ANALISA FORENSIK PEMALSUAN TIMESTAMP PADA NEW TECHNOLOGY FILE SYSTEM (NTFS)

TUGAS AKHIR

OLEH :

Rizky Soufi Gustiawan

09011281520111

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

ANALISA FORENSIK PEMALSUAN *TIMESTAMP* PADA *NEW TECHNOLOGY FILE SYSTEM* (NTFS)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

Rizky Soufi Gustiawan

09011281520111

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

LEMBAR PENGESAHAN

ANALISA FORENSIK PEMALSUAN *TIMESTAMP* PADA *NEW TECHNOLOGY FILE SYSTEM* (NTFS)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

RIZKY SOUFI GUSTIAWAN
09011281520111

Palembang, Juli 2020

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP 196612032006041001	**NIP 197806172006041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 23 Juli 2020

Tim Penguji :

1. **Ketua : Aditya Putra P Prasetyo,S.Kom., MT**
2. **Sekretaris : Deris Stiawan, M.T., Ph.D.**
3. **Anggota I : Ahmad Heryanto, M.T.**
4. **Anggota II : Rahmat Fadli Isnanto, M.Sc**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERYATAAN

Yang bertanda tangan dibawah ini:

Nama	: Rizky Soufi Gustiawan
NIM	: 09011281520111
Program Studi	: Sistem Komputer
Judul	: Analisa Forensik Pemalsuan *Timestamp* pada *New Technology File System* (NTFS)

Menyatakan bahwa laporan Tugas Akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plaiat dalam laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, Juli 2020

Rizky Soufi Gustiawan

HALAMAN PERSEMBAHAN

“Do not make it a burden but make it a spirit,
towards infinity and to exceed it”

Tugas akhir ini saya persembahkan untuk :

- ***Kedua Orang tua dan Adik – adik saya***
- ***Dosen Pembimbing dan Penguji***
- ***Sahabat – sahabat saya***
- ***Teman Seperjuangan Sistem Komputer 2015***
- ***Almamaterku***

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarokatuh

Puji dan syukur penulis haturkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan Proposal tugas akhir ini dengan judul **"Analisa Forensik Pemalsuan *Timestamp* pada *New Technology File System* (NTFS).** Shalawat dan salam tak lupa kita junjungkan kepada Nabi kita Rasulullah SAW beserta keluarga, sahabat dan para pengikutnya hingga akhir zaman.

Pada penyusunan proposal ini, penulis menyampaikan ucapan terima kasih kepada semua pihak yang telah memberikan segala kemudahan, bimbingan, pengarahan, dorongan, bantuan, ide dan saran baik moril maupun materil selama penyusunan Proposal tugas akhir ini. Untuk itu penulis mengucapkan banyak terimakasih kepada :

1. Allah SWT yang telah memberikan kesehatan kepada penulis sehingga penulis dapat menyelesaikan Proposal tugas akhir ini dengan tepat waktu.
2. Kedua orang tua serta keluarga yang telah memberikan dukungan dan doa untuk kelancaran pengerjaan Proposal tugas akhir ini.
3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Dosen Pembimbing Akademik Bapak Ahmad Heryanto,S.Kom., M.T.
6. Bapak Deris Stiawan, M.T., Ph.D. selaku pembimbing tugas akhir di jurusan Sistem Komputer.
7. Seluruh teman-teman angkatan 2015 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Tim Tugas Akhir (Apri dan Juan) yang senantiasa menemani dan memberi masukan.
9. Team Basecamp Komunitas dan Nenda yang telah menjadi wadah tempat curhat dan bercerita.

10. Teman Sohib Kii Maks (Abil, Toby, Agus, Edo) yang menjadi teman bemain dan berkumpul.
11. Azwar dan Endi selaku teman tempat bertanya masalah berkas dan materi yang telah membantu selama ini.
12. Teman – teman SK(c)ang ku yang tercinta selaku teman seperjuangan angkatan 2015.

Penulis menyadari bahwa masih banyak kekurangan dalam laporan ini dan masih jauh dari kesempurnaan. Mengingat kurangnya pengetahuan dan pengalaman penulis. Untuk itu segala kritik dan saran, sangatlah penting bagi penulis.

Semoga proposal tugas akhir ini bisa bermanfaat bagi pembaca ataupun bagi penulis sendiri. Demikian yang bisa penulis sampaikan.
Wassalamu'alaikum Wr. Wb.

Palembang, Juli 2020

Penulis

Rizky Soufi Gustiawan

ANALISA FORENSIK PEMALSUAN *TIMESTAMP* PADA *NEW TECHNOLOGY FILE SYSTEM* (NTFS)

Rizky Soufi Gustiawan (09011281520111)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : rsoufi70@gmail.com

ABSTRAK

Forensik digital adalah bagian dari ilmu forensik yang mencakup penemuan dan penyelidikan data pada perangkat digital yang bertujuan untuk membuktikan kejahatan komputer secara ilmiah supaya bisa memperoleh barang bukti digital yang bisa dipakai untuk menangkap dan menemukan pelaku cyber crime. Penelitian dilakukan bertujuan untuk penyelidikan dan menganalisa pemalsuan timestamp pada file dengan ekstensi .PDF. Timestamp adalah detail waktu suatu file berupa Modify, Access, dan Change / Create yang ada pada file system, peneliti melakukan pengujian pada timestamp modify. Pengecekan timestamp dilakukan dengan cara melakukan perintah command get lastmodified pada command prompt Windows dan mengakses metadata pada file untuk mengetahui informasi yang terdapat pada metadata. Selanjutnya timestamp yang diperoleh dibandingkan untuk di analisa keduanya apakah mempunyai timestamp yang sama atau tidak. Algoritma String Matching digunakan untuk membandingkan timestamp hasil pada command stat dan informasi metadata. Hasil dari penelitian ini memperlihatkan bahwa pemalsuan dapat diperoleh dengan mengetahui perbandingan antara timestamp command get lastmodified dan isi informasi metadata, jika timestamp sama bisa dipastikan timestamp asli, jika berbeda maka timestamp terbukti palsu.

Kata Kunci : Forensik Digital, Barang Bukti Digital, *Cyber Crime, Timestamp, PDF, Command Prompt Windows, Metadata, String Matching.*

TIMESTAMP FRAUD FORENSIC ANALYSIS ON NEW TECHNOLOGY FILE SYSTEM (NTFS)

Rizky Soufi Gustiawan (09011281520111)

Dept of Computer Engineering, Faculty of Computer Science,

Sriwijaya University

Email : rsoufi70@gmail.com

ABSTRACT

Digital Forensics is a part of forensic science that includes inventions and Data investigation on a digital device that aims to prove scientific computer crimes in order to obtain digital evidence that can be used to capture and find cyber crime actors. Research is aimed at investigating and analyzing timestamp fraud on files with extensions. Pdf. Timestamp is the time detail of a file in the form of Modify, Access, and Change/Create files in the file system, researchers perform tests on timestamp Modify. A timestamp check is done by performing the command get lastmodified command at the Windows command prompt and accessing the metadata on the file to find out the information contained in the metadata. Furthermore the timestamp obtained compared to the analysis both whether to have the same timestamp or not. The String Matching algorithm is used to compare the result timestamp in the stat command and metadata information. The result of this study shows that counterfeiting can be obtained by knowing the comparison between get lastmodified and the timestamp of the metadata information, if the same timestamp can be ensured the original timestamp, if different then the timestamp proved false.

Keywords : Digital forensics, Digital proof item, Cyber Crime, Timestamp, PDF, Command Prompt Windows, Metadata, String Matching.

DAFTAR ISI

Halaman

BAB II TINJAUAN PUSTAKA

BAB III METODOLOGI PENELITIAN

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I. PENDAHULUAN

1.1 Latar Belakang

Forensik digital adalah bagian dari ilmu forensik yang mencakup penemuan dan penyelidikan materi (data) yang ditemukan pada perangkat digital. Sebagai ilmu yang masih baru, dibutuhkan pemahaman dan kemampuan untuk menguasai ilmu ini. Penguasaan ilmu ini tidak hanya ditujukan pada kemampuan teknis saja tetapi juga terikat dengan bidang lainnya, seperti bidang hukum [1]. Barang bukti digital merupakan informasi yang tersimpan di dalam perangkat penyimpanan perangkat elektronik dalam bentuk berkas digital yang dipakai untuk keperluan melakukan suatu kejahatan serta barang yang diperoleh dari sebuah kejahatan. Secara fisik, barang bukti digital tersimpan di dalam perangkat penyimpanan dalam bit-bit informasi yang tidak terlihat oleh mata sehingga memerlukan proses pengolahan menjadi informasi yang terlihat oleh mata [2].

Penelitian sebelumnya [3] menjelaskan metode forensik komputer untuk mendeteksi pemalsuan sistem berkas *timestamp* pada Windows NTFS pada $Log*File* untuk merubah atribut $STANDARD_INFORMATION dan $*FILE*_NAME. Ada beberapa operasi *file* pada $Log*File* yaitu membuat *file*, menghapus *file*, menambah isi *file*, memotong *file*, mengatur *file*, merubah nama *file* dan merubah hak akses *file*. Cara kerjanya yaitu dengan memalsukan atau manipulasi *timestamp* pada *file* yang dipilih menggunakan program perubah waktu setelah itu membandingkan dan menganalisa antara *file* yang sudah dipalsukan dan *file* asli. Pada pekerjaan itu [3] tidak menjelaskan bagaimana teknik dipakai dalam memalsukan *timestamp,* sehingga penulis harus menemukan sendiri teknik yang tepat dalam penelitian tersebut.

Selanjutnya [2] membahas analisa forensik komputer pada *timestamp* sistem berkas NTFS dengan memanipulasi *timestamp* pada *file* dengan ekstensi .pdf Analisa melibat kan *file* .pdf, *file* tersebut dimanipulasi *timestamp* nya dengan memakai *tools Attribute Magic Free 2.4*. *File* yang asli maupun salinan yang telah di palsukan sebelumnya di identifikasi dengan digital *hashing* menggunakan metoda MD5 dan pengambilan informasi *timestamp* menggunakan tool WMIC.

Kemudian dari hasil penelitian [2] diperoleh bahwa nilai *hash* tidak berubah karena algoritma nilai MD5 memang tidak untuk mempengaruhi perubahan string pada karakter atribut berkas.

Dalam melakukan penelitian ini penulis harus menemukan metode yang cocok dalam menemukan cara yang tepat untuk mengenali *Timestamp* asli dan palsu. Metode yang penulis temukan adalah metode String Matching yang dimana menurut penulis adalah metode yang tepat dalam mengerjakan penelitian ini. Menurut Rosaria algoritma string matching adalah sebuah algoritma yang digunakan dalam pencocokkan suatu pola kata tertentu terhadap suatu kalimat atau teks panjang. Algoritma string matching sendiri dapat dilakukan dengan beberapa cara tertentu, antara lain cara Brute Force dan cara Knuth- Morris-Pratt (KMP) [4].

Pada tugas akhir ini penulis berusaha merancang sebuah skenario dimana *timestamp* pada *dataset file* .pdf dipalsukan menggunakan *tool "Attribute Magic 2.4"* pada sistem operasi Windows dengan *file system* NTFS dan membandingkan string *timestamp* antara *command* "*get lastmodified*" dan metadata *dataset* yang sudah di manipulasi serta menggunakan metode *String Matching* untuk mencocokkan *timestamp* yang dipalsukan.

1.2 Tujuan

Dalam melakukan penelitian ini pastilah terdapat tujuan dan manfaat yang dapat diperoleh.

1. Menerapkan investigasi forensik digital untuk mendeteksi pemalsuan *timestamp* pada *file system* windows
2. Mengetahui *timestamp* asli dan palsu
3. Menerapkan metode *String Matching* untuk pencocokan antara *timestamp* pada metadata dan *command* "get lastmodified"

1.3 Manfaat

Dalam melakukan penelitian ini pastilah terdapat manfaat yang dapat diperoleh :

1. Memberikan kemudahan dalam mengenali pemalsuan *timestamp* pada *file*
2. Mendapatkan alternatif metode forensik digital terhadap investigasi pemalsuan *timestamp*

1.4 Rumusan Masalah

Adapun rumusan masalah dalam tugas akhir ini yaitu sebagai berikut :

1. Bagaimana membuat skema untuk pemalsuan *timestamp*?
2. Bagaimana analisa forensik untuk *timestamp* yang dipalsukan dan yang asli?
3. Bagaimana pembuktian *timestamp* yang sudah dipalsukan dan yang normal?

1.5 Batasan Masalah

Adapun batasan masalah dalam tugas akhir ini yaitu sebagai berikut :

1. Pemalsuan *timestamp* dilakukan pada *file system NTFS* di sistem operasi Windows.
2. *Dataset* dibuat menyesuaikan dengan skema pada riset ini.
3. Pemalsuan *timestamp* dilakukan pada *dataset file* .pdf
4. Menampilkan *timestamp* sesudah dan sebelum dipalsukan menggunakan wmic dengan *command* “get lastmodified”.
5. *Timestamp* yang dianalisa berupa *modify* (M).
6. Menggunakan *tool* “*Attribute Magic 2.4*” untuk memanipulasi *timestamp*
7. Menggunakan program Hexedit untuk melakukan pembacaan metadata pada *dataset*

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini akan melewati beberapa tahapan sebagai berikut :

1. Metode study pustaka / literatur)

   Dalam tahap ini ini dilakukan sesuai dengan kerelevanan penelitian sebelumnya yang mengacu banyaknya artikel, paper, jurnal dan buku yang berhubungan dengan penelitian ini yang berjudul "Analisa Forensik Pemalsuan *Timestamp* Pada *New Technology File system* (NTFS).

2. Metode Konsultasi

   Pada metode ini, peneliti melakukan konsultasi kepada orang-orang yang dianggap memiliki pengetahuan dan wawasan terhadap permasalahan yang di temui saat pembuatan Tugas Akhir.

3. Metode perancangan dan pembuatan sistem

   Tahapan ini merupakan tahapan dimana menentukan perangkat yang dibutuhkan untuk penelitian ini, baik berupa perangkat keras maupun lunak.

4. Pengujian

   Tahapan ini berupa pengujian yang sesuai dengan parameter yang ditentukan oleh batasan masalah.

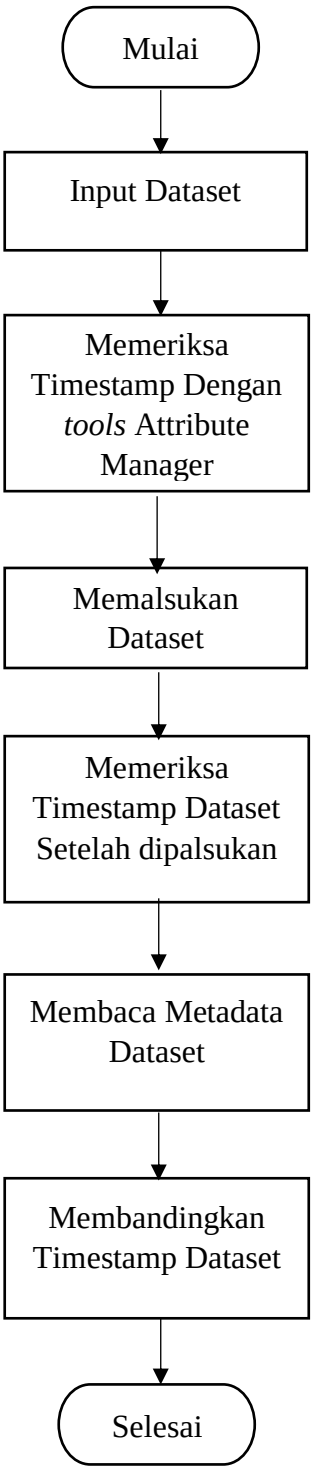
5. Metode Observasi

   Metode ini dilakukan dengan pengamatan dan pencatatan terhadap data yang diperoleh

6. Hasil dan Analisa

   Pada tahap ini didapatkan hasil serta analisa penulis dalam penulisan tugas akhir. Tahapan ini juga terdapat beberapa poin saran dari penulis untuk penelitian selanjutnya. Tahapan ini berisi hasil pengujian pada penelitian tersebut kemudian dianalisa forensik hasil tersebut guna mengetahui pemalsuan *timestamp*.

Pada Gambar 1.1 berikut ditampilkan metodologi penelitian secara visual dalam bentuk diagram air yang merepresentasikan proses pelaksanaan penelitian :



Gambar 1.1 Diagram Air Metodologi Penelitian

1.7 Sistematika Penulisan

Dalam melakukan pembuatan laporan tugas akhir, terdapat sistematika penulisan yang akan di tulis dalam membuat laporan tugas akhir ini. Penyusunan tugas akhir ini dibuat sistematika penulisan untuk memudahkan dan menjelaskan inti dari tiap bab yang dijelaskan sebagai berikut:

BAB I PENDAHULUAN

Pada Bab I akan terdiri dari latar belakang, tujuan dan manfaat, rumusan dan batasan masalah, metodologi penelitian, dan sistematika penulisan yang mengacu pada landasan topik penelitian.

BAB II TINJAUAN PUSTAKA

Pada Bab II akan berisi tentang dasar teori forensic digital, timestamp, *New Technology File System* (NTFS), *Portable Document Format* (PDF), metadata dan hexadecimal.

BAB III METODOLOGI PENELITIAN

Pada Bab III akan membahas penjelasan secara sistematis mengenai bagaimana proses penelitian dilakukan, tahapan perancangan sistem, dan penerapan metode penelitian.

BAB IV PENGUJIAN DAN ANALISIS

Pada Bab IV menjelaskan tentang hasil pengujian yang dilakukan serta menganalisa dari hasil data yang didapat.

BAB V KESIMPULAN

Pada Bab V berisi kesimpulan dari hasil pengujian yang dilakukan, menjawab tujuan yang dicapai dari BAB I (Pendahuluan), dan saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] Raharjo. Budi. “Sekilas Mengenai Forensik Digital”. *Jurnal Sosioteknologi Edisi 29* . 2013

[2] N. Budhisantosa, “Analisis Forensik Komputer Pada Timestamps Sistem Berkas NTFS,” *Forum Ilm. Fak. Ilmu Komput. Univ. Esa Unggul*, vol. 13, no. 2, pp. 166–173. 2016.

[3] G. S. Cho, “A Computer Forensic Method For Detecting Timestamp Forgery In NTFS,” *Comput. Secur.*, vol. 34, pp. 36–46. 2013.

[4] Rosaria, Maya. 2015. Implementasi Algoritma Pencocokan String Knuth morris-Pratt Dalam Aplikasi Pencarian Dokumen Digital Berbasis Android. Jurnal Rekursif, Vol. 3 No.2 November. 2015

[5] Bramantio. R. N. *Analisa Forensik Pemalsuan Timestamp pada Fourth Extended File System (ext4)*. 2019

[6] Sulianta. Feri. *Komputer Forensik*. PT.Elex Media Komputindo Jakarta. 2013

[7] L. "SysDev Laboratories", “File system type and data recovery chances,” *internet*, 2017. [Online]. Available : http://www.raisedr.com/kb/recovery_cha.php. [Accessed: 11-Nov-2019].

[9] Techterms.com, “PDF Definition,” *internet*, 2018. [Online]. Available: https://techterms.com/definition/pdf. [Accessed: 15-Nov-2019].

[10] M. Rouse, “Metadata Definition,” *internet*, 2014. [Online]. Available: https://whatis.techtarget.com/definition/metadata. [Accessed: 15-Nov-2019].

[11] M. Rouse, “Hexadecimal,” *Internet*, 2005. [Online]. Available: https://whatis.techtarget.com/definition/hexadecimal. [Accessed: 15-Nov-2019].