lost because they are no longer recorded in the NTFS file system (New Technology File System) in the Windows operating system. This study uses a digital forensics research workshop method to investigate digital forensics to obtain digital evidence. The active trim feature on the solid state drive is proven to affect the practice of examination and recovery, with this condition the percentage of successful recovery of files is only 29% and 88% with the trim feature is disabled.

Keywords : digital forensics, digital forensics research workshop, solid state drive

1. Pendahuluan

Di Indonesia, menurut Digital Laboratorium Forensik Mabes Polri pada tahun 2006 hingga 2015, seperti yang terihat pada gambar 1. Kejahatan *cyber crime* tiap tahunnya mengalami peningkatan yang signifikan pada tahun 2015 terdapat 149 kasus *cycber crime* 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. (Ademu, 2011). Barang bukti dapat berupa bentuk fisik dari perangkat elektronik tersebut atau dapat berupa media

penyimpanan *(storage device)* yaitu *hard disk / solid state drive*, sedangkan barang bukti *digital* dapat berupa *file* dokumen, *file history,* atau *file log* yang berisikan data - data.



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 me[1]komparasikan berbagai *tools forensics* seperti Autopsy, OSForensics dan RecoveryMyFiles 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 forensi*[5] dilakukan untuk mendapatkan bukti *digital* yang *valid.* (Alharbi, 2011). *Digital forensics* adalah cabang ilmu forensik yang bersangkutan dengan penggunaan informasi *digital* yang dihasilkan, disimpan dan ditransmisikan oleh komputer sebagai sumber bukti dalam investigasi dan proses hukum. (Rahaditya, 2016).

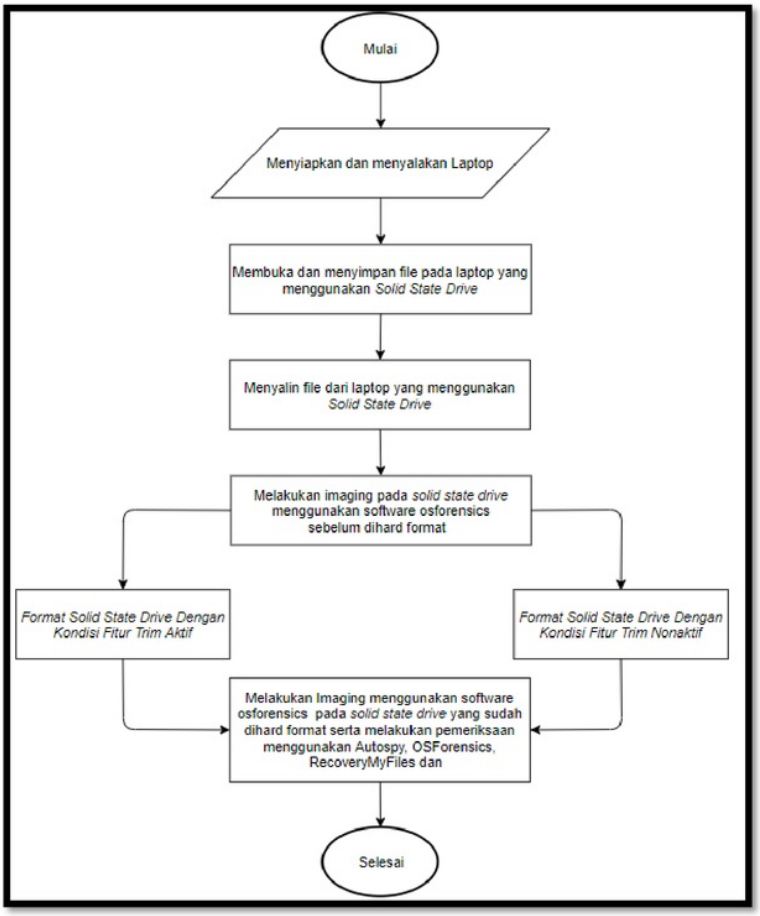
Investigasi *digital forensics* memiliki cara yang berbeda untuk mendapatkan bukti *digital* seperti komputer *forensics*, *mobile forensics*, *network forensics* dan *database forensics*. [8]omputer *forensics* adalah ilmu *forensics* yang menjelaskan keadaan saat ini di artefak *digital* yang berkaitan dengan bukti legal yang ditemui pada komputer dan media penyimpanan dari peristiwa *cyber crime.* (Bahadur, 2015). komputer *forensics* pada me[3]a penyimpanan *solid state drive* yang di *hard format* untuk mendapatkan bukti *digital* berkaitan dengan *files recovery*, yaitu suatu metode untuk mengambil *file logical* 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. Hal ini menjadikan tantangan bagi investigator *forensics*, bagaimana bukti *digital* pada media penyimpanan *solid state drive* yang di *hard format* ? dan bagaimana mekanisme *digital forensics research workshop* untuk mendapatkan bukti *digital* dari *solid state drive* yang di *hard format* ?

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 RecoveryMyFile 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*.

2. Metode

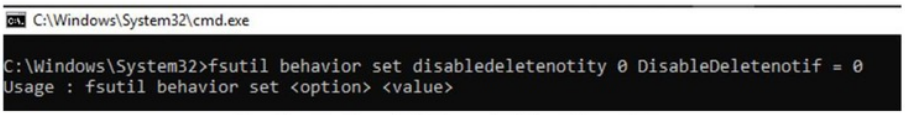
Penelitian ini menadaptasi dan mengimplementasikan metode *digital forensics research workshop* (DFRWS). Metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis sehingga dapat dijadikan pedoman dalam 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. Pembuatan skenario dibuat agar simulasi dapat berjalan sesuai yang diharapkan dan dapat memenuhi target yang diinginkan.



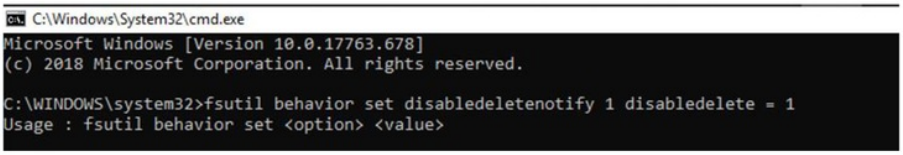
Gambar 2. Alur Skenario

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, Autopsy dan RecoveryMyFiles. Alur pada skenario dapat dilihat pada gambar 2. dibagi menjadi 2 kondisi saat melakukan *hard format* dengan kondisi mengaktifkan fitur *trim* dan menonaktifkan fitur *trim* pada laptop.

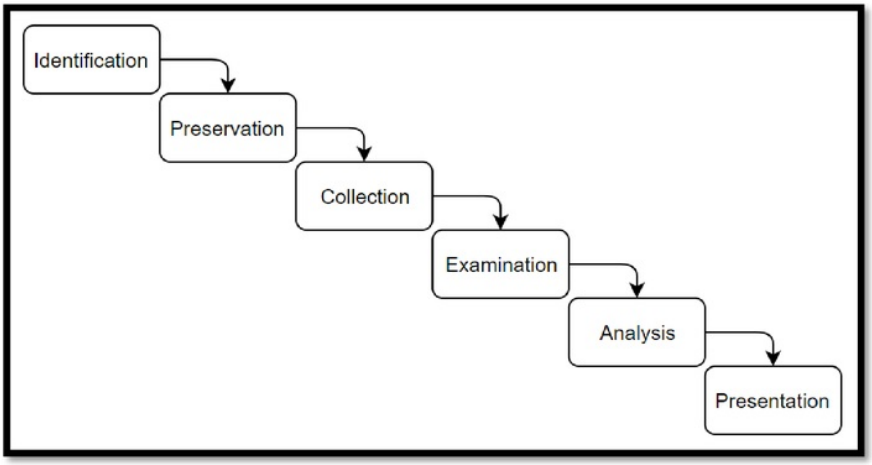


Gambar 3. Kondisi Mengaktifkan Fitur *Trim*



Gambar 4. Kondisi Menonaktifkan Fitur *Trim*

Proses investigasi 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).

Tahap *identification* ini untuk melakukan penentuan kebutuhan yang akan diperlukan untuk penyelidikan dan pencarian bukti digital.

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.

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.

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.

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.

Tahap presentation untuk tahap in dimana melaporkan dan mempresentasikan hasil analisa sehingga dapat dipahami oleh publik.

3. Hasil dan Pembahasan

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 :

A. Tahap *Identification*

Tahap identifikasi dilakukan dengan mencari informasi dari kasus yang terjadi sebelumnya untuk dijadikan sebagai rujukan tentang pemahaman pada barang bukti yang sedang dilakukan pencarian.

Name	Date modified	Size
EXCEL1.xlsx	16/07/2019 18:17	335 KB
EXCEL2.xlsx	22/07/2019 10:01	44 KB
EXCEL3.xlsx	10/07/2019 21:59	128.920 KB
JPG1.jpg	16/07/2019 14:15	545 KB
JPG2.jpg	16/07/2019 11:17	1.693 KB
JPG3.jpg	23/05/2019 2:59	100 KB
PDF1.pdf	11/04/2019 17:23	308 KB
PDF2.pdf	11/04/2019 17:25	1.229 KB
PPT1.pptx	18/07/2019 16:46	45 KB
PPT2.pptx	16/07/2019 19:38	4.691 KB
TEXT1.txt	29/04/2019 7:54	3 KB
TEXT2.txt	29/04/2019 8:22	4 KB
WORD1.doc	02/04/2019 23:47	189 KB
WORD2.docx	02/04/2019 23:44	69 KB
WORD3.docx	16/01/2019 11:08	72 KB
WORD4.docx	11/05/2019 23:56	47 KB
WORD5.docx	13/02/2019 18:01	73 KB

Gambar 6. Sebelum di *Hard Format*

Name	Date modified	Size
EXCEL1.xlsx	08/08/2019 9:56	212 KB
EXCEL2.xlsx	08/08/2019 9:56	31 KB
EXCEL3.xlsx	08/08/2019 9:57	103.315 KB
JPG1.jpg	16/07/2019 14:15	545 KB
JPG2.jpg	16/07/2019 11:17	1.693 KB
JPG3.jpg	23/05/2019 2:59	100 KB
PDF1.pdf	11/04/2019 17:23	308 KB
PDF2.pdf	11/04/2019 17:25	1.229 KB
PPT1.pptx	08/08/2019 9:59	52 KB
PPT2.pptx	08/08/2019 9:59	4.307 KB
TEXT1.txt	08/08/2019 10:00	2 KB
TEXT2.txt	08/08/2019 10:00	2 KB
WORD1.doc	08/08/2019 10:00	84 KB
WORD2.docx	08/08/2019 10:01	49 KB
WORD3.docx	08/08/2019 10:04	67 KB
WORD4.docx	08/08/2019 10:04	22 KB
WORD5.docx	08/08/2019 10:03	67 KB

Gambar 7. Sesudah di *Hard Format*

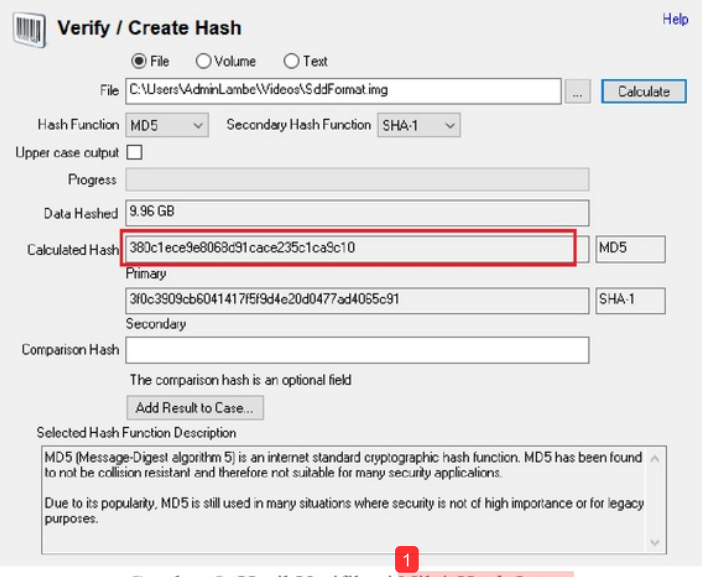
Sesuai dengan adanya pelaporan dari pelapor, bahwa ada indikasi perubahan data atau *file* yang terdapat pada laptop yang menggunakan *solid state drive*. Terdapat beberapa *file* yang hilang atau terhapus oleh *user* dan perubahan *size file* sebelumnya. Kita dapat mengetahui telah terjadi perubahan besarnya *size file* dan terbentuknya *date modified* yang baru. Tahap identifikasi ini melakukan identifikasi terhadap keadaan sebelum dan setelah terjadi.

B. 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.

C. Tahap *Collection*

Sesuai dengan scenario, 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*.

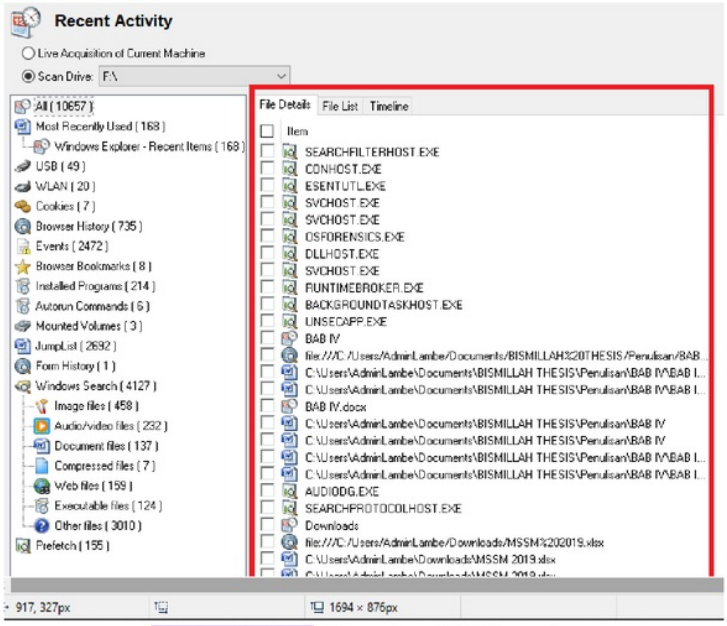


Gambar 8. Hasil Verifikasi Nilai *Hash Image*

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*.

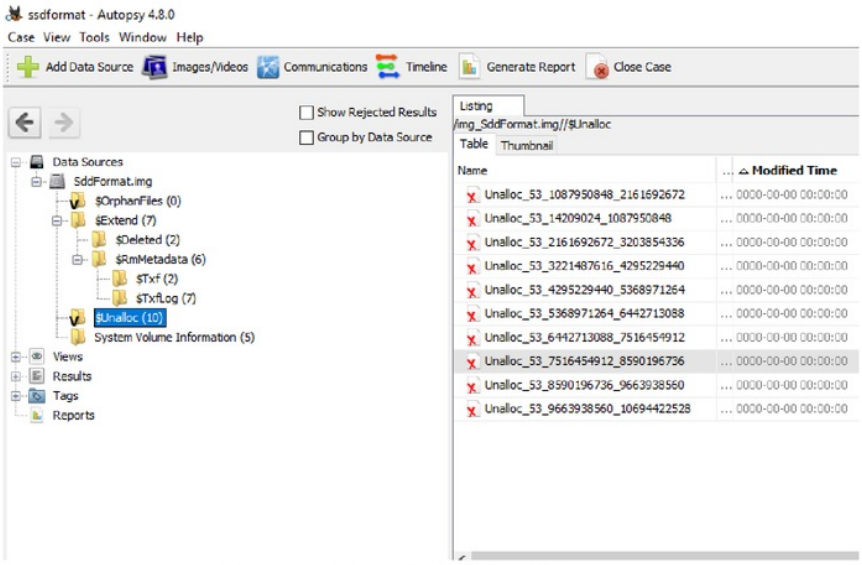
D. Tahap *Examination*

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 RecoveryMyFiles. Hasil eksaminasi dan analisa dengan OSforensics menunjukan struktur direktori dapat dilihat, namun hanya dapat dilihat catatan terakhir laptop saat digunakan (*recent activity*) dapat dilihat dari gambar 9.



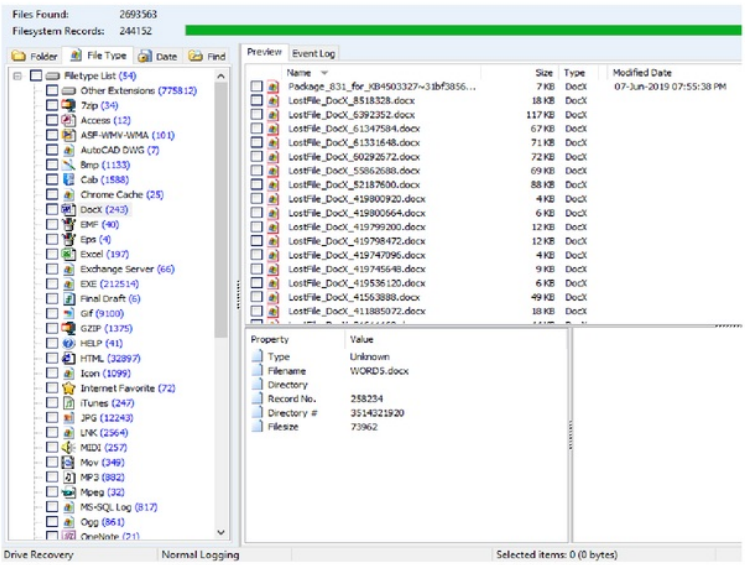
Gambar 9. Hasil Eksaminasi OSForensics

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.



Gambar 10. Hasil Eksaminasi Autospy

Sedangkan menggunakan RecoveryMyFiles 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 11. Hasil Eksaminasi RecoveryMyFiles

Setelah melihat hasil eksaminasi dari 3 penggunaan *tools forensics,* RecoveryMyFiles merupakan hasil yang paling banyak. 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.*

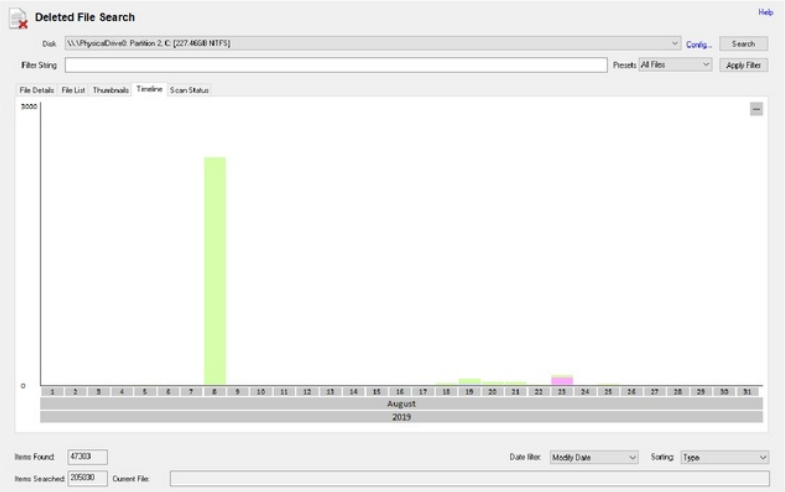
E. Tahap *Analysis*

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.

Gambar 12. Aktivitas *User* Pada Laptop

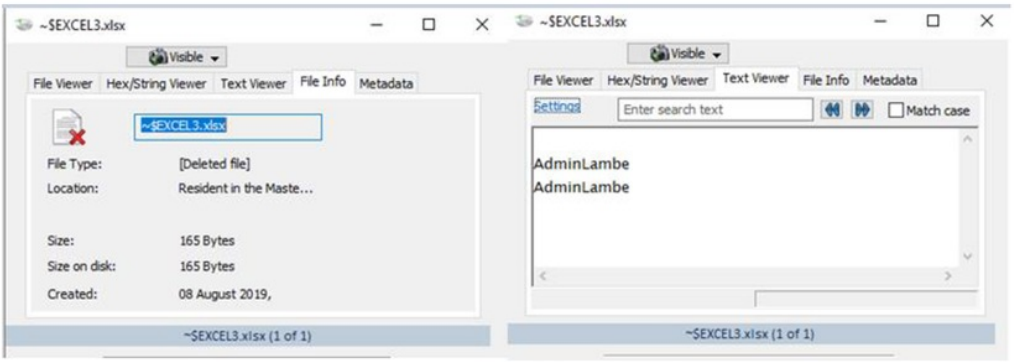
Dengan menggunakan OSForensics dapat dilihat aktivitas *user* pada penggunaan laptop, bahwa pada tanggal 8 Agustus 2019 merupakan aktivitas paling intens dibandingkan tanggal yang lain dibulan Agustus 2019, dengan menggunakan fitur *delete file search* yang ada pada

tools OSForensics. Kita dapat mengetahui bahwa telah terjadi penghapusan *file* pada tanggal tersebut, dapat dilihat pada gambar 13.



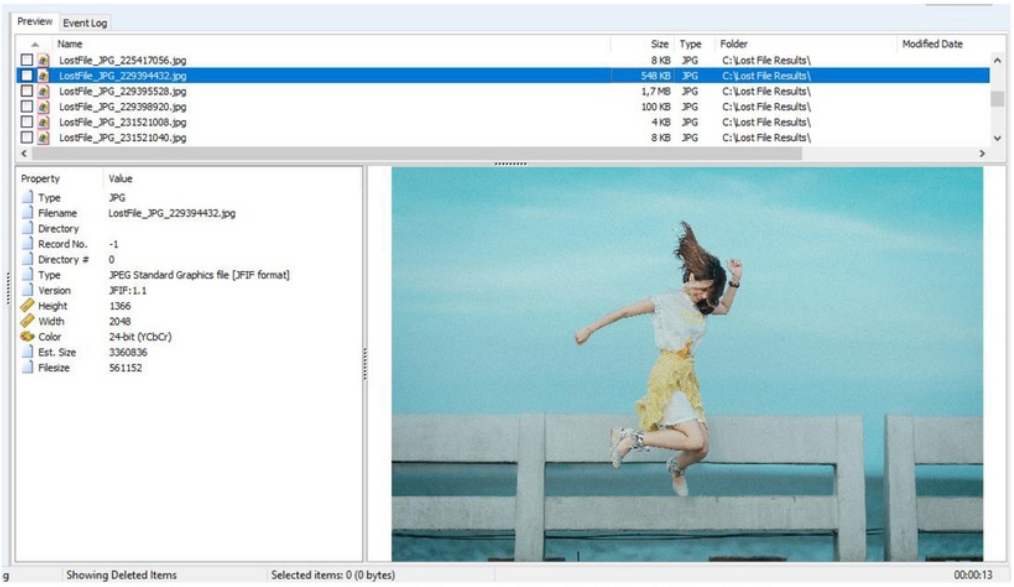
Gambar 13. Hasil *Scaning Delete File Search*

Dengan menggunakan fitur *delete file search* pada OSForensics kita dapat mengetahui *user* yang digunakan untuk melakukan penghapusan *file* pada laptop yang dijadikan barang bukti. Dan dilihat dari tanggal pada saat *file* tersebut hilang sesuai dengan fitur *history user activity* dan fitur *delete file search*. Dari informasi yang telah diperoleh dapat mempertegas asumsi kita bahwa telah terjadi penghapusan file pada tanggal 8 Agustus 2019 menggunakan user AdminLambe dapat dilihat pada gambar 14.



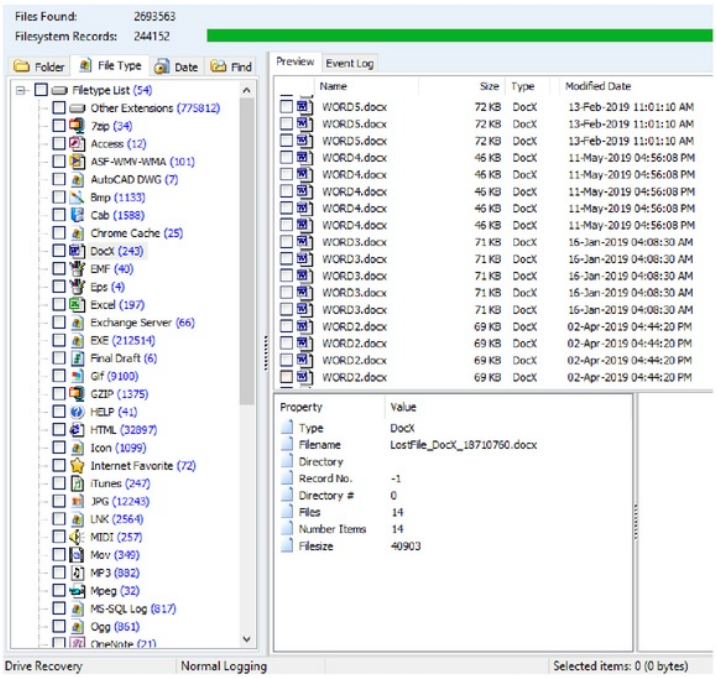
Gambar 14. Bukti User Yang Digunakan

Sesuai dengan skenario yang telah dibuat, saat melakukan *hard format* pada *solid state drive* kita mengkondisikan dengan mengaktifkan fitur *trim* dan menonaktifkan fitur *trim* pada *solid state drive*. Hasil *recovery* dengan menggunakan RecoveryMyFiles untuk *solid state drive* dengan kondisi mengaktifkan fitur *trim* dari *files* yang telah di *hard format* menemukan 5 *file* yang berhasil di-*recovery* dari 17 *file* yang dijadikan bahan simulasi. Sedangkan skenario dengan kondisi menonaktifkan fitur *trim* pada *solid state drive* saat di *hard format*, hasil dari *recovery* dengan menggunakan RecoveryMyFiles. Dari *files* yang telah di *hard format* hanya *file extension* *.ppt yang tidak dapat di-*recovery*, sedangkan *file* yang lainnya dijadikan bahan simulasi berhasil di-*recovery*.



Gambar 15. Hasil *Recovery* Kondisi Fitur Trim Aktif

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. Dengan melihat *size file* yang berhasil di-*recovery* memiliki nilai yang serupa dengan *size file* asli.



Gambar 16. Hasil *Recovery* Kondisi Fitur Trim Nonaktif

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*.

F. *Prsentation*

Untuk melihat keaslian dari *file* tersebut maka dilakukan teknik *hashing* menggunakan *tools* OSfornesic, diasumsikan bahwa jika nilai *hash file* asli dengan *file* yang telah dilakukan perubahan memiliki nilai *hash* yang sama, dapat dikatakan tidak terjadi suatu penghilangan atau perubahan *file* pada *solid state drive*. Sedangkan jika memiliki hasil nilai *hash* yang berbeda maka perlu dibandingkan dengan nilai hash hasil *recovery*, untuk menunjukan bahwa telah terjadi penghilangan atau perubahan *file* pada *solid state drive*. Sehingga hasil yang didapat dari *recovery solid state drive* yang di *hard format* dapat dijadikan sebagai bukti *digital* yang *valid*.

Name	MD5	Size
EXCEL1.XLSX	4B8A2562A8E8C442214ED25A29F20BBF	333.5 KB
EXCEL2.XLSX	7252AC58B256325FE9C9B4C5258ECB55	43.95 KB
EXCEL3.XLSX	07771229B712F57974BC503DAA8A3B0F	125.9 MB
JPG1.JPG	32BC68E49B2E8A22786DB89A82066FF0	544.6 KB
JPG2.JPG	FD245D64AB8C4ECEC49B733A14125BC7	1.65 MB
JPG3.JPG	9A2BAAD48A060D8F7DC87F880F0A427F	99.72 KB
PDF1.PDF	B14E9EA22C6F0B2797CA73F2E17EBCDD	307.7 KB
PDF2.PDF	5767885985C9A14CB51F6233A968B19C	1.20 MB
PPT1.PPTX	008A606A03E5E112DA026D900A3B9761	44.04 KB
PPT2.PPTX	E213E30F09EE82EE2E8909CBB974293A	4.58 MB
TEXT1.TXT	5306D858B71E76AE50B1617FFB4FD5CB	2.54 KB
TEXT2.TXT	A39B531EA2CC9576717BA003C5CBE82B	3.50 KB
WORD1.DOC	9999100CE66F91255625F913E4B5119B	188.5 KB
WORD2.DOCX	EF6D1EDE51ADD3C0380C4F8ABC1B84A2	68.83 KB
WORD3.DOCX	63E9283A835BFE0DDBF8EA05A9790A36	71.13 KB
WORD4.DOCX	BE2BE5509468F8F0DC57C7E5AB0869A9	46.27 KB
WORD5.DOCX	8270CF54ECCCF8E89184B16D313A6637	72.23 KB

Gambar 17. Niai *hashing* pada *file asli*

Dapat kita lihat dari gambar 17 dengan gambar 18 nilai *hash* dan *size file* dari *file* asli dengan *file* yang telah dilakukan perubahan memiliki nilai hash yang berbeda, *size file* juga mengalami perbedaan *size* nya. Sehingga dapat dikatakan telah terjadi suatu penghilangan atau perubahan file pada solid state drive. Maka dari itu, kita perlu membandingkan hasil nilai *hashing* pada *file* asli dengan hasil nilai *file hashing* yang berhasil di-*recovery* pada *solid state drive* yang di hard format dengan kondisi fitur *trim* aktif dan fitur trim *nonaktif*.

Name	MD5	Size
EXCEL1.XLSX	524A1CDD800F8451EF81E81C505C9C48	211.6 KB
EXCEL2.XLSX	55680363BAF02061318908992D0BB619	30.24 KB
EXCEL3.XLSX	147CC0E334160BCA9C4F4B891E052140	100.9 MB
JPG1.JPG	32BC68E49B2E8A22786DB89A82066FF0	544.6 KB
JPG2.JPG	FD245D64AB8C4ECEC49B733A14125BC7	1.65 MB
JPG3.JPG	9A2BAAD48A060D8F7DC87F880F0A427F	99.72 KB
PDF1.PDF	B14E9EA22C6F0B2797CA73F2E17EBCDD	307.7 KB
PDF2.PDF	5767885985C9A14CB51F6233A968B19C	1.20 MB
PPT1.PPTX	A2F50F5D3E99A2E06AC7DD589256EA58	51.18 KB
PPT2.PPTX	2D5D5FEB45A0389ACF56A7BB06143906	4.21 MB
TEXT1.TXT	97D72DDFB60A98D62D7A7C54F6BA37F4	1.67 KB
TEXT2.TXT	3DEF1CB538CEB8AFDB4534171C2F7166	1.87 KB
WORD1.DOC	D65D432B6A61C427CBD83DC4ED447F04	83.50 KB
WORD2.DOCX	4E4B61C335657F7DFCCAF46381E9199A	48.83 KB
WORD3.DOCX	CD679D4E28A56E9EB309EF5F11079E9A	66.51 KB
WORD4.DOCX	A7AD22FC08F3764FCD0E88E890ED6C98	21.73 KB
WORD5.DOCX	59FAF0932C0765997CE4BB4EA6C9D421	66.36 KB

Gambar 18. Niai *Hashing* Pada *File* Perubahan

Dari *file* yang berhasil di-*recovery* pada *solid state drive* yang di *hard format* dengan kondisi fitur *trim* aktif dan fitur *trim* nonaktif memliki jumlah yang berbeda. Perbandingan files yang berhasil di-recovery dengan kondisi fitur *trim* aktif dan nonaktif sebagai berikut :

Table 1. Rincian Hasil *Recovery File* 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**

Lanjutan Table 1. Rincian Hasil *Recovery File* fitur *trim* aktif dan nonaktif

Nama File	Hasil Recovery Fitur Trim Aktif	Hasil Recovery Fitur Trim Nonaktif
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 2. 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**

Lanjutan Table 2. Hasil Verifikasi dan Validasi Keaslian *File* dengan *Hashing*

File Asli	*Recovery* Fitur *Trim* Aktif	*Recovery* Fitur Nonaktif
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
JPG1.JPG Nilai MD5 : 32bc68e49b2e8a22786db89a82066ff0	LostFile_JPG_229394432.jpg Nilai MD5 : 32bc68e49b2e8a22786db89a82066ff0	JPG1.JPG Nilai MD5 : 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.*

4. 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*.

5. Kesimpulan dan Saran

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 dua kesimpulan yaitu sebagai berikut :

A. Kesimpulan

Bukti *digital* diperoleh menggunakan *tools* RercoveryMyFiles dari hasil *recovery solid state drive* yang di *hard format* dengan kondisi fitur *trim* aktif dan nonaktif memilki hasil yang beragam. Jika dilakukan perhitungan tingkat *presentase* keberhasilan yang di-*recovery* dengan kondisi fitur *trim* aktif hanya memiliki nilai 29 % yang diperoleh dari 17 *file* yang disiapkan untuk pengujian, yang berhasil di-*recovery* hanya 5 *file*. Sedangkan fitur *trim* nonaktif 88% yang berhasil di-*recovery* hanya 15 *file* dari 17 *file*. 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.

B. Saran

Saat menangani kasus penghilangan data pada media penyimpanan *solid state drive* dengan kondisi fitur *trim* aktif. Diperlukan *tools forensics professional* yang lebih banyak. Penggunaan *tools forensics* seperti winhex and x-ways *forensics* memiliki banyak keunggulan dalam proses *recovery* sehingga dapat membantu proses *digital forensics* dalam mendapatkan bukti digital. (Vidilia, 2016). Dan Penangan suatu kasus kejahatan komputer dengan media penyimpanan *solid state drive* yang di *hard format* dengan kondisi fitur *trim* aktif untuk menemukan bukti *digital* Dengan menggunakan *operation system* Windows 10 Home 64 bit. Maka diperlukan penanganan proses *digital forensics* yang cepat setelah *solid state drive* di *hard format*, untuk mendapatkan informasi mengenani penanganan bukti *digital* dari media penyimpanan. Karena *file system NTFS (New Technology File System)* yang ada pada *operation system Windows* akan menghapus *file* lebih cepat untuk me-reset *blok - blok* yang ada pada disk menjadi ruang kosong untuk menjadi tambahan pada *solid state drive.* (Alastair, 2013).

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

ORIGINALITY REPORT

19%	16%	3%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	11%
2	Andri Lesmana Suryana, Reza El Akbar, Nur Widiyasono. "Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)", Jurnal Edukasi dan Penelitian Informatika (JEPIN), 2016 Publication	2%
3	www.scribd.com Internet Source	2%
4	media.neliti.com Internet Source	1%
5	Submitted to Udayana University Student Paper	1%
6	Submitted to Universitas Mercu Buana Student Paper	1%
7	www.marcomattiucci.it	

	Internet Source	<1%
8	onnadia.blogspot.com Internet Source	<1%
9	Submitted to Lebanese American University Student Paper	<1%
10	sentia.polinema.ac.id Internet Source	<1%
11	pcsupport.about.com Internet Source	<1%
12	www.pricebook.co.id Internet Source	<1%
13	mursic.ifrance.com Internet Source	<1%
14	Submitted to Universitas Kristen Satya Wacana Student Paper	<1%
15	Submitted to University of Glamorgan Student Paper	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		