FORENSIK SISTEM *FILE EXT4* STUDI KASUS *FILE* DI SISTEM OPERASI *LINUX*

Resi Utami Putri

Jurusan Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Jalan Kaliurang Km.14,5 Sleman, Yogyakarta 55184
Email : resiutami@uii.ac.id

ABSTRACT

Research discusses one of the files system in the operating Linux system, which Ext4 (Extended Fourth) which is a continuation of the Ext2 and Ext3. The method used in this study is the forensic investigation is to collect, maintain, and analyze. This study was conducted with a simulation file. Results from this study is a file can be known when the file is created to be modified. This study also uses some Linux default tool nor a forensic tool.

Keywords : File System, Linux, Ext4, Forensic.

1. PENDAHULUAN

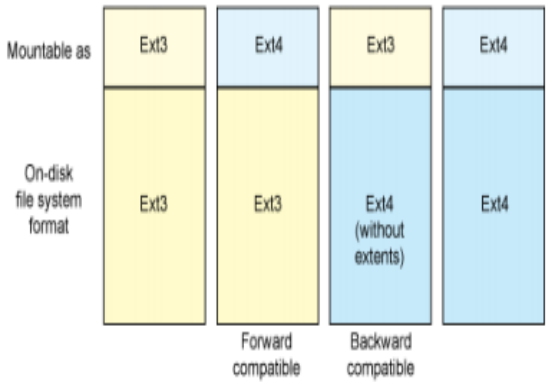
Forensik digital merupakan ilmu yang mempelajari dan menelusuri tentang jejak dalam peralatan elektronik yang akan digunakan sebagai barang bukti di pengadilan. Forensik digital dibagi menjadi beberapa bagian yaitu forensik komputer, forensik *mobile* dan sebagainya. Sedangkan, forensik sistem *file* bisa termasuk keduanya. Focus pada penelitian ini adalah pada sistem file yang paling baru yaitu *Ext4*.

Sistem *file Ext4* mulai muncul pada tahun 2008 dan mulai bisa digunakan pada versi kernel ke 2.6.28. pada saat ini belum banyak penelitian sejenis yang membahas sistem *file Ext4* ini. Sehingga penulis berkeinginan membahas sistem *file* tersebut.

Metode yang digunakan dalam penelitian ini adalah investigasi forensik. Pada investigasi forensik terdapat beberapa tahapan yaitu mengumpulkan, mempertahankan, dan menganalisis. Dalam hal ini sebagai bahan dari penelitian adalah *file* yang dibuat di sistem operasi *linux Ubuntu* pada sistem *file Ext4*. Sebagain batasan dalam penelitian ini adalah peneliti hanya melakukan simulasi terhadap suatu *file txt* dan *jpeg*.

1.1. Tinjauan Teoritis

Sistem *file* pada *Linux* dasar menggunakan *Ext2* hingga digantikan oleh *Ext3*. Setelah *Ext3* lalu muncul kembali yang paling baru yaitu *Ext4* seperti terlihat pada gambar 1. Sedangkan beberapa perbedaan dari masing-masing sistem *file* bisa dilihat pada gambar 2 menurut cao, 2007.

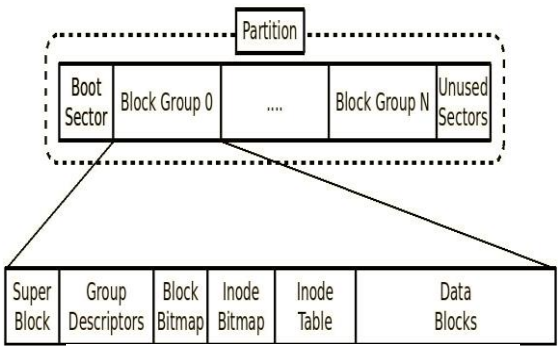


Gambar 1. Sistem *File Extended* (Jones, 2009).

Ext4 memiliki 48 alamat blok. Dimana pada blok pertama disebut dengan super blok. Di dalam *superblock* terdapat metadata yang berisi tentang partisi, lihat gambar 3.

	ext3	ext4dev
filesystem limit	16TB	1EB
file limit	2TB	16TB
limit	2**32	2**32
default inode size	128 bytes	256 bytes
block mapping	indirect block map	extents
time stamp	second	nanosecond
sub dir limit	2**16	unlimited
EA limit	4K	>4K
preallocation	in-core reservation	for extent file
deframentation	No	yes
directory indexing	disabled	enabled
delayed allocation	No	yes
multiple block allocation	basic	advanced

Gambar 2. Perbedaan *Ext3* dan *Ext4* (cao, 2007).



Gambar 3. Sistem *File* (wei, 2010).

1.2. Penelitian Terkait

Sistem operasi *Linux* yang bersifat *open source*, memiliki beberapa *file system* yaitu *extended*, yaitu *ext2*, *ext3*, dan *ext4*. *Extended 4* (*Ext4*) merupakan generasi terbaru yang muncul pada tahun 2008. Ada beberapa penelitian yang membahas sistem *file* tersebut dimulai dari tahun awal kemunculan sistem *file Ext4* hingga sekarang.

Dimulai dari penelitian tentang sistem *file* metadata pada forensik digital oleh Buchholz (2004) membahas mengenai informasi yang dibutuhkan oleh investigator forensik dalam penanganan sistem file.

Lou (2009) meneliti tentang *recovery file* pada *event log*, yang merupakan *file* yang menyimpan beberapa informasi pada sistem operasi *windows*. Lou dkk menggunakan metode konten dan struktur internal *event log*.

Penelitian lain membahas *file system Ext2* (wei, 2010) membahas *file system* dasar yaitu *Ext2* dengan menggunakan metode berorientasi obyek yang bertujuan untuk mendesain *parsing platform*. Wei melakukan *parsing file* data biner pada *disk* untuk dikonversi ke antarmuka yang mudah dibaca sehingga memudahkan untuk membangun alat forensik komputer.

Aronson (2011) meneliti tentang *file carving* yang merupakan proses untuk me *recovery file* dengan teknik validasi format dan rekonstruksi *file*. Aronson dkk secara khusus membahas *file* format bertipe *GIF*.

Penelitian pada *file system Ext4* pada sistem operasi android 2.3, *Gingerbread* dilakukan oleh kim, dkk (2012) dengan berdasarkan jurnal log. Kim, dkk mengembangkan alat *JDForensic* yang bisa mengekstrak jurnal log untuk menganalisis dan mengembalikan data yang dihapus.

Analisis *Ext4* untuk forensik digital juga diteliti oleh Fairbanks (2012) yang membahas struktur data *Ext4* seperti *extend*. *Fairbanks* juga mendiskusikan sistem *file superblock*, blok grup *layout* dan pemetaan data *inode*. Penelitiannya menggunakan *tool debugfs* dan *e2fsprogs*.

Penelitian mengenai *recovery* data pada *virtual machine* dilakukan oleh Healey (2013) yang membahas dari sisi investigator forensik. Healey dkk merekomendasikan untuk menggunakan *Huffman Code Tables* untuk membangun *header* data dalam *fragment file*.

2. PEMBAHASAN

Penelitian dilakukan pada *Ubuntu 14.04* dengan versi kernel 3.13.0 (lihat gambar 4) dengan sistem *file Ext4*. *Ext4* pada umumnya berjalan pada kernel 2.6.28. Dikarenakan sistem *file extended* mempunyai ruang penyimpanan yang paling besar atau tak terbatas dari sistem *file* yang sebelumnya.

```
root@ubuntu:~# uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:08:14 UTC 2014 i686
i686 i686 GNU/Linux
```

Gambar 4. Versi Kernel *Linux*.

Setelah melacak kernel yang digunakan lalu melihat sistem *file* yang digunakan, seperti terlihat pada gambar 5.

```
root@ubuntu:/home/resi/Documents# cd
root@ubuntu:~# parted /dev/sda 'print'
Model: VMware, VMware Virtual S (scsi)
Disk /dev/sda: 107GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start   End    Size    Type      File system     Flags
 1      1049kB  105GB  105GB   primary   ext4            boot
 2      105GB   107GB  2144MB  extended
 5      105GB   107GB  2144MB  logical   linux-swap(v1)

root@ubuntu:~#  mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/cgroup type tmpfs (rw)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
none on /run/user type tmpfs (rw,noexec,nosuid,nodev,size=104857600,mode=0755)
none on /sys/fs/pstore type pstore (rw)
systemd on /sys/fs/cgroup/systemd type cgroup (rw,noexec,nosuid,nodev,none,name=
systemd)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,user=res
i)
gvfsd-fuse on /root/.gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev)
```

Gambar 5. Cek Sistem *File Ext4*.

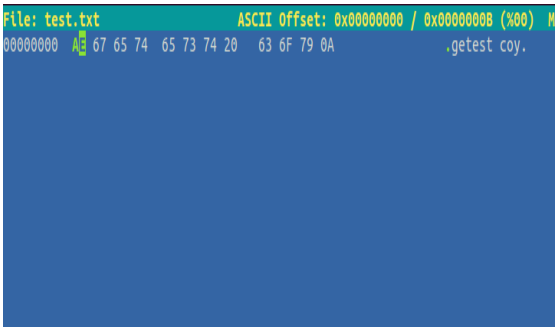
Dalam simulasi *file* menggunakan dua *file* yaitu *file text* dan *jpeg*. Berikut adalah hasil statistik dari masing - masing *file*, bisa dilihat pada gambar 6 dan gambar 7.

Pada masing - masing gambar terdapat *MAC time*, merupakan singkatan dari M (*modified*), A (*access*) dan C (*create*). M menunjukkan kapan sebuah *file* di modifikasi. A menunjukkan kapan saja sebuah *file* di akses. C menunjukkan kapan sebuah *file* dibuat.

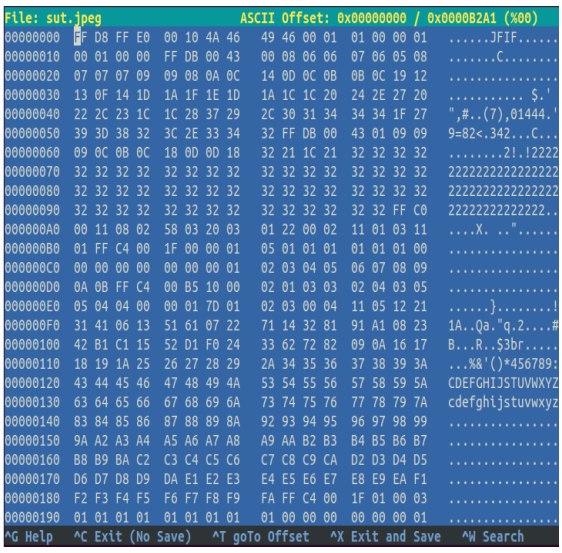
```
root@ubuntu:~# cd /home/resi/Documents/
root@ubuntu:/home/resi/Documents# ls
sut.jpeg  test  test.txt  ways  ways~
root@ubuntu:/home/resi/Documents# stat test.txt
  File: 'test.txt'
  Size: 12              Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 2359520     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2015-06-02 21:23:55.120417463 -0700
Modify: 2015-05-28 15:10:57.624519154 -0700
Change: 2015-05-28 15:10:57.624519154 -0700
 Birth: -
root@ubuntu:/home/resi/Documents# stat sut.jpeg
  File: 'sut.jpeg'
  Size: 45730           Blocks: 96         IO Block: 4096   regular file
Device: 801h/2049d      Inode: 2359981     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/    resi)   Gid: ( 1000/    resi)
Access: 2015-06-02 20:07:24.806068495 -0700
Modify: 2015-06-02 19:53:16.726069684 -0700
Change: 2015-06-02 19:53:16.726069684 -0700
 Birth: -
```

Gambar 6. Simulasi *File Text* dan *Jpeg*.

Selanjutnya setelah melihat statistik dari setiap *file*, bisa melihat isi dari *file* tersebut. *File* tersebut dilihat dalam bilangan *hexa* dengan menggunakan *tool hexaeditor*. Bisa dilihat pada gambar 7 dan gambar 8.



Gambar 7. *Hexeditor File Test.Txt.*



Gambar 8. *Hexeditor File Sut.Jpeg.*

3. KESIMPULAN

Dari hasil pengamatan *file text* dan *jpeg*, penelitian ini dilakukan baru sebatas pengamatan awal terhadap suatu *file*. Pada masing - masing *file* juga bisa dilihat *MAC time*-nya juga isi *file* tersebut dalam bentuk *hexa* desimal. Untuk penelitiannya lebih lanjut akan dilakukan investigasi secara mendalam terhadap suatu *file*.

DAFTAR PUSTAKA

Aronson, L., Bos, J.V.D. Towards an Engineering Approach to File Carver Construction. *35th Annual Computer Software and Applications Conference Workshops*. IEEE, 2011.

Buchholz, F., Spafford, E. On The Role of File System Metadata in Digital Forensics. Digital Investigation hal. 298-309. Elsevier Ltd, 2004.

Cao, M., Bhattacharya, S., Tso, T. *Ext4: The Next Generation of Ext2/3 Filesystem*. IBM Corporation, 2007.

Fairbanks, K.D. *An Analysis of Ext4 for Digital Forensics*. Digital Investigation. Elsevier Ltd, 2012.

Healey, N.J., Angelopoulou, O., Evans, D. A discussion on the Recovery of Data from a Virtual Machine. *Fourth International Conference on Emerging Intelligent Data and Web Technologies*. IEEE, 2013.

Jones. *Anatomy of Ext4, Get to know the fourth extended file system*. IBM Corporation, 2009.

Kim, D., Park, J., Lee, K.G., Lee, S. *Forensic Analysis of Android Phone Using Ext4 File System Journal Log*. Science+Business Media Dort. Springer, 2012.

Lou, Y., Wang, P., Xu, M., Zheng, N. Automated Event Log File Recovery based on Content Characters and Internal Structure. *The 1st International Conference on Information Science and Engineering* (ICISE2009). IEEE, 2009.

Wei, C., Mei, L.C. The Analysis and Design of Linux System Based on Computer Forensic. *International Conference on Computer Design and Application (ICCDA 2010)*. Volume 2. IEEE, 2010.