

PERBANDINGAN CARVING TOOLS FOREMOST DAN SCALPEL

Ruchdi Muttaqin, Arini, Fitri Mintarsih

Program Studi Teknik Informatika, Fakultas Sains dan Teknologi,
UIN Syarif Hidayatullah Jakarta

ABSTRAK

Penyimpanan data dalam bentuk digital kini telah banyak dilakukan. Perlu alat yang memiliki performa baik untuk menangani kasus kehilangan data. Untuk mengetahui performa dari alat carving foremost dan scalpel digunakan model simulasi menurut chase et all yang memiliki enam langkah penting yaitu: mendefinisikan masalah, membangun model simulasi, menentukan nilai awal variable dan parameter, melakukan evaluasi hasil, melakukan validasi, dan membuat proposal penelitian baru. Hasil dari simulasi yang dilakukan menunjukkan performa yang diberikan oleh foremost relatif lebih baik dibanding dengan scalpel.

Kata Kunci : Carving, Foremost, Scalpel

I. PENDAHULUAN

1.1. Latar Belakang

Komputer kini telah menjadi populer di masyarakat, kegunaan komputer dalam kehidupan sehari-hari pun semakin luas. Penyimpanan data dalam bentuk digital pun juga semakin banyak. Penyimpanan data dalam bentuk digital memiliki banyak kelebihan, namun demikian data dalam bentuk digital sangat rentan untuk hilang atau terhapus. Untuk itu dibutuhkan suatu cara untuk menangani kehilangan data digital. Hal ini menyebabkan munculnya kebutuhan spesialis computer forensic untuk menganalisa media penyimpanan digital untuk dapat mengembalikan data digital yang hilang.

Menurut Golden G. Richard III dalam jurnalnya yang berjudul Scalpel: A Frugal, High Performance File Carver, disc carving merupakan aspek penting dalam computer forensic untuk dapat mengembalikan data yang telah terhapus atau dihapus. Disc carving bekerja dengan menggunakan data raw yang terdapat dalam media penyimpanan. Alat forensic seperti ILOOK, Encase, dan FTK (Forensic Tools Kit) mengembalikan data dengan berfokus pada metadata. Penggunaan metadata menjadi efektif apabila metadata yang dibutuhkan ada dalam media penyimpanan yang bersangkutan, dan apabila metadata yang dibutuhkan tidak ada biasanya cara ini akan mengalami kegagalan. Namun demikian data yang bersangkutan seringkali masih terdapat dalam disc yang bersangkutan, hanya perlu menggunakan cara yang sesuai (dengan menggunakan informasi raw) untuk dapat mendapatkan data tersebut.

FTK dan Encase merupakan alat yang sesuai untuk masalah pengembalian data menggunakan metadata namun keduanya merupakan produk berbasis Microsoft Windows dan harganya sangat mahal. Dengan mahalnya biaya yang perlu dikeluarkan dan metode ekstraksi yang closed source merupakan penghambat utama bagi komunitas forensic yang ingin menggunakan alat yang bagus dan dapat dengan baik melakukan ekstraksi file. Hal ini menyebabkan beberapa developers dan forensic researcher bergerak untuk membuat komunitas open source.

Menurut Nicholas Mikus dalam tesisnya yang berjudul An Analysis of Disc Carving Techniques, di dunia open source Sleuthkit milik Brian Carrier menjadi alat standar untuk melakukan analisis forensic di sistem UNIX. Alat ini menyediakan kemampuan yang cukup lengkap bagi penguji yang menggunakan sistem UNIX dan bagi pihak-pihak yang tidak dapat menggunakan alat keluaran dari Windows karena mengalami kesulitan finansial. Namun demikian terdapat satu kekurangan dari Sleuthkit yaitu tidak terdapatnya fungsi carving. Di sistem UNIX terdapat beberapa alat carving seperti tcpxtract, chaosreader, msramdmp, Foremost dan Scalpel. Namun hanya Foremost dan Scalpel yang memiliki fungsi untuk melakukan carving pada media penyimpanan seperti harddisk atau flashdisk. Foremost sendiri awalnya dikembangkan di US Air Force (dikembangkan oleh Kris Kendall dan Jesse Kornblum dari USA Air Force Office of Special Investigations) yang kemudian dikembangkan kembali oleh Nick Mikus untuk mendapatkan performa yang lebih baik. Sedangkan Scalpel merupakan penulisan ulang dari Foremost 0.69 yang dilakukan oleh Golden G. Richard III, untuk

meningkatkan performa dan mengurangi penggunaan memori.

Menurut Thomas Laurenson dalam jurnalnya yang berjudul *Performance Analysis of File Carving Tools*, disc carving, dapat menjadi proses yang sulit dan kompleks dan lebih jauh lagi membingungkan dengan banyaknya alat forensik yang tersedia. Banyak investigator forensik yang tidak sadar akan kemampuan atau keterbatasan dari berbagai macam alat untuk melakukan carving. Dari banyaknya alat untuk melakukan carving, tentunya investigator digital menginginkan alat yang dapat memberikan performa terbaik dan dapat dinilai berdasarkan: 1) Prosentase file yang dapat dikembalikan, 2) Kebenaran dan kehandalan keluaran dari alat (validitas), 3) Kecepatan proses (durasi).

Berdasarkan uraian diatas penulis tertarik untuk melakukan penelitian dengan judul “Perbandingan Carving Tools Foremost dan Scalpel” yang dapat digunakan oleh investigator digital sebagai referensi dalam memilih alat carving yang lebih sesuai untuk melakukan pengembalian data digital.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang penulis uraikan, identifikasi masalah pada penelitian ini adalah sebagai berikut: 1. Manakah yang lebih cepat durasi proses pengembalian file antara Foremost dan Scalpel? 2. Manakah yang mampu lebih banyak mengembalikan file yang telah hilang antara Foremost dan Scalpel? 3. Bagaimanakah validitas file yang dikembalikan menggunakan foremost dan scalpel

II. DASAR TEORI

2.1 Disk Drive

Menurut EC Council (2010:2) disk drive adalah sebuah mekanisme membaca dan menulis data kedalam disk. Disk dalam disk drive berputar dengan kecepatan tinggi, dan heads dalam disk drive berguna untuk membaca dan menulis data. Disk drive dengan tipe yang berbeda menggunakan disk dengan tipe yang berbeda pula. Untuk contoh, sebuah hard disk drive (HDD) mengakses hard disk, dan sebuah floppy disk drive (FDD) mengakses floppy disk. Sebuah optical disk drive (ODD) membaca dan menulis dari optical disc.

2.2 File System

Menurut Merola (2008:5) file system adalah sebuah struktur untuk penyimpanan data dan pengorganisasian file komputer dan data yang ada

didalamnya untuk membuatnya mudah diakses dan ditemukan. Beberapa file system yang umum digunakan antara lain: File Allocation Table (FAT) / New Technology File System (NTFS) pada sistem operasi Windows, dan UFS / JFS pada sistem operasi UNIX. Software file system bertanggung jawab dalam mengorganisasi sector pada disk (biasanya 512 bytes tiap sector) kedalam file dan directory dan menjaga sector tetap pada file yang bersangkutan (allocated) dan menjaga sector mana yang masih belum digunakan (unallocated).

2.3 File dan Carved File

Menurut Merola (2008:7) file adalah sebuah istilah yang digunakan di dunia komputer untuk mengindikasikan sebuah blok dari informasi yang disimpan (binary digits) seperti sebuah dokumen dalam file doc, dan sebuah foto dalam file jpg atau sebuah program dalam file exe. Selanjutnya tergantung dari aplikasi yang bersangkutan untuk memahami blok dari binary digits dengan tujuan untuk menampilkan atau mengeksekusi konten yang ada dengan benar. Files dapat dibuat, dipindah, dimodifikasi, diduplikat, dan dihapus. Dalam banyak kasus, program komputer yang berjalan di komputer yang melakukan operasi tersebut, namun demikian pengguna juga dapat melakukan manipulasi terhadap file bila dibutuhkan.

Hampir setiap sistem komputer menggunakan ekstensi dalam nama file untuk membantu mengidentifikasi apa yang dikandung oleh suatu file (tipe file). Misalnya, ekstensi terdiri dari sebuah titik pada akhir nama sebuah file, diikuti tiga huruf untuk mengidentifikasi tipe dari file, selanjutnya nama file dengan akhiran “.txt” mengidentifikasikan sebuah file teks. Sebenarnya ekstensi diperkenalkan untuk membantu sistem operasi dalam mengidentifikasi program apa yang berasosiasi dengan suatu file. Untuk beberapa alasan sekarang ini program cenderung menganalisa struktur dari file daripada melihat ekstensi dari file, oleh karena itu sekarang ini magic number telah menjadi standar yang digunakan oleh industri. Menurut Nicholas Mickus (2005:2) file adalah sebuah ruang pada disk yang telah teralokasi (allocated) dalam beberapa block pada file system. Carved file menurut NIST (2014:3) adalah, sebuah file yang dibuat oleh alat carving yang diakui sebagai salah satu sumber file yang terdapat dalam arena pencarian.

2.4 Data Block

Data Block menurut NIST (2014:3) adalah, alokasi unit data (block) yang spesifik dari filesystem, yang biasanya merupakan kelipatan dari

512 bytes. Beberapa filesystem dapat menggunakan istilah lain untuk menggambarkan block data seperti, cluster dalam filesystem FAT.

2.5 Slack Space

Menurut Mickus (2005:2) slack space adalah sebuah ruang yang tidak digunakan dari sebuah block yang allocated untuk sebuah file. Ruang ini berada diantara byte terakhir dari sebuah file dan akhir dari block yang bersangkutan. Jumlah slack space yang dimiliki oleh sebuah file dapat dihitung sebagai ukuran file modulus ukuran block. Jadi karena semua file tidak berakhir tepat pada batas block, maka kelebihan ruang ini dapat digunakan untuk menyembunyikan data dari tampilan file system.

2.6 Magic Number

Menurut Merola (2008:8) magic number memiliki banyak artian, namun apabila berfokus pada file, maka magic number memiliki arti sebuah nilai konstan yang digunakan untuk mengidentifikasi sebuah format. Mendeteksi konstan adalah sebuah cara sederhana untuk membedakan format suatu file, pada dasarnya setiap file mempunyai header dan footer dengan tujuan agar dapat dikenali, sebagai contoh sebuah file pdf dimulai dengan “%PDF” and diakhiri dengan “%EOF” sedangkan file gambar jpg dimulai dengan “0xFFD8” dan diakhiri dengan “0xFFD9”. Nilai konstan ini disebut magic number.

2.7 Fragmentation

Menurut Pal dan Memon (2009:62) dengan ditambahkan sebuah file, dimodifikasi, dan dihapus, kebanyakan file system mengalami fragmentasi. Fragmentasi file dikatakan terjadi ketika tidak disimpan dalam urutan yang benar dalam cluster yang berurut pada disk. Menurut Beek (2011:5) sistem operasi modern mencoba menulis file tanpa fragmentasi karena file akan lebih cepat ditulis dan dibaca. Tetapi ada tiga kondisi dimana sistem operasi harus menulis file dengan dua atau lebih fragmen: 1. Sector Kosong Hampir Habis Tidak terdapat lagi sector berdekatan yang mampu menampung file tanpa fragmentasi. Hal ini biasanya terjadi apabila drive telah digunakan dalam waktu yang lama, dan diisi hampir mendekati kapasitas maksimal, dan memiliki banyak file yang ditambah dan dihapus kurang lebih secara acak dari waktu ke waktu. 2. Penambahan Data Pada File Jika data ditambahkan pada file yang sudah ada, tidak terdapat unallocated sectors diakhir dari file untuk mengakomodasi data yang baru. Dalam kasus ini beberapa file system akan merelokasi file asli, tetapi kebanyakan hanya

akan menuliskan data yang ditambahkan pada lokasi lain. 3. Keterbatasan File system File System tidak memiliki kemampuan untuk menulis file dengan ukuran tertentu secara berurut. Sebagai contoh, Unix File System (UFS) akan melakukan fragmentasi pada file yang panjang atau memiliki bytes pada akhir file yang tidak akan muat pada jumlah sector yang sama.

2.8 Konsep Carving

2.8.1 Disc Carving, Data Carving, File Carving

Menurut Mickus (2005:2) disc carving adalah kemampuan untuk mendapatkan kembali file sebuah medium yang memiliki atau tidak memiliki filesystem. Disc carving biasanya digunakan untuk melakukan ekstraksi file dari unallocated atau slack space dari file system yang diberikan.

Disc carving merupakan sinonim dari data carving. Menurut Merola (2008:4) data carving adalah proses dari ekstraksi sebuah koleksi data dari seperangkat data yang lebih besar. Teknik data carving biasanya digunakan pada investigasi digital ketika ruang unallocated dari file system dianalisa untuk mengekstrak file. File di carve dari ruang unallocated menggunakan nilai header dan footer tertentu. Struktur file system tidak digunakan selama proses ini berlangsung. Menurut Beek (2011:3) file carving berurusan dengan raw data pada media dan tidak menggunakan struktur file system selama proses berlangsung. Berdasarkan tiga definisi diatas maka dapat dikatakan disc carving, data carving, dan file carving merupakan sebuah sinonim dimana ketiganya menggunakan raw data dan tidak menggunakan struktur dari file system selama proses berlangsung.

2.8.2 Klasifikasi Carving

Disc carving dapat dikelompokkan sebagai basic dan advanced. Basic disc carving diasumsikan: 1. Awal dari file tidak tertimpa. 2. File tidak terfragmentasi. 3. File tidak dikompresi. Pada dasarnya carving jenis ini dibuat menggunakan header dan footer. Sedangkan advanced disc carving terjadi walau file mengalami fragmentasi, dimana file yang terfragmentasi: 1. Tidak berurutan 2. Rusak 3. Hilang

2.9 Alat Carving

2.9.1 Foremost

Menurut Merola (2008:19) foremost adalah alat yang terkenal, awalnya dikembangkan di US Airforce (dikembangkan oleh Kris Kendall dan Jesse Kornblum dari U.S Air Force Office of Special Investigation). Foremost berkerja pada sebuah image file, seperti yang dibuat dari dd,

safeback, encase, dan lain-lain, atau secara langsung dari sebuah drive. Menurut Mickus (2005:7) foremost adalah sebuah alat forensik yang open source dibuat untuk platform linux dan dikembangkan oleh agen spesial Kris Kendall dan Jesse Kornblum dari U.S Air Force Office of Special Investigation. Sesuai dengan 17 USC 105, alat ini tidak diberikan perlindungan hak cipta karena merupakan pekerjaan dari pemerintah Amerika Serikat. Alat ini terinspirasi dan didesain untuk mengimitasi fungsi dari program DOS CarvThis yang ditulis oleh Defense Computer Forensic Lab.

Foremost memungkinkan pemeriksa forensik untuk mendapatkan kembali file atau partial file secara otomatis dari sebuah bit image (atau langsung dari media yang bersangkutan) berdasarkan file header dan file footer yang telah ditentukan dalam sebuah file konfigurasi. Foremost bekerja dengan cara membaca media yang sedang diamati kedalam memori dengan ukuran yang telah ditentukan. Secara default ukuran potongan memorinya adalah 10MB, kemudian image akan dianalisa 10MB setiap waktu. Tiap potongan akan mencari file headers yang terkandung didalam file konfigurasi. Jika header yang cocok ditemukan maka foremost akan berusaha mencari akhir dari file yang bersangkutan. Foremost akan mencari footer (yang menandakan akhir dari file) sampai batas ukuran file yang ditentukan di file konfigurasi dicapai. Jika footer ditemukan maka file yang dipulihkan akan ditulis ke disk penyimpanan yang lain. Tetapi bila tidak ditemukan maka foremost akan mengeluarkan file dengan ukuran maksimum setelah header yang ditemukan. Jika footer tidak ditentukan maka foremost akan mengeluarkan file sesuai dengan ukuran maksimum yang ditentukan di file konfigurasi setiap ditemukan header yang bersangkutan. Menggunakan batas ukuran file yang tersedia berarti menghentikan foremost menambah data apabila footer yang sesuai tidak ditemukan. Ini merupakan pendekatan yang cukup efisien jika pasangan header/footer didefinisikan secara unik tetapi ini bukan merupakan kasus yang sering terjadi. Flowchart dan pseudo code foremost penulis lampirkan pada skripsi ini. Foremost dapat berjalan di sistem operasi linux dan windows. Untuk melakukan instalasi foremost di sistem operasi linux khususnya ubuntu, dapat dilakukan dengan melakukan perintah “sudo apt-get install foremost” pada terminal.

```
ruchdimuttaqin@ruchdimuttaqin:~$ sudo apt-get install foremost
```

Gambar 2.1: Perintah install foremost

Apabila proses instalasi sudah selesai maka foremost sudah dapat digunakan dan dapat di cek dengan memasukan perintah “foremost -V” pada terminal.

```
ruchdimuttaqin@ruchdimuttaqin:~$ foremost -V
1.5.7
This program is a work of the US Government. In
copyright protection is not available for any w
This is free software; see the source for copyl
warranty; not even for MERCHANTABILITY or FITNE
ruchdimuttaqin@ruchdimuttaqin:~$
```

Gambar 2.2: Memeriksa foremost

Untuk di sistem operasi windows dapat mengunduh file yang telah disediakan di sourceforge.net/projects/foremost/. Setelah proses pengunduhan selesai dapat dilakukan ekstraksi pada file yang telah diunduh dan melakukan proses compile kepada file yang telah di ekstraksi karena untuk versi windows foremost disediakan dalam bentuk source code. Foremost merupakan aplikasi yang berjalan di terminal dan tidak memiliki Graphical User Interface (GUI). Untuk menggunakan foremost masukan perintah foremost pada terminal yang telah terbuka. Untuk melihat perintah apa saja yang terdapat pada foremost dapat menggunakan perintah “man foremost”. Pada foremost terdapat banyak mode carving yang bisa dipilih, secara default kita dapat menjalankan proses carving dengan menggunakan perintah “foremost -v -T -i imagefile” di terminal.

```
@ruchdimuttaqin:~
ruchdimuttaqin@ruchdimuttaqin:~$ foremost -v -T -i imagefile
```

Gambar 2.3: Perintah menjalankan foremost

Perintah tersebut akan menjalan kan foremost dengan mode verbose [-v] dan akan membuat timestamp pada direktori keluaratan [-t] dengan media yang akan dilakukan pemeriksaan adalah imagefile [-i]. Setelah proses carving selesai maka akan menghasilkan folder dengan nama tipe file yang bersangkutan sesuai dengan tipe file apa saja yang ditemukan selama proses carving dan sebuah file teks yang berisikan laporan dari proses carving yang telah dilakukan.

2.9.2 Scalpel

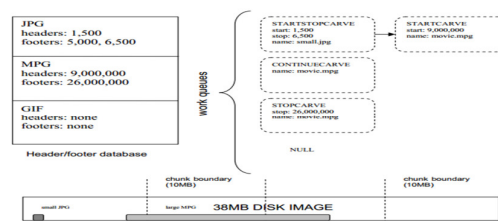
Menurut Merola (2008:23) scalpel adalah penulisan ulang lengkap dari foremost 0.69 yang dilakukan oleh Golden G. Richard III, untuk meningkatkan performa dan mengurangi penggunaan memori. Saclpel adalah file carver yang cepat dan file system independent yang membaca database definisi header dan footer dan

mengekstrak file yang cocok dari seperangkat imagefile atau file raw device.

Menurut Richard III (2005:2) scalpel adalah sebuah file carver dengan performa tinggi dengan tiga kebutuhan desain utama: 1) Frugality: file carver harus mampu berjalan pada mesin dengan sumberdaya minimal. 2) High Performance: scalpel melakukan file carving secepat mungkin tanpa mengorbankan akurasi dari operasi carving. 3) Support for distributed implementation: teknik-teknik dasar dari file carver harus siap untuk beradaptasi platform digital forensik berbasis cluster yang terdistribusi.

Berikut adalah prinsip yang digunakan oleh scalpel: 1) Waktu pencarian header dan footer harus diminimalkan. Hal ini berarti menggunakan algoritma pencarian string yang cepat untuk meminimalkan pencarian yang sia-sia. 2) Penyalinan memori ke memori harus dikurangi. File carver melakukan penyalinan jutan byte data. Meskipun operasi disk lebih lambat dari penyalinan memori, pemakaian memori yang berlebih dapat menurunkan performa. Apabila mungkin data harus ditulis langsung dari buffer yang digunakan untuk membaca disk/image. 3) Waktu penulisan harus dikurangi dengan hanya melakukan carving sesuai jumlah yang dibutuhkan investigator. Karena operasi penulisan pada disk mekanik mahal, hanya file yang cocok dengan spesifikasi pencarian yang harus ditulis. Scalpel bekerja dengan dua kali menelusuri tiap disk image secara beraturan. Telurusan yang pertama membaca keseluruhan disk image dalam potongan yang besar (dengan nilai default 10MB). Tiap potongan mencari file header yang dan sebuah database mengenai tempat header ditaruh. Setelah indeksasi header selesai, sebuah pencarian dilakukan untuk mencari footer. Untuk beberapa file yang footer nya telah didefinisikan pencarian footer dilakukan potongan yang sekarang saja jika footer berpotensi cocok dengan header yang ada dalam file. Hali ini mungkin terjadi dalam dua kondisi. Kondisi pertama apabila header yang berpotensi cocok terdapat dalam potongan yang sekarang. Kondisi yang kedua header yang berpotensi cocok terdapat di potongan sebelumnya dari image file, tetapi cukup dekat dengan potongan yang sekarang untuk memenuhi ukuran maksimal untuk tipe file yang bersangkutan. Lokasi dari tiap footer yang cocok disimpan. Setelah penelusuran yang pertama selesai, scalpel telah memiliki indeks yang lengkap dari header dan footer, yang digunakan untuk mengisi satu set pekerjaan berurut yang mengendalikan operasi carving selama penelusuran kedua. Untuk tiap file header dalam indeks, sebuah percobaan dilakukan untuk

mencocokkan header dengan footer yang sesuai. Satu pekerjaan berurut memiliki asosiasi dengan tiap potongan disk dan sebuah file yang akan dikembalikan, tiap urutan paling tidak mengandung salah satu dari tipe antrian kerja berikut: STARTCARVE: Sebuah operasi file carving yang dimulai dari potongan disk yang bersangkutan. Lokasi awal header berada dalam potongan ini. File yang di carve akan terbuka dan porsi awal dari file yang bersangkutan di tulis. STARTSTOPCARVE: Operasi file carving dimulai dan berakhir pada satu potongan disk ini. File terbuka beberapa porsi dari ukuran potongan ditulis dan file ditutup. CONTINUECARVE: Operas file carving mencakup potongan. Seluruh isi dari potongan ditulis ke file yang sedang di carve dan file tetap terbuka. STOPCARVE: Operasi file carving berhenti pada potongan ini. Sebagian porsi dari potongan ini ditulis ke file yang sedang di carve dan file ditutup.

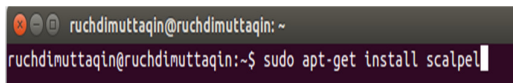


Gambar 2.4: Antrian kerja pada scalpel

Selama penelusuran kedua pada sebuah disk image, scalpel melakukan pemrosesan disk image menggunakan potongan-potongan (dengan ukuran potongan yang sama seperti pada penelusuran pertama). Seperti yang dijelaskan diatas, tiap potongan memiliki asosiasi dengan sebuah antrian kerja yang akan dijalankan ketika sebuah potongan dibaca. Penggunaan antrian kerja dicontohkan pada gambar diatas. Dimana pada contoh diatas sebuah 38MB disk image diamati, yang mengandung dua buah file. Penelusuran pertama telah membuat database header dan footer. Untuk file JPG header berada pada byte 1,500 yang berpasangan dengan footer yang berada pada byte 6,500. Untuk MPG, header berada pada byte 9,000,000 berpasangan dengan footer yang berada pada byte 26,000,000. Sebuah antrian kerja STARTSTOPCARVE disimpan pada potongan 0 dari disk image bersamaan dengan operasi lengkap dari operasi carve file JPG. Sebuah STARTCARVE ditempatkan di potongan 0 untuk antrian kerja file MPG yang akan menyebabkan carving akan dimulai dari bytes 9,000,000 selama pemrosesan dari potongan 0. CONTINUECARVE akan disimpan pada potongan 1 dan antrian kerja akan

menghasilkan penulisan seluruh potongan 1 kedalam file MPG. Akhirnya potongan 2 diproses, dan STOPCARVE akan menyalin 6MB pertama dari potongan 2 kedalam file MPG dan menutup file. Sisa dari potongan 2 akan sepenuhnya dilewati karena sudah tidak terdapat antrian kerja pada potongan tersebut. Motivasi penggunaan antrian kerja adalah untuk penggunaan maksimal dari data yang dibaca dari setiap potongan. Tidak ada aksi salin memori ke memori dilakukan. Flowchart dan pseudo code dari scalpel penulis lampirkan dalam skripsi ini.

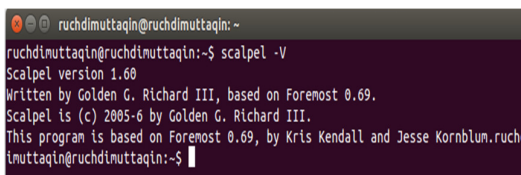
Scalpel berjalan di sistem operasi linux, untuk proses instalasi scalpel khususnya di ubuntu dapat dilakukan dengan memasukan perintah “sudo apt-get install scalpel” pada terminal.



```
ruchdimuttaqin@ruchdimuttaqin:~$ sudo apt-get install scalpel
```

Gambar 2.5: Perintah install scalpel

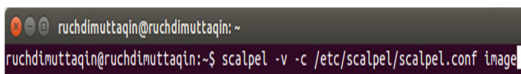
Setelah proses instalasi selesai maka secara otomatis scalpel sudah dapat digunakan dan untuk memastikan scalpel telah terinstall dapat memasukan perintah “scalpel -V” pada terminal.



```
ruchdimuttaqin@ruchdimuttaqin:~$ scalpel -V
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Scalpel is (c) 2005-6 by Golden G. Richard III.
This program is based on Foremost 0.69, by Kris Kendall and Jesse Kornblum.
ruchdimuttaqin@ruchdimuttaqin:~$
```

Gambar 2.6: Pengecekan instalasi scalpel

Scalpel merupakan aplikasi tanpa GUI dan dijalankan pada terminal. Untuk melihat perintah apa saja yang dapat digunakan dapat memasukan perintah “man scalpel” pada terminal. Pada scalpel terdapat banyak mode *carving* yang dapat kita pilih. Secara default kita dapat menjalankan proses *carving* dengan menggunakan perintah “scalpel -v -c /etc/scalpel/scalpel.conf image”.



```
ruchdimuttaqin@ruchdimuttaqin:~$ scalpel -v -c /etc/scalpel/scalpel.conf image
```

Gambar 2.7: Perintah menjalankan scalpel

Perintah tersebut akan menjalankan scalpel dengan mode *verbose* [v] dengan menggunakan file konfigurasi yang terdapat pada *path* /etc/scalpel/scalpel.conf [c] dan akan melakukan pemeriksaan terhadap file image. Setelah proses carving selesai akan muncul folder baru yang dengan isi file yang berhasil dikembalikan oleh scalpel dan sebuah file teks yang berisikan audit dari proses carving yang telah dijalankan.

2.10 Alat Carving Yang Baik

Menurut Laurenson (2013:1), file carving merupakan teknik yang sangat kuat karena file komputer dapat dikembalikan dari raw data tanpa memperdulikan file system yang digunakan, dan pengembalian file mungkin untuk dilakukan walau metadata yang ada telah sepenuhnya dirusak. Alat carving dapat dinilai baik dengan melihat dari: 1.

Kecepatan proses merupakan hal yang penting karena ketika melakukan pengembalian file terhadap barang bukti dengan memori penyimpanan yang sangat besar. Apabila kecepatan proses alat carving lambat maka akan mengakibatkan pengumpulan informasi dari file yang kembali juga menjadi lama. 2. Jumlah file yang kembali dan Jumlah file yang kembali dari alat carving dianggap penting karena ketika banyak file yang kembali maka semakin banyak juga informasi yang dapat ditemukan. 3. Kehandalan file yang kembali. Ketika jumlah file yang kembali banyak tetapi tidak disertai dengan kehandalan file, maka file-file tersebut hanya akan membuat sulit investigator digital karena banyaknay file kembali yang diperiksa tidak dapat memberikan informasi sebanyak file kembalian yang handal (file dengan isi yang sama pada saat sebelum dihapus/valid)

2.11 Integritas File

Integritas file dalam suatu pengembalian file adalah hal yang penting. Hal ini dianggap penting karena pada file yang kembali dari hasil carving tidak secara pasti merupakan file yang sama persis seperti file yang sebelumnya dihapus (tidak valid). Untuk memastikan integritas dari suatu file dapat menggunakan fungsi hash yang merupakan salah satu bagian dari ilmu kriptografi

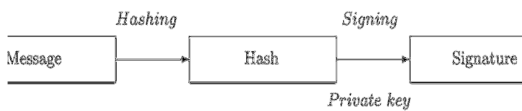
2.11.1 Kriptografi

Kriptografi menurut Solanki (2012:1), adalah sebuah cabang dari ilmu komputer yang berhubungan dengan keamanan. Kriptografi mendukung operasi seperti enkripsi dan dekripsi. Kriptografi diimplementasikan dalam bentuk fungsi hash, algoritma kunci simetris, algoritma kunci publik. Kriptografi menurut Ko’scielny et all (2013:1), adalah ilmu merubah, atau melakukan encoding informasi menjadi sebuah bentuk yang tidak dipahami oleh siapapun yang tidak tahu kunci yang tepat. Dalam bentuk yang demikian informasi dapat dikirim dengan aman melalui saluran komunikasi atau disimpan dalam arsip data dengan akses terbatas atau bahkan dilarang.

2.11.1.1 Fungsi Hash

Algoritma fungsi hash menurut Ko’scielny et all (2013:132), memproduksi nilai hash (yang

dikenal sebagai digests atau fingerprint) dari pesan. Secara umum, nilai hash digunakan untuk mendeteksi apakah pesan atau file telah mengalami perubahan sejak nilai hash dibuat.



Gambar 2.8: Proses hashing

Algoritma hash menurut Solanki (2012:1), umumnya disebut sebagai algoritma message digest, adalah sebuah algoritma yang menghasilkan bit vektor dengan ukuran tetap dari pesan M dengan ukuran yang berubah-ubah. Bit vektor disebut sebagai hash dari pesan. Hash memiliki banyak metode dalam penggunaannya. Yang populer digunakan antara lain adalah MD5 dan SHA-1. Pada metode MD5 telah ditemukan bug yang menyebabkan metode MD5 menjadi tidak aman. Sedangkan untuk SHA-1 untuk saat ini masih dianggap aman dan dapat digunakan untuk memeriksa integritas dari suatu file.

2.11.1.1.1 SHA-1

SHA-1 menurut Schmitt dan Jordaen (2013:1), merupakan praktek standar dalam forensik digital yang digunakan untuk pemeliharaan barang bukti dan menjamin integritas dari barang bukti digital.

SHA-1 menurut Kościelny et al (2013:140), algoritma yang mirip dengan MD5, didesain oleh NIST dalam kerjasama dengan NSA dan di terbitkan sebagai standar federal FIPS FUB 180 pada tahun 1993. Singkatan dari SHA adalah Secure Hash Algorithm. Masukannya adalah pesan dengan ukuran apa saja kurang dari 18446744073709551616 bits, dan keluarannya adalah nilai hash dengan ukuran 160-bit.

2.12 GNU ddrescue

GNU ddrescue ialah alat untuk pengembalian data. GNU ddrescue menyalin data dari satu file atau block dari perangkat (harddisk, disc, cdrom dll) ke tempat lain, berusaha untuk menyelamatkan data ketika terjadi kesalahan membaca. GNU ddrescue terdapat di sistem operasi linux. Untuk dapat menggunakan ddrescue penulis terlebih dahulu melakukan instalasi, berikut adalah cara yang penulis lakukan untuk melakukan instalasi gnu ddrescue:

1. Membuka terminal kemudian memasukan perintah “sudo apt-get install gddrescue”

```

uchdimuttaqin: ~
uchdimuttaqin:~$ sudo apt-get install gddrescue
  
```

Gambar 2.9: Perintah install GNU ddrescue

2. Setelah perintah selesai dijalankan maka GNU ddrescue sudah dapat digunakan. Untuk mengetahui penggunaan gnu ddrescue lebih lanjut dapat memasukan perintah “ddrescue -h” pada terminal.

```

uchdimuttaqin@uchdimuttaqin:~$ ddrescue -h
GNU ddrescue - Data recovery tool.
Copies data from one file or block device to another,
trying hard to rescue data in case of read errors.

Usage: ddrescue [options] infile outfile [logfile]
You should use a logfile unless you know what you are doing.
If you reboot, check the device names before restarting ddrescue.
Do not use options '-F' or '-g' without reading the manual first.

Options:
-h, --help                display this help and exit
-V, --version             output version information and exit
-s, --min-read-rate=<bytes> minimum read rate of good areas in bytes/s
-A, --try-again           mark non-split, non-trimmed blocks as non-tried
-b, --sector-size=<bytes> sector size of input device [default 512]
-B, --binary-prefixes    show binary multipliers in numbers [SI]
-c, --cluster-size=<sectors> sectors to copy at a time [128]
-C, --complete-only      do not read new data beyond logfile limits
-d, --direct              use direct disc access for input file
-D, --synchronous        use synchronous writes for output file
-e, --max-errors=[+]<n> maximum number of [new] error areas allowed
  
```

Gambar 2.10: Perintah help gnu ddrescue

2.13 Masalah Yang Ditemui Pada Pengembalian File

Pada pengembalian file, media penyimpanan yang akan dilakukan investigasi sangatlah beragam, mulai dari yang memiliki memori penyimpanan kecil (misal flashdisk) sampai yang memiliki memori penyimpanan sangat besar (misal harddisk eksternal dengan ukuran 1 TB keatas). Pada pengembalian file media penyimpanan yang memiliki ukuran sangat besar akan mengakibatkan proses pengembalian file menjadi lebih lama dibanding dengan media penyimpanan yang memiliki ukuran lebih kecil. Hal ini menjadi masalah ketika dalam suatu percobaan pengembalian file media penyimpanan yang akan di investigasi memiliki memori penyimpanan yang besar dan proses pengembalian file harus dilakukan dalam waktu yang singkat tanpa mengurangi kehandalan file yang berhasil dikembalikan.

III. METODE PENELITIAN

3.1. Jenis Penelitian

Jenis penelitian dari penulisan ini adalah penelitian simulasi dimana penulis membuat model simulasi yang kemudian dijalankan untuk dianalisa hasil dari tiap model simulasi yang dijalankan.

3.2. Tempat dan Waktu Penelitian

Penelitian ini dilakukan di UIN Jakarta , Ciputat, dengan waktu penelitian dari Juli sampai Desember 2014.

3.3. Subjek Penelitian

Subjek dari penelitian ini adalah performa dari carving tools foremost dan scalpel.

3.4. Teknik dan Alat Pengumpulan Data

Penulis melakukan penelitian dengan menggunakan metode simulasi menurut chaset et all yang terdiri dari 6 langkah yaitu: 1. Mendefinisikan Masalah, 2. Membangun Model Simulasi, 3. Membuat Spesifikasi Nilai Dari Variable dan Parameter, 4. Mengevaluasi Hasil, 5. Melakukan Validasi, 6. Membuat Proposal Penelitian Baru.

IV. PEMBAHASAN

4.1 Mendefinisikan Masalah

Pada tahap mendefinisikan masalah, penulis mendefinisikan masalah sesuai dengan rumus masalah yang telah ditentukan pada bab 1 di sub bab rumusan masalah dan menentukan variabel sistem yang dapat dan tidak dapat dikendalikan, yaitu: i. Manakah yang lebih cepat durasi proses pengembalian file antara Foremost dan Scalpel? ii. Manakah yang mampu lebih banyak mengembalikan file yang telah hilang antara Foremost dan Scalpel? iii. Bagaimanakah validitas file yang dikembalikan menggunakan foremost dan scalpel? Variable sistem yang dapat dikendalikan adalah sebagai berikut: i. Sistem operasi yang digunakan Pada penelitian ini penulis menggunakan sistem operasi ubuntu 14.04 ii. Ukuran media penyimpanan yang digunakan Ukuran media penyimpanan yang penulis gunakan adalah 8GB iii. Spesifikasi komputer yang digunakan Spesifikasi komputer yang penulis gunakan adalah komputer dengan prosesor intel core i3, dan memori ram 6GB Variable sistem yang tidak dapat dikendalikan adalah sebagai berikut: i. Lokasi block tempat file disimpan dalam flashdisk

4.2 Membangun Model Simulasi

Pada tahap membangun model simulasi, penulis menentukan parameter dan variable berdasarkan definisi masalah yang telah ditentukan pada tahap sebelumnya, berikut adalah model simulasi yang penulis buat: i. Parameter a. Durasi proses carving Durasi proses carving penulis tentukan menjadi parameter karena pada penelitian ini durasi proses carving dari foremost dan scalpel adalah hal yang hendak diperbaiki (semakin cepat semakin baik) dan akan berubah-ubah sesuai dengan mode carving yang digunakan. Pada penelitian ini penulis akan melakukan simulasi untuk mengetahui durasi proses carving file avi, jpg, wav, dan semua file yang ditentukan di

batasan masalah penelitian ini. b. Jumlah file yang kembali Jumlah file penulis tentukan sebagai parameter karena jumlah file yang kembali merupakan aspek penting yang hendak diperbaiki dan akan mengalami perubahan nilai sesuai dengan mode carving yang digunakan. c. Validitas file yang kembali Validitas file penulis tentukan sebagai parameter karena termasuk hal yang penting dan hendak diperbaiki dan akan mengalami perubahan nilai sesuai dengan mode carving yang digunakan. ii. Variable Pada penelitian ini penulis menentukan mode carving dan daftar file sebagai variable dari model simulasi yang penulis buat. Karena mode carving pada penelitian ini akan mempengaruhi nilai yang akan dihasilkan oleh parameter yang telah penulis tentukan.

Adapun mode carving yang akan penulis jalankan adalah sebagai berikut:

1. Hanya akan mengembalikan file avi a) Foremost: foremost -v -T -i image -t avi b) Scalpel: scalpel -v -c /etc/scalpel/scalpel.conf image (file konfigurasi pada scalpel diubah sehingga hanya akan mencari file avi)
2. Hanya mengembalikan file jpg a) Foremost: foremost -v -T -i image -t jpg b) Scalpel: scalpel -v -c /etc/scalpel/scalpel.conf image (file konfigurasi pada scalpel diubah sehingga hanya akan mencari file jpg)
3. Hanya akan mengembalikan file wav a) Foremost: foremost -v -T -i image -t wav b) Scalpel: scalpel -v -c /etc/scalpel/scalpel.conf image (file konfigurasi pada scalpel diubah sehingga hanya akan mencari file wav)
4. Mengembalikan semua file yang ditentukan di subab batasan masalah a) Foremost: foremost -v -T -i image b) Scalpel: scalpel -v -c /etc/scalpel/scalpel.conf image (file konfigurasi pada scalpel diubah sehingga akan mencari semua file yang terdapat pada batasan masalah)

4.3 Membuat Spesifikasi Nilai Dari Variable dan Parameter

Karena keterbatasan yang penulis miliki, maka tiap tipe file penulis hanya menyiapkan 3 buah file dan dengan ukuran file yang penulis tentukan secara acak. Namun demikian penghitungan terhadap prosentase file kembali yang valid tetap bisa dilakukan.

4.4 Mengevaluasi Hasil

Berikut adalah hasil evaluasi yang penulis lakukan:

Tabel 4.1: Hasil Evaluasi Foremost Scalpel

No.	Tipe File	Mode Pencarian	Durasi
1	avi	foremost -v -T -i image -t avi	00:01:27
2	wav	foremost -v -T -i image -t wav	00:01:27
3	wav	scalpel -v -c /etc/scalpel/scalpe l.conf image	00:01:29
4	jpg	foremost -v -T -i image -t jpg	00:01:30
5	avi	scalpel -v -c /etc/scalpel/scalpe l.conf image	00:01:36
6	jpg	scalpel -v -c /etc/scalpel/scalpe l.conf image	00:01:57
7	jpg, gif, bmp, png, avi, exe, mpg, wav, wmv, mov, pdf, ppt, xls, doc, zip, rar, htm, cpp	foremost -v -T -i image -t jpg	00:07:20
8	jpg, gif, bmp, png, avi, exe, mpg, wav, wmv, mov, pdf, ppt, xls, doc, zip, rar, htm, cpp	scalpel -v -c /etc/scalpel/scalpe l.conf image	00:20:21

4.5 Melakukan Validasi

Berikut adalah hasil validasi yang penulis lakukan:

Tabel 4.2: Validasi Hasil

No	Tipe File	Validitas		File Kembalian		Waktu	
		Foremost	Scalpel	Foremost	Scalpel	Fore- most	Scal- pel
1	Avi	0%	0%	2	2		
2	bmp	66.66%	0%	2	1		
3	cpp	0%	0%	0	0		
4	docx	0%	0%	1	12		
5	exe	0%	0%	3	0		
6	gif	0%	0%	6	6		
7	htm	0%	0%	3	3		
8	jpg	100%	0%	10	7		
9	mov	0%	0%	0	8		
10	mpg	33.33%	0%	2	1013		
11	ole (xls, ppt)	0%	0%	6	0		
12	pdf	100%	33.33%	3	2		
13	png	66.66%	0%	41	32		
14	rar	100%	0%	3	0		
15	wav	0%	0%	3	3		
16	wmv	100%	0%	4	0		
17	zip	0%	0%	6	155		
Total		566.65%	33.33%	95	1244	00:0 7:20	00:2 0:21
Rata-rata		33.33%	1,961%				

Setelah melakukan perbandingan validasi, penulis melakukan pemeriksaan terhadap file yang kembali secara acak dan penulis menemukan beberapa file yang tampak baik-baik saja tetapi file tersebut tidak valid karena nilai hash yang dimiliki tidak sama dengan nilai hash sebelum file dihapus.

4.6 Membuat Proposal Penelitian Baru

Untuk lebih memahami lebih lanjut tingkah laku dari foremost dan scalpel, penulis mengusulkan penelitian baru dengan merubah variable pencarian default menjadi pencarian dengan mode yang lain (seperti mode pencarian cepat) sehingga parameter dari simulasi yang dilakukan dapat diteliti lebih lanjut.

V. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil metode simulasi tahap evaluasi dan validitas diperoleh kesimpulan bahwa carving tool foremost memiliki kemampuan carving yang lebih baik dibanding dengan scalpel yaitu durasi lebih cepat, tingkat validitas file yang dikembalikan lebih tinggi, dan jumlah file rusak yang kembali relatif lebih sedikit

5.2. Saran

Berikut adalah saran untuk penelitian sejenis berikutnya: 1. Melakukan carving dengan mode yang lain (yang tersedia) untuk lebih memahami lebih lanjut tingkah laku dari foremost dan scalpel. 2. Data yang didapat dari hasil penelitian dapat ditampilkan dalam format yang lebih menarik seperti dalam bentuk grafik.

DAFTAR PUSTAKA

- [1] Al-Azhar, Muhammad Nuh. 2012. Digital Forensic: Panduan Praktis Investigasi Komputer. Jakarta: Penerbit Salemba Infotek.
- [2] Beek, Christiaan. 2011. Introduction To File Carving
- [3] Chase et all. 2006. A New Monte Carlo Simulation Method for Tolerance Analysis of Kinematically Constrained Assemblies
- [4] EC-Council. 2010. Computer Forensics Investigating Hard Disk, File & Operating System
- [5] Ko'ścielny, Czesław et all. 2013. Modern Cryptography Primer: Theoretical Foundations and Practical Applications. Springer.
- [6] Laursen, Thomas. 2013. Performance Analysis Of File Carving Tools

- [7] Madani, Sajjad.A. 2010. Wireless Sensor Networks: Modelling and Simulation
- [8] Merola, Antonio. 2008. Data Carving Concepts
- [9] Mikus, Nicholas. 2005. AN ANALYSIS OF DISC CARVING TECHNIQUES.
- [10] Nadeem Ashraf, Muhammad. 2012. Forensic Multimedia File Carving
- [11] NIST. Forensic File Carving Tool Specification. 2014.
- [12] Pal, Anandabrata dan Memon, Nasir. 2009. The Evolution Of File Carving
- [13] Richard III, Golden G. 2005. Scalpel:A Frugal, High Performance File Carver
- [14] Schmitt, Veronica dan Jordaan, Jason. Establishing the Validity of Md5 and Sha-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms. 2013
- [15] Solanki, Yogendra Singh. Performance Based Design and Implementation of a SHA-1 Hash Module on FPGA. 2012.