

TUGAS AKHIR

Analisis Metode Live Forensics Pada Perangkat Memory Laptop Untuk Pencarian Artefak Digital Berbasis Linux



Oleh:

M.AINUL YAQIN

NIM. 1410651149

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2019**

TUGAS AKHIR

Analisis Metode Live Forensics Pada Perangkat Memory Laptop Untuk Pencarian Artefak Digital Berbasis Linux

**Diajukan sebagai salah satu syarat untuk kelulusan
Strata Satu (S-1) Jurusan Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Jember**



Oleh:

M.AINUL YAQIN

NIM. 1410651149

DOSEN PEMBIMBING

Triawan Adi Cahyanto. M.Kom

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2019

HALAMAN PENGESAHAN

Analisis Metode Live Forensics Pada Perangkat Memory Laptop Untuk Pencarian Artefak Digital Berbasis Linux

M.AINUL YAQIN

1410651149

Telah mempertanggung jawabkan Laporan Tugas Akhirnya pada sidang
Tugas Akhir tanggal 05 Juli 2019 sebagai salah satu syarat kelulusan
dan mendapatkan gelar Sarjana Komputer (S.Kom)

di

Universitas Muhammadiyah Jember

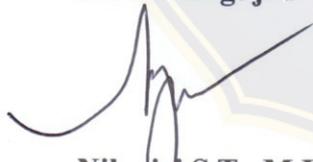
Dosen Pembimbing



Triawan Adi Cahyanto. M.Kom

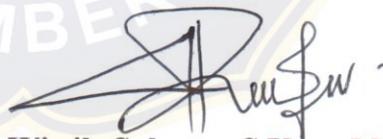
NPK. 12 03 719

Dosen Penguji 1



Agung Nilogiri, S.T., M.Kom
NIP. 19770330 200501 1 002

Dosen Penguji 2



Wiwik Suharso, S.Kom, M.Kom
NIP. 19760906 200501 1003

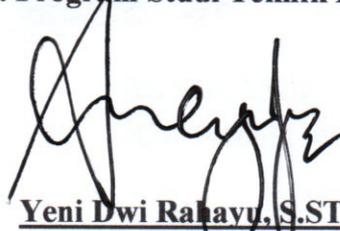
Mengesahkan.

Dekan Fakultas Teknik


Ir. Suhartinah, M.T
NPK. 95 05 246

Mengetahui.

Ketua Program Studi Teknik Informatika


Yeni Dwi Rahayu, S.ST., M.Kom
NPK. 11 03 590

PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : M.Ainul Yaqin

NIM : 1410651149

Institusi : Program Studi Teknik Informatika, Fakultas Teknik
Universitas Muhammadiyah Jember.

Menyatakan bahwa Tugas Akhir yang berjudul ” **Analisis Metode Live Forensics Pada Perangkat Memory Laptop Untuk Pencarian Artefak Digital Berbasis Linux**” Bukan merupakan Tugas Akhir orang lain sebagian maupun keseluruhan kecuali dalam bentuk kutipan yang telah di sebutkan sumbernya.

Demikian surat pernyataan ini di buat dengan sebenar-benarnya dan apabila pernyataan ini tidak benar, penulis bersedia mendapatkan sanksi dari akademik.

Jember, 23 September 2019



M.Ainul Yaqin

NIM.1410651149

KATA PENGANTAR

Segala puji bagi Allah SWT yang telah memberikan rahmat dan karuniaNya kepada penulis, sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Shalawat dan salam senantiasa tercurah kepada Rasulullah SAW yang mengantarkan manusia dari zaman kegelapan ke zaman yang terang benderang ini. Penyusunan skripsi ini dimaksudkan untuk memenuhi sebagian syarat-syarat guna mencapai gelar Sarjana Komputer di Universitas Muhammadiyah Jember.

Penulis menyadari bahwa penulisan ini tidak dapat terselesaikan tanpa dukungan dari berbagai pihak baik moril maupun materil. Oleh karena itu, penulis ingin menyampaikan ucapan terima kasih kepada semua pihak yang telah membantu dalam penyusunan skripsi ini terutama kepada:

1. Kedua orang tua, ayahanda tercintadan ibunda tersayang yang telah memberikan dukungan baik moril maupun materil serta doa yang tiada henti-hentinya kepada penulis.
2. IbuIr. Suhartinah, M.T, selaku Dekan Fakultas Teknik Universitas Muhammadiyah Jember.
3. IbuYeni Dwi Rahayu, S.ST,. M.Kom, selaku Ketua Jurusan Teknik Informatika Universitas Muhammadiyah Jember.
4. Bapak Triawan Adi Cahyanto. M.Kom, selaku dosen Pembimbing Skripsi yang telah berkenan memberikan tambahan ilmu dan solusi pada setiap permasalahan atas kesulitan dalam penulisan skripsi ini.
5. Seluruh teman-teman seangkatan, Angkatan 2014 yang selalu mengisi hari-hari menjadi sangat menyenangkan.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna oleh karena itu, penulis mengharapkan segala bentuk saran serta masukan bahkan kritik yang membangun dari berbagai pihak. Semoga skripsi ini dapat bermanfaat bagi para pembaca.

Jember, September 2019

Penulis,

M.Ainul Yaqin

DAFTAR ISI

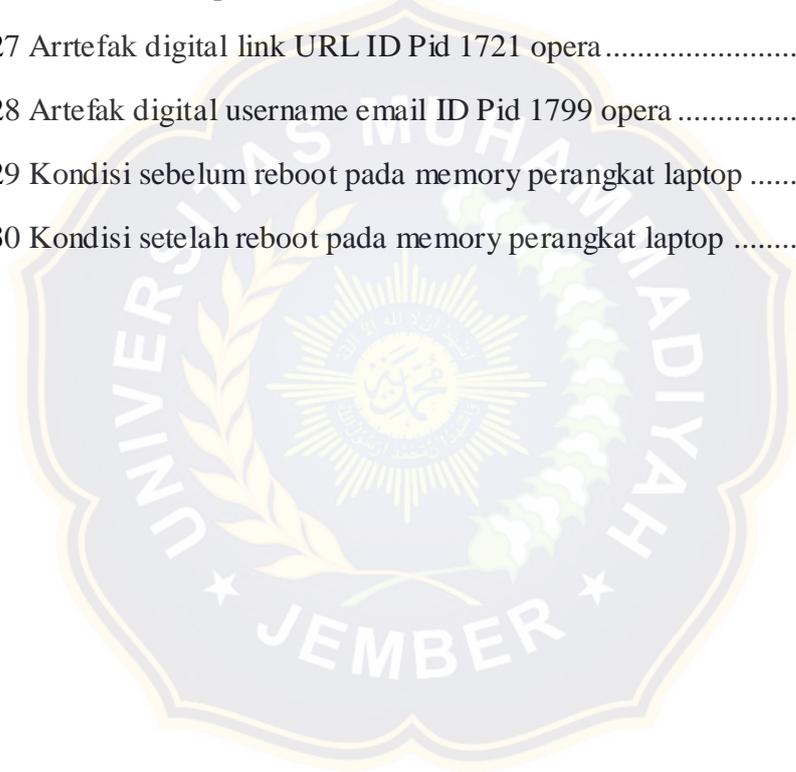
HALAMAN PENGESAHAN	i
PERNYATAAN	ii
MOTTO	iii
KATA PENGANTAR	iv
ABSTRAK	v
DAFTAR ISI	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
BAB 2 TINJAUAN PUSTAKA	4
2.1 Email.....	4
2.2 User_id dan Password.....	4
2.3 PayPal	4
2.4 Link URL.....	5
2.5 Forensics Digital.....	5
2.6 Memory.....	5
2.7 Live Forensics.....	5
2.8 Komputer	6
2.9 Sistem Operasi	7
2.10Sistem Operasi Linux	8
2.11Linux Memory Extractor (LiME).....	9
2.12Volatility	9
2.13Penelitian Terdahulu	9
BAB 3 METODOLOGI PENELITIAN	11
3.1 Studi Pustaka	11
3.2 Metode Penelitian	11
3.2.1Pre-Analisis	12

3.2.2 Analisis.....	12
3.2.3 Post Analisis.....	12
3.3 Tempat dan Waktu Penelitian.....	13
3.4 Persiapan Alat dan Bahan.....	13
3.5 Skenario Kasus.....	14
3.6 Simulasi Kasus.....	16
3.7 Olah TKP dan Pengamanan Barang Bukti.....	16
3.8 Akuisisi Data Live Forensics.....	16
3.9 Kerangka Akuisisi memory.....	16
BAB 4 ANALISIS DAN HASIL.....	19
4.1 Data.....	19
4.1.1 Sumber Data.....	19
4.1.2 Proses Pengambilan Data.....	19
4.2 Identifikasi Kebutuhan.....	19
4.3 Akuisisi Memory Pada Perangkat Laptop Menggunakan LiME.....	20
4.4 Volatility.....	21
4.5 Scanning Proses.....	21
4.6 Scanning Web Browser.....	22
4.7 Pencarian Bukti.....	24
4.7.1 Pencarian Data Artefak_1 Web Browser Firefox.....	25
4.7.2 Pencarian Data Artefak_2 Web Browser Chrome.....	27
4.7.3 Pencarian Data Artefak_3 Web Browser Opera.....	29
4.8 Analisis Hasil.....	32
4.8.1 Kesimpulan Hasil Analisis Memory Perangkat Laptop.....	35
4.8.2 Kesimpulan Akhir Analisa Memory Perangkat laptop.....	36
4.9 Pengujian Memory Sebelum Dan Setelah Dilakukan Shutdown.....	36
38	
5.1 Kesimpulan.....	38
5.2 Saran.....	39
DAFTAR PUSTAKA.....	40
LAMPIRAN.....	

DAFTAR GAMBAR

Gambar 2.1 Berbagai Macam Sistem Operasi Komputer	8
Gambar 3.1 Model Forensics Digital	11
Gambar 3.2 Ilustrasi Kasus Penyalahgunaan Account.....	15
Gambar 3.2 Flowchart Proses Akuisisi memory pada perangkat laptop	17
Gambar 4.1 Membuat module LiME	20
Gambar 4.2 Akuisisi memory perangkat laptop berbasis linux	20
Gambar 4.3 Command di Volatility berbasis linux.....	21
Gambar 4.4 Perintah untuk mengecek profile kernel volatility berbasis linux	21
Gambar 4.5 Scanning memory artefak_1	21
Gambar 4.6 Scanning memory artefak_2.....	22
Gambar 4.7 Scanning artefak_3	22
Gambar 4.8 Aktifitas web browser pada memory perangkat laptop pada artefak_1	22
Gambar 4.9 Aktifitas web browser pada memory perangkat laptop pada artefak_2.....	23
Gambar 4.10 Aktifitas web browser pada memory perangkat laptop pada artefak_3	22
Gambar 4.11 Artefak digital username facebook ID Pid 1832 firefox	24
Gambar 4.12 Artefak digital password facebook ID Pid 1832 firefox	24
Gambar 4.13 Artefak digital username email ID Pid 1832 firefox	25
Gambar 4.14 Artefak digital password email ID Pid 1832 firefox	25
Gambar 4.15 Artefak digital username paypal ID Pid 1832 firefox	25
Gambar 4.16 Artefak digital password paypal ID Pid 1832 firefox	26
Gambar 4.17 Artefak digital username facebook ID Pid 2122 chrome	26
Gambar 4.18 Artefak digital username email ID Pid 2122 chrome.....	27
Gambar 4.19 Artefak digital username email ID Pid 2310 chrome	27
Gambar 4.20 Artefak digital username facebook ID Pid 1720 chrome	27
Gambar 4.21 Artefak digital username email ID Pid 1720 chrome.....	28

Gambar 4.22 Artefak digital link URL ID Pid 1720 chrome	28
Gambar 4.23 Artefak digital username paypal ID Pid 2428 chrome	29
Gambar 4.24 Artefak digital username dan password paypal ID Pid 2428 opera ..	29
Gambar 4.25 Artefak digital username facebook ID Pid 1721 opera	30
Gambar 4.26 Artefak digital username password paypal dan username facebook ID Pid 1721 opera	30
Gambar 4.27 Arrtefak digital link URL ID Pid 1721 opera	31
Gambar 4.28 Artefak digital username email ID Pid 1799 opera	31
Gambar 4.29 Kondisi sebelum reboot pada memory perangkat laptop	36
Gambar 4.30 Kondisi setelah reboot pada memory perangkat laptop	37



DAFTAR TABEL

Tabel2.1 Ulasan dan Usulan Penelitian.....	10
Tabel3.1 Spesifikasi Laptop Dengan Sistem Operasi Linux Ubuntu.....	13
Tabel3.2 Software Analisis Digital Forensics.....	14
Tabel4.1 Hasil analisis artefak_1	32
Tabel4.2 Hasil analisis artefak_2	32
Tabel4.3 Hasil analisis artefak_3	33
Tabel4.4 Kesimpulan hasil analisis memory pada perangkat laptop	35

