

**ANALISIS DIGITAL FORENSIK PADA *E-MAIL* SEBAGAI
BARANG BUKTI DIGITAL DALAM PENANGANAN KASUS
PENIPUAN**



SKRIPSI

Muhammad Zaki Muallim

1503040014

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN SAINS
UNIVERSITAS MUHAMMADIYAH PURWOKERTO
FEBRUARI 2020**

**ANALISIS DIGITAL FORENSIK PADA *E-MAIL* SEBAGAI
BARANG BUKTI DIGITAL DALAM PENANGANAN KASUS
PENIPUAN**



SKRIPSI

Muhammad Zaki Muallim

1503040014

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN SAINS
UNIVERSITAS MUHAMMADIYAH PURWOKERTO
FEBRUARI 2020**

HALAMAN PERSETUJUAN

Skripsi yang diajukan oleh:

Nama : Muhammad Zaki Muallim

NIM : 1503040014

Program Studi : Teknik Informatika

Fakultas : Teknik dan Sains

Perguruan Tinggi : Universitas Muhammadiyah Purwokerto

Judul : Analisis Digital Forensik Pada *E-mail* Sebagai
Barang Bukti Digital Dalam Penanganan Kasus
Penipuan.

Telah disetujui untuk diajukan dalam sidang skripsi
Purwokerto, 18 Maret 2020

PEMBIMBING

Ermadi Satriya Wijaya, S.T., M.Kom.

NIK. 2160767

HALAMAN PENGESAHAN

Skripsi yang diajukan oleh:

Nama : Muhammad Zaki Muallim
NIM : 1503040014
Fakultas : Teknik dan Sains
Perguruan tinggi : Universitas Muhammadiyah Purwokerto
Judul : Analisis Digital Forensik Pada E-mail Sebagai Barang Bukti Digital Dalam Penanganan Kasus Penipuan.

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer (S.Kom.) pada Program Studi Teknik Informatika, Fakultas Teknik dan Sains, Universitas Muhammadiyah Purwokerto.

DEWAN PENGUJI

- Penguji 1 (Pembimbing) : Ermadi Satriya Wijaya, S.T., M.Kom.
- Penguji 2 : Muhammad Hamka, S.T., M.Kom
- Penguji 3 : Mukhlis Prasetyo Aji, S.T., M.Kom.

Ditetapkan di : Purwokerto
Tanggal : Juni 2020

Mengetahui

Dekan Fakultas Teknik dan Sains



Teguh Marhendi, S.T., M.T., ASEAN.Eng., IPM
NIK. 2160172

(Handwritten signatures of the examiners)

HALAMAN PERNYATAAN ORISINALITAS

Saya yang bertandatangan di bawah ini :

Nama : Muhammad Zaki Muallim

NIM : 1503040014

Fakultas : Teknik dan Sains

Perguruan Tinggi : Universitas Muhammadiyah Purwokerto

menyatakan dengan sebenar-benarnya bahwa skripsi ini adalah hasil karya saya dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar serta bukan hasil penjiplakan dari karya orang lain.

Demikian pernyataan ini saya buat dan apabila kelak di kemudian hari terbukti ada unsur penjiplakan, saya bersedia mempertanggungjawabkan sesuai dengan ketentuan yang berlaku.

Purwokerto, Juni 2020

Yang membuat pernyataan

MEYERA TEMPAH

66809AHF539256458

6000
ENAM RIBURUPIAH

Muhammad Zaki Muallim

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI
UNTUK KEPENTINGAN AKADEMIS**

Sebagai sivitasi akademika Universitas Muhammadiyah Purwokerto dan demi pengembangan ilmu pengetahuan, saya yang bertandatangan dibawah ini :

Nama : Muhammad Zaki Muallim

NIM. : 1503040014

Fakultas : Teknik dan Sains

Perguruan Tinggi : Universitas Muhammadiyah Purwokerto

Jenis Karya : Skripsi

Menyetujui untuk memberikan Hak Bebas Royalti Noneksklusif (*Non-eclusive Royalty-Free Right*) kepada Universitas Muhammadiyah Purwokerto atas karya saya yang berjudul :

**ANALISIS DIGITAL FORENSIK PADA E-MAIL SEBAGAI
BARANG BUKTI DIGITAL DALAM PENANGANAN KASUS
PENIPUAN**

berserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Muhammadiyah Purwokerto berhak menyimpan, mengalihmedia/mengalihformatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan memublikasikan skripsi saya dengan tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Pernyataan ini saya buat dengan sebenarnya.

Dibuat di

Purwokerto

Pada Tanggal

Juni 2020

Yang Menyatakan,



Muhammad Zaki Muallim

HALAMAN PERSEMBAHAN

Skripsi ini

Kupersembahkan untuk :

Ibu Umi Salamah dan Kakak-Kakakku Tercinta



HALAMAN MOTTO

Mengikuti hawa nafsu tidak akan ada habisnya, maka dari itu kita harus selalu bersyukur. “Bacalah surat al-ikhlas dan al-Mu’awwidzatain (Surat al-Falaq dan an-Nas) saat petang dan pagi tiga kali, niscaya ia mencukupimu dari segala sesuatu.”

(Hadits diriwayatkan oleh Abu Dawud dan at-Tirmidzi, Beliau berkata, “Hadits Hasan Shahih”).



ANALISIS DIGITAL FORENSIK PADA *E-MAIL* SEBAGAI BARANG BUKTI DIGITAL DALAM PENANGANAN KASUS PENIPUAN

Muhammad Zaki Muallim

ABSTRAK

Email adalah salah satu alat media untuk berkomunikasi dan bisa menjadi alat kejahatan untuk mendapatkan keuntungan. Penipuan menggunakan *email* sudah banyak merugikan masyarakat dengan cara mengirimkan pesan *email* yang tidak diketahui siapa pengirim *email* tersebut. Salah satu *email* yang sering digunakan untuk penipuan adalah *Gmail*, *sever* ini banyak digunakan oleh masyarakat untuk melakukan kejahatan penipuan berupa transaksi *chat* yang didalamnya berupa *teks*, gambar, *video* untuk melakukan penipuan dengan cara membajak nama perusahaan atau nama seseorang. Tujuan dari penelitian ini adalah menemukan isi pesan yang dikirimkan menggunakan *email* dan menemukan *email* yang asli untuk mendapatkan bukti digital untuk dijadikan bukti-bukti kejahatan sesuai dengan konsep analisis bukti digital penipuan menggunakan *email*. Pada penelitian ini barang bukti elektronik yang berupa laptop pelaku dan laptop korban. Korban berperan sebagai penerima pesan *email* yang dirugikan oleh pelaku. Sumber data pada penelitian ini berasal dari simulasi dan skenario yang telah dibuat, penelitian ini menggunakan 2 laptop yaitu laptop *asus* dan *lenovo*. Analisis data pada penelitian ini menggunakan metode *NIST (National Institute of Standar Technology)* yang memiliki langkah-langkah penelitian yaitu *collection, examination, analysis, dan reporting*. Objek data yang diambil berupa isi pesan pada *Gmail* yang didalamnya berupa transaksi *chat*, gambar, *video*, dan bukti transfer. Pencarian bukti kejahatan penipuan dengan *Gmail* menggunakan *FTK Imager* dan untuk mencari alamat *email* yang asli menggunakan *myipaddres, Iptrackeronline, Ipgeolocation, dan Grabify*. Hasil yang diperoleh berupa bukti pesan *email* yang dihapus oleh pelaku antara lain bukti chat, gambar yang berekstensi *jpg* dan *video* yang berekstensi *mp4*.

Kata kunci : *Email, Gmail, myipaddres, Iptrackeronline, Ipgeolocation, dan Grabify*.

DIGITAL FORENSIC ANALYSIS OF E-MAIL AS DIGITAL EVIDENCE GOODS IN THE HANDLING OF FRAUD CASE

Muhammad Zaki Muallim

ABSTRACT

Email is one of the media tools to communicate and can be a crime tool for profit. Fraud using email has done a lot of harm to society by sending email messages that are not known who sent the email. One of the emails that is often used for fraud is Gmail, this server is widely used by the public to commit fraudulent crimes in the form of chat transactions in which in the form of text, images, videos to commit fraud by hijacking a company's name or someone's name. The purpose of this study is to find the contents of messages sent using e-mails and find original e-mails to obtain digital evidence to be used as evidence of crime in accordance with the concept of digital fraud proof analysis using e-mail. In this study, electronic evidence in the form of the perpetrator's laptop and the victim's laptop. The victim acts as the recipient of an email message that is harmed by the perpetrator. The data source in this study comes from simulations and scenarios that have been made, this study uses 2 laptops namely Asus and Lenovo laptops. Analysis of the data in this study uses the NIST (National Institute of Technology Standards) method which has research steps in the collection, examination, analysis, and reporting. Data objects taken in the form of message content in Gmail in which in the form of chat transactions, images, videos, and proof of transfer. Search for evidence of fraud with Gmail using FTK Imager and to find the original email address using myipaddres, Iptrackeronline, Ipgeolocation, and Grabify. The results obtained in the form of proof of e-mail messages deleted by the perpetrators include proof of chat, images with the extension of jpg and video with the extension of mp4.

Keywords: Email, Gmail, myipaddres, Iptrackeronline, Ipgeolocation, and Grabify.

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas berkat rahmat, anugerah, serta hidayah-Nya sehingga laporan skripsi ini dapat terselesaikan dengan baik sesuai waktu yang ditentukan. Judul yang diambil adalah “**ANALISIS DIGITAL FORENSIK PADA *E-MAIL* SEBAGAI BARANG BUKTI DIGITAL DALAM PENANGANAN KASUS PENIPUAN**”. Tujuan penulisan skripsi ini merupakan salah satu syarat wajib bagi mahasiswa program S-1 di program studi Teknik Informatika, Fakultas Teknik dan Sains, Universitas Muhammadiyah Purwokerto.

Terselesainya skripsi ini tidak terlepas dari bantuan banyak pihak, sehingga pada kesempatan ini dengan segala kerendahan hati dan penuh rasa hormat, menghaturkan terima kasih yang sebesar-besarnya kepada :

1. Yth. Bapak Dr. Anjar Nugroho, M.S.I., M.H.I., selaku Rektor Universitas Muhammadiyah Purwokerto.
2. Yth. Ir. Teguh Marhendi, S.T., M.T., ASEAN.Eng., IPM, selaku Dekan Teknik dan Sains.
3. Yth. Ermadi Satriya Wijaya, S.T., M.Kom., selaku dosen pembimbing skripsi, yang sudah membimbing dalam mengerjakan skripsi hingga terselesainya skripsi ini.
4. Yth. Bapak Feri Wibowo, S.Kom., M.Cs., selaku Ketua Prodi Teknik Informatika Universitas Muhammadiyah Purwokerto.
5. Dosen Teknik Informatika Universitas Muhammadiyah Purwokerto yang telah memberi banyak ilmu sehingga dapat terselesainya skripsi ini.
6. Yang tersayang dan tercinta, Ibu Umi Salamah, kakak saya Mohammad Rois Ridlo dan Ibnu Allimudin, serta keluarga yang dengan ketulusan hati sudah memberikan do’a dan dukungan tanpa henti hingga skripsi ini selesai.

7. Orang-orang terdekat saya, Aniszhadenna Damayanti, Ranggi, Pandhu, Tanjung, Kukuh, Hanip, Guna, Uji Bagus, Iqbal, Dewa, Azhi, Gilang Eksayuda, Biki, Maul, Pradipta, Aji CP, Yoga, Aji TW, Teguh, Ardianto, Alvin, Mas Tata. Esa, Raras, Margareth, Mas Bagus, “Para Team Wawiwu” (Dimas, Agung, Anjar, Thofik, Sulis, Yoli, Bom-Bom, Andi, Dio, Yadi, Rian, dan Teman-teman yang dipurwokerto), dan semuanya yang tak bisa disebutkan satu persatu, yang telah memberikan semangat dan dukungan terus menerus.
8. Teman-teman Teknik Informatika 2015, yang sudah berjuang bersama sejak awal memulai bangku perkuliahan hingga detik ini.
9. Teman-teman kelompok KKN 013 Desa Karangcegak (Arif, Sandi, Dimas, Hafid, Bowo, Via, bibah, Eka, Gita) yang sudah pernah berjuang bersama dalam suka dan duka selama 32 hari di Desa Karangcegak, pengalaman yang tak akan terlupakan, senang dapat berkenalan dengan kalian.
10. Semua pihak yang tidak dapat disebutkan satu per satu yang telah memberi semangat untuk menyelesaikan tugas akhir ini.

Akhir kata, dengan harapan yang besar semoga laporan skripsi ini dapat memberikan manfaat yang berarti. Dan yang terpenting adalah semoga dapat turut serta memajukan ilmu pengetahuan.

Purwokerto, Juni 2020

Muhammad Zaki Muallim

DAFTAR ISI

ANALISIS DIGITAL FORENSIK PADA <i>E-MAIL</i> SEBAGAI BARANG BUKTI DIGITAL DALAM PENANGANAN KASUS PENIPUAN.....	i
HALAMAN PERSETUJUAN	Error! Bookmark not defined.
HALAMAN PENGESAHAN.....	ii
DEWAN PENGUJI.....	Error! Bookmark not defined.
HALAMAN PERNYATAAN ORISINALITAS ...	Error! Bookmark not defined.
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	vii
ABSTRAK	viii
ABSTRACT	ix
KATA PENGANTAR.....	x
DAFTAR ISI.....	xii
DAFTAR TABEL	xv
DAFTAR GAMBAR.....	xvi
BAB 1 PENDAHULUAN	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	3
C. Batasan Masalah	3
D. Tujuan Penelitian	4
E. Manfaat Penelitian	4
BAB II TINJAUAN PUSTAKA.....	5
A. Penelitian Terdahulu	5

B. Landasan Teori.....	7
1. <i>E-mail</i>	7
2. Digital Forensik	8
3. Komputer Forensik	10
4. National Institute of Standards and Technology (NIST)	10
5. FTK (<i>Forensic Tool Kit</i>).....	11
BAB III METODE PENELITIAN.....	12
A. Jenis Penelitian	12
B. Waktu Dan Tempat.....	13
C. Variabel Yang Diteliti.....	13
D. Sumber Data	13
E. Alat Penelitian.....	13
F. Analisis Data	14
G. Langkah-langkah penelitian.....	19
BAB IV HASIL DAN PEMBAHASAN	20
A. Sumber Data	20
B. Analisis Data.....	24
1. <i>Collection</i>	24
a. Identifikasi laptop korban.....	24
b. Identifikasi laptop pelaku dan prmbuktian laptop pelaku	27
2. <i>Examination</i>	29
3. <i>Analysis</i>	36
4. <i>Reoprtng</i>	44
5. <i>Tracking email</i>	45

BAB V PENUTUP.....	55
A. Simpulan.....	55
B. Saran	56
DAFTAR PUSTAKA	57



DAFTAR TABEL

Tabel 4.1 Identifikasi laptop korban	26
Tabel 4.2 Identifikasi laptop pelaku.....	28
Tabel 4.3 Hasil akuisisi pada laptop korban	31
Tabel 4.4 Hasil akuisisi pada laptop pelaku.....	34
Tabel 4.5 Nilai hash file	35
Tabel 4.6 Hasil analisis temuan bukti kejahatan.....	43
Tabel 4.7 Uji perbandingan hasil digital.....	44
Tabel 4.8 Perbandingan hasil tracking.....	53
Tabel 4.9 uji perbandingan bukti digital.....	54



DAFTAR GAMBAR

Gambar 3.1 Metode NIST Versi 800-86 Kent et al., (2017).....	12
Gambar 3.2 Skenario untuk mendapatkan data.....	15
Gambar 4.1 Laptop korban	20
Gambar 4.2 Laptop korban	21
Gambar 4.3 Pesan yang dikirim oleh pelaku ke email korban.....	21
Gambar 4.4 Chat email pada laptop korban.....	22
Gambar 4.5 Lanjutan chat email pada laptop korban	22
Gambar 4.6 File yang dikirim oleh korban	23
Gambar 4.7 File yang diterima oleh pelaku	23
Gambar 4.8 Laptop korban	24
Gambar 4.9 Identifikasi laptop korban.....	25
Gambar 4.10 Serial Number laptop milik korban.....	26
Gambar 4.11 Laptop pelaku	27
Gambar 4.12 Identifikasi laptop korban	27
Gambar 4.13 Serial Number laptop pelaku.....	28
Gambar 4.14 Membuka FTK Imager.....	30
Gambar 4.15 Memilih destinasi data yang akan diambil.....	30
Gambar 4.16 Proses pengambilan data pada laptop korban	31
Gambar 4.17 Hasil data yang telah diambil dari laptop korban.....	31
Gambar 4.18 Laptop membuka FTK Imager	32
Gambar 4.19 Memilih destinasi data yang akan diambil.....	32
Gambar 4.20 Proses pengambilan data pada laptop pelaku	33
Gambar 4.21 Hasil data yang telah diambil dari laptop pelaku	33
Gambar 4.22 Gambar nilai hash milik korban.....	34
Gambar 4.23 Gambar nilai hash milik pelaku	35
Gambar 4.24 Bukti chat gmail pada laptop korban.....	38
Gambar 4.25 Bukti transfer yang dikirimkan kepada pelaku	39
Gambar 4.26 Bukti kartu mahasiswa yang dikirimkan kepada pelaku.....	39
Gambar 4.27 Bukti chat gmail pada laptop pelaku	41

Gambar 4.28 Bukti transfer yang diterima pelaku	42
Gambar 4.29 Bukti kartu mahasiswa yang diterima oleh pelaku.....	43
Gambar 4.30 Video berbentuk file mp4.....	43
Gambar 4.31 Gambar hasil tracking email pelaku.....	46
Gambar 4.32 Gambar hasil tracking email pelaku.....	47
Gambar 4.33 Gambar hasil tracking email pelaku.....	48
Gambar 4.34 Gambar hasil tracking email pelaku.....	49
Gambar 4.35 Gambar hasil tracking email pelaku.....	50
Gambar 4.36 Gambar hasil tracking email pelaku.....	51
Gambar 4.37 Gambar hasil tracking email pelaku.....	51
Gambar 4.38 Persamaan google chrome.....	52
Gambar 4.39 Gambar perbedaan header.....	52
Gambar 4.40 Gambar perbedaan header lanjutan	53

