JURNAL RESISTOR | ISSN 2598-7542 | E-ISSN 2598-9650
Vol. 7 No 3 – December 2024 | https://s.id/jurnalresistor
DOI: https://doi.org/10.31598
Publishing: Prahasta Publisher

Analisis Forensik Pemalsuan Dokumen PDF Menggunakan Metode National Institute of Justice (NIJ)

Marcel Afandi[1], Rifki Amrulloh[2], Khairunnisak Nur Isnaini[3], Didit Suhartono[4]

[1,2,3,4]Departemen Informatika, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto
Jl. Letjend Pol. Soemarto No. 126, Purwokerto, Indonesia

e-mail: marcelafandi026@gmail.com [1], kikiamrulloh23@gmail.com [2], nisak@amikompurwokerto.ac.id[3], didit@amikompurwokerto@ac.id[4]
Kontak WA: +628986660369[3]

Received : June, 2024	Accepted : November, 2024	Published : December, 2024

Abstract

With the rapid growth of information and communication technology, the need for a sophisticated digital forensic approach to security has become more urgent. The problem that needs to be resolved using digital forensic steps is the indication of alteration and falsification of documents with the .pdf extension. By involving various forensic analysis methods, such as metadata examination, physical observation, hash value, analysis using Principal Component Analysis (PCA), and the use of forensic tools such as Adobe Acrobat Reader, Exiftools, imageforensic.org and HashMyFile, it is expected to address existing crime cases. This research aims to study the challenges posed by digital documents, emphasizing the need for innovative approaches to uncover hidden information, detect alterations, and authenticate the integrity of PDF files. The combination of the NIJ method and Analysis using PCA produces an accurate and precise analysis as seen from the dimensionality reduction capability of PCA. The results show that the NIJ method and PCA analysis can be used to prove the authenticity of a PDF document by finding changes in the PDF document. In addition, this research also provides recommendations for the development of forensic techniques in supporting the reliability and security of digital documents. It is hoped that this research can make a valuable contribution to the development of forensic techniques.

Keywords: *digital forensic, NIJ, Exiftools, PCA, forgery*

Abstrak

Dengan pesatnya pertumbuhan teknologi informasi dan komunikasi, kebutuhan akan keamanan pendekatan digital forensik yang canggih menjadi semakin mendesak. Masalah yang perlu diselesaikan menggunakan langkah digital forensik adalah inidkasi adanya perubahan dan pemalsuan dokumen yang berekstensi .pdf. Dengan melibatkan berbagai metode analisis forensik, seperti pemeriksaan metadata, pengamatan fisik, nilai hash, analisis menggunakan Principal Component Analysis (PCA), dan penggunaan alat forensik seperti Adobe Acrobat Reader, Exiftools, imageforensic.org dan HashMyFIle diharapkan dapat menangani kasus kejahatan yang ada. Penelitian ini bertujuan mempelajari tantangan yang ditimbulkan oleh dokumen digital, menekankan perlunya pendekatan inovatif untuk mengungkap informasi tersembunyi, mendeteksi perubahan, dan mengautentikasi integritas file PDF. Gabungan metode NIJ dan Analisis menggunakan PCA menghasilkan analisis yang akurat dan tepat terlihat dari kemampuan pengurangan dimensi PCA. Hasil penelitian menunjukkan bahwa metode NIJ dan analisis PCA

dapat digunakan untuk membuktikan keaslian suatu dokumen PDF dengan ditemukannya perubahan pada dokumen PDF tersebut. Selain itu, penelitian ini juga memberikan rekomendasi untuk pengembangan teknik forensik dalam mendukung keandalan dan keamanan dokumen digital. Penelitian ini diharapkan dapat memberikan sumbangsih yang signifikan terhadap kemajuan teknik forensik..

Kata Kunci: *digital forensik, NIJ, Exiftools, PCA, pemalsuan*

1. PENDAHULUAN

Keaslian citra memegang peranan penting karena jika suatu citra dimanipulasi, informasi yang disampaikan sebagai informasi visual dapat berubah [1]. Penyebaran gambar digital yang dibuat oleh pihak lain untuk kepentingan pribadi atau kolektif telah menimbulkan kerugian yang cukup besar bagi semua pihak, baik individu maupun organisasi. Karena gambar digital dapat dijadikan berita atau bukti isu sosial yang autentik. Banyak tujuan berbeda yang dapat digunakan dalam manipulasi gambar digital, termasuk penjahat untuk menipu penyidik. Misalnya, dalam kasus pornografi, gambar yang direkayasa dapat merusak nama dan reputasi seseorang, bahkan perusahaan [2].

Dengan bantuan teknologi yang terus berkembang, termasuk forensik digital, kejahatan tersebut dapat diatasi. Forensik digital merupakan salah satu cabang ilmu yang bertujuan untuk mengumpulkan informasi dan menyelidiki barang bukti digital agar dapat dijadikan bukti yang sah di hadapan hukum. [3]. Forensik digital melibatkan penangkapan bukti digital secara ilmiah sehingga dapat digunakan sebagai bukti [4]. Contoh pemalsuan dokumen sebagaimana dalam perkara dibawah ini, terdakwa RUSDI HARDANTO SUHARGO alias RUSDI Bin SUHARGO melakukan perbuatan yang disengaja dan melawan hukum dengan memanipulasi, membuat, mengubah, menghilangkan, memusnahkan informasi elektronik seperti dokumen elektronik dengan tujuan menjadikan informasi elektronik dan dokumen lektronik tersebut dianggap seolah-olah sebagai data otentik.

Di antara berbagai jenis dokumen yang dapat dimanipulasi, format file PDF adalah yang paling umum digunakan untuk menyimpan informasi guna mempermudah akses dan tampilan. [5], sehingga rentan terhadap serangan karena dapat dengan mudah dimanipulasi menggunakan perangkat lunak yang dapat diakses secara gratis melalui jaringan Internet. Contoh perangkat lunak yang digunakan seperti *Adobe Acrobat Reader, Foxit PhantomPDF*, dan perangkat lunak lainnya [6].

Hal ini diperkuat dengan data dari Pusiknas Bareskrim Polri menunjukkan 95 tindak pidana yang melibatkan pemalsuan dokumen dan surat asli. Rata-rata, polisi harus menangani tujuh tindak pidana pemalsuan dokumen dan surat asli setiap harinya. Data diambil pada tanggal 1 hingga 12 Januari 2022 [7]. Dengan rentannya pemalsuan dokumen yang ada analisis forensik pemalsuan dokumen dapat menjadi solusi ideal dalam situasi seperti ini karena menganalisis dokumen identifikasi pengguna melalui pemeriksaan ilmiah dan tidak memberikan ruang bagi penjahat [8]. Keunggulan dari analisis forensik dalam praktik hukum pidana yaitu dapat menemukan kebenaran dan keadilan bahkan untuk kasus lama sekalipun [9].

Untuk mendukung metode pengembangan, dipilihlah salah satu teknik analisis *Principal Component Analysis (PCA)* yang merupakan teknik yang digunakan dalam statistik dan analisis data untuk mengurangi ukuran kumpulan data sambil tetap mempertahankan informasi penting [10]. *PCA* bekerja dengan cara mengidentifikasi pola pada data dan menemukan hubungan antar variabel yang ada [11]. Dari sudut pandang praktis, analisis komponen utama bertujuan untuk mengubah sebagian besar variabel yang awalnya digunakan dan berkorelasi satu sama lain menjadi kumpulan variabel independen baru yang lebih kecil (yang tidak lagi berkorelasi) [12]. Penelitian ini akan dilakukan dengan dengan menggunakan alat salah satunya yaitu *Exiftools* dan *imageforensic.org*. Kedua tools ini merupakan aplikasi yang memungkinkan untuk menganalisis dokumen PDF untuk membuktikan apakah dokumen tersebut telah diedit atau masih dalam keadaan asli belum memberikan akses pada metadata [13]. Metadata mungkin berisi data pribadi seperti garis lintang dan bujur (Lokasi GPS), tanggal pembuatan dan modifikasi, atau nama penulis [14].

Penelitian yang dilakukan Desti Mualfah, Afdel Viransa, dan Hasanatul Fu'adah Amran [15] mengkaji analisis keamanan *browser* untuk mengakses media sosial memakai metodologi NIJ (*National Institute of Justice)*). Penelitian ini bertujuan untuk menerapkan forensik secara langsung pada keamanan *browser* untuk mengakses jejaring sosial *Facebook* dan *Instagram.* Tujuannya adalah untuk menemukan bukti digital dari analisis yang dilakukan melalui *browser*. Hasil penelitian ini Hasil penelitian ini menunjukkan bahwa *Google Chrome, Mozilla Firefox* dan *Microsoft Edge* tidak aman saat mengakses jejaring sosial *Facebook*. Sementara Mozilla Firefox adalah yang paling aman untuk mengakses jejaring sosial Instagram. Data yang diperoleh dalam penelitian ini dikumpulkan dengan menggunakan alat pencitraan *FTK*.

Penelitian yang dilakukan Yuwono, Fadlil, dan Sunardi [16] bertujuan untuk menguji perbandingan kinerja *software* forensik yang bertujuan untuk *file carving*. Tujuan dari penelitian ini adalah untuk dapat memperoleh barang bukti dengan menggunakan *dead forensic* dan *live forensic*. Forensik kematian memerlukan data disimpan secara permanen pada perangkat penyimpanan (*hard drive*). Investigasi langsung menganalisis apa yang berjalan pada sistem atau data volatil yang disimpan dalam *RAM* atau dikirimkan melalui jaringan. File yang dibuat berada dalam aliran data menggunakan pengetahuan tentang metadata format filenya. Tipe file yang dikembalikan adalah tipe gambar *JPG, JPEG* dan *PNG,* serta dokumen *Doc, Docx* dan *PDF*.

Pada penelitian yang dilakukan oleh Endina Putri Purwandari [17], Penelitian ini membahas penggunaan *Principal Component Analysis (PCA)* dalam pengenalan sketsa wajah untuk aplikasi forensik. Tujuan dari penelitian ini adalah mengenali gambar wajah dari gambar sketsa pensil dengan mengekstraksi fitur menggunakan *PCA* dan menghitung jarak *Euclidean* antara gambar uji dan gambar latih. Penelitian ini menyimpulkan bahwa aplikasi ini dapat membantu dalam mencocokkan data sketsa dengan foto wajah untuk identifikasi kriminal. Namun, beberapa faktor yang masih dapat mempengaruhi hasil pengenalan sketsa wajah, seperti lingkungan pengambilan gambar dan kualitas gambar sketsa [18].

Pada penelitian yang dilakukan oleh Muhammad Adil Kustian [19] membahas analisis forensik menggunakan fungsi hash untuk menentukan keaslian video, metadata gambar, dan *magic number file*. Penulis menggunakan tiga alat yaitu *Forevid, ExifTool*, dan *WinHex* untuk menganalisis dan menentukan keaslian file. Eksperimen melibatkan perbandingan metadata, hash, dan magic number dari dokumen asli dengan file yang dimanipulasi. Hasilnya menunjukkan bahwa alat-alat ini dapat menemukan file forensik yang diperlukan dalam proses forensik. Artikel ini juga memberikan gambaran tentang fungsi *hash*, metadata, dan *magic number*, serta fungsi dan penggunaan ketiga alat tersebut.

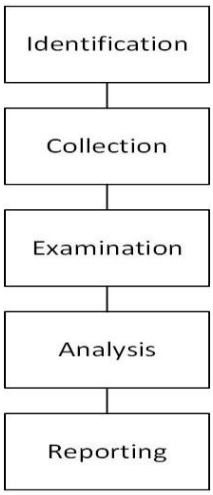
Oleh karena itu, analisis forensik dokumen PDF memanfaatkan *National Institute of Justice (NIJ)* diharapkan dapat membantu menentukan apakah dokumen PDF telah dimanipulasi atau tidak. Seperti diungkapkan pada artikel Steven Marcellino [20], Penggunaan pendekatan penelitian ini diadaptasi dari Metodologi Analisis Forensik *National Institute of Justice (NIJ)*. Pendekatan ini digunakan untuk menjelaskan bagaimana melakukan langkah-langkah penelitian agar proses penelitian dapat selesai secara sistematis dan dapat dijadikan pedoman dalam memecahkan permasalahan yang ada [21]. Hal ini didukung dengan adanya *identification, collection, examination, analysis, reporting* yang setiap tahapannya lebih terstruktur membuatnya lebih efisien [22].

Diharapkan bahwa jurnal penelitian ini diharapkan mampu memberikan pengaruh yang berharga terhadap pengembangan teknik torensik untuk mendeteksi perubahan dan pemalsuan dokumen PDF, sehingga dapat meningkatkan keandalan dan keamanan data digital dalam berbagai konteks, termasuk hukum, bisnis, dan keamanan informasi.

2. METODE PENELITIAN

Dalam penelitian ini, kami mengadopsi dan menerapkan metode analisis forensik dari *National Institute of Justice (NIJ)*. Metode ini menguraikan langkah-langkah penelitian yang akan ditempuh agar proses dan alur penelitian dapat diketahui secara sistematis sehingga dapat digunakan sebagai acuan dalam mengungkap masalah yang ada.[23]. Langkah-langkah metode *National Institute of Justice*

(NIJ) terbagi dalam beberapa tahap, yaitu *identification, collection, examination, analysis,* dan *reporting*.



Gambar 1: Alur Metode NIJ

2.1 Metode Penelitian

Penulis mengadaptasi dan menerapkan metode National Institute of Justice (NIJ) guna menjelaskan tahapan penyelidikan secara sistematis proses, sehingga metode tersebut menjadi rujukan dalam menyelesaikan permasalahan yang ada [20]. Penjelasan langkah-langkah pada metode NIJ adalah sebagai berikut:

2.1.1 *Identification*

Pada tahap ini penulis melakukan kegiatan seleksi berkas dan mengklasifikasikan bukti-bukti kasus kejahatan digital berupa file dokumen PDF untuk membantu penyidikan mengungkap bukti-bukti kasus kejahatan dunia maya. Menurut Sunardi, Iman Riadi dan Joko Triyanto pada tahap ini akan diperoleh gambaran lengkap tentang identifikasi dan pendataan untuk mengamankan data barang bukti secara lengkap [24].

2.1.2 *Collection*

Pada tahap ini mengumpulkan data bukti guna merangsang pencarian investigasi untuk bukti digital kejahatan. Langkah ini mencakup proses pengambilan data dari sumber data yang akurat dan menjaga keaslian bukti digital perubahan. Pengambilan dilakukan melalui studi kasus, eksperimen, dan observasi. Penelitian ini menggunakan barang bukti berupa dokumen PDF [25].

Gambar 2: Barang Bukti Dokumen PDF

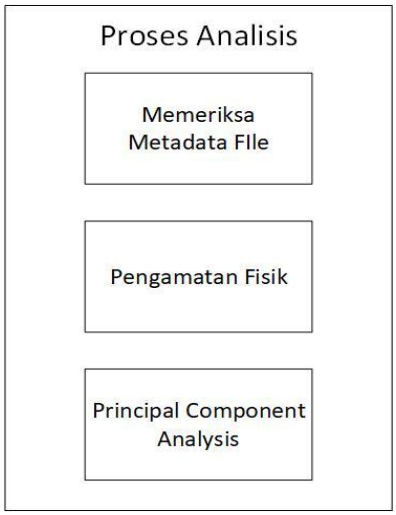
2.1.3 *Examination*

Tahap *examination* dilakukan dengan validasi terhadap data yang diperoleh secara forensik pada tahap sebelumnya, serta memastikan bahwa data yang diperoleh dalam bentuk file adalah asli dan sesuai dengan data yang diperoleh pada situasi kasus kejahatan di lapangan. Oleh karena itu, file digital hasil ekstraksi harus dilakukan validasi menggunakan teknik *hashing* [15]. Metode hashing adalah teknik menambah, menghapus, dan mencari data dengan menelusuri alamat kunci yang diperoleh dari aturan fungsi untuk mendapatkan suatu data yang valid [26].

2.1.4 *Analysis*

Tahapan ini dilakukan dengan tujuan menganalisis hasil pemeriksaan bukti digital berupa file .pdf dari hasil yang sudah diketahui metadata dan nilai hashnya [3]. Pada penelitian ini, dilakukan analisis sebagai berikut:

a. Memeriksa metadata file yang akan diperiksa keasliannya. Analisis metadata ini dilakukan di awal untuk mengetahui detail tentang sumber file. Poin yang diamati adalah *MAC (Modification Time, Access Time* dan *Creation Time)*.
b. Melakukan observasi fisik dan melakukan penilaian awal terhadap adanya kejanggalan yang ditemukan pada surat tersebut.
c. Melakukan *PCA* untuk memeriksa metadata, pengamatan fisik dan analisis *PCA*.



Gambar 3: Tahap Proses Analisis

2.1.5 *Report*

Tahap Reporting dilaksanakan setelah bukti digital dikumpulkan pada tahap pemeriksaan dan analisis. Pada tahap ini, hasil analisis akan dilaporkan, termasuk menjelaskan tindakan yang dilakukan dan memberikan rekomendasi untuk perbaikan kebijakan, metode, alat, atau aspek pendukung lain didalam proses investigasi digital.[15].

2.2 Alat Penelitian

Alat penelitian yang digunakan di penelitian ini meliputi perangkat lunak yang dapat mengakses metadata dan dapat mendeteksi perubahan pada dokumen baik secara fisik maupun yang membutuhkan kemampuan yang spesifik yang dapat mengakses *Principal Componen Analysis (PCA)* seperti pada Tabel 1 dibawah ini

Tabel 1: Alat Penelitian digunakan untuk membantu penelitian

No	Perangkat Lunak Forensik	Deskripsi
1	Acrobat Reader	Salah satu dari berbagai jenis perangkat lunak yang dapat digunakan untuk membaca, mencatat, mencari, memverifikasi, menandai secara digital, dan mencetak data dalam format PDF yang dikeluarkan oleh Adobe.
2	Exiftools	*ExifTool adalah perangkat lunak gratis dan sumber terbuka yang digunakan untuk membaca, menulis, dan memodifikasi metadata.*
3	imageforensic.org	*Website* yang digunakan pada bidang digital forensik untuk analisis dokumen dan gambar
4	HashMyFile	HashMyFile adalah utilitas ringan dari NirSoft untuk menghitung hash file seperti MD5, SHA-1, SHA-256, dan CRC32. Alat ini berguna untuk memverifikasi integritas file, mendeteksi perubahan, membantu forensik digital, serta membandingkan file yang sama.

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

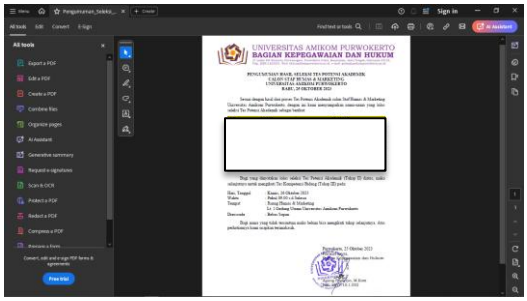
Bagian ini berisi uraian mengenai data hasil penelitian yang telah dipaparkan.

1. Identification

Langkah pertama dalam pendekatan Forensik *NIJ* adalah Identifikasi. Proses yang dilakukan pada tahap ini meliputi identifikasi barang bukti file dokumen dan permasalahan yang perlu dipecahkan. Permasalahan penelitian ini adalah bagaimana memecahkan masalah analisis forensic untuk mendeteksi perubahan dan pemalsuan dokumen PDF.

2. Collection

Pada tahap ini, peneliti melanjutkan proses pengumpulan file bukti yang dianalisis berupa file PDF yang memiliki satu halaman yang berisi Pengumuman Hasil Seleksi Tes Potensi Akademik Calon Staf Humas & Marketing Universitas Amikom Purwokerto yang di upload oleh *official website* pada tanggal 30 Oktober 2023.



Gambar 4: *Collection Document*

Ekstensi yang digunakan dari barang bukti adalah ".pdf", selanjutnya melakukan penilaian hash yang dapat dilihat pada Gambar 5.

```
Filename          : Pengumuman_Seleksi_TPA_-_Calon_Staf_Humas_Marketing.pdf
MD5               : d104da5b392476526a6c1dcc351de7dc
SHA1              : f414bb050b3f19f57451cdaf3335d3451d783973
CRC32             : 3df1ba54
SHA-256           : 5b3e98b9f4029f633c71293d39f74ed79c6d2c2337f9c0045f1cfe7a09b13e84
SHA-512           : 78dc99c68f692cbaa74e2d2c8d3a33a5785078fde1872530ffe0e62595f2c574
                    eb8174282b7acfefe1542ae6f7b0499587e917e1cba5b9105ba6f62fef726329
SHA-384           : e773ea481ae42fabdaa1b8d8073ef7e662449f2cbf342efb0cf3e7711a0d5e97
                    15503111ded8b5e2f6d07df763a61816
Full Path         : D:\apk\hashmyfiles-x64\Pengumuman_Seleksi_TPA_-_Calon_Staf_Humas
                    _Marketing.pdf
Modified Time     : 10/25/2023 8:30:22 PM
Created Time      : 2/18/2025 7:20:56 PM
Entry Modified Time: 2/18/2025 7:21:25 PM
File Size         : 578,201
File Version      :
Product Version   :
Identical         :
Extension         : pdf
File Attributes   : A
Hash Start Time   : 2/18/2025 7:27:24 PM
Hash End Time     : 2/18/2025 7:27:24 PM
Hashing Duration  : 00:00:00.040
```

Gambar 5: Nilai Hash

Hashing adalah teknik yang digunakan untuk menerima string yang panjangnya sembarang dan menghasilkan konversi string dengan panjang yang tetap. Algoritma MDS, SHA1, CRC32, SHA-256, SHA-512 dan SHA-384 digunakan pada kasus ini.

3. Examination

Proses eksaminasi (pemisahan dan penjagaan integritas barang bukti dilakukan dengan memisahkan dan membuat *soft copy* barang bukti berformat pdf dan analisis dilakukan menggunakan *soft copy* barang bukti supaya integritas barang bukti tetap terjaga dan dapat digunakan kembali apabila dibutuhkan.

4. Analysis

Proses analisa dilakukan dengan beberapa tahapan yaitu :

4.1. Memeriksa Metadata

Analisis metadata dilakukan untuk mengetahui detail sumber file, khususnya *Change Time* (Tanggal Modifikasi), *Access time, Birth Time* (Tanggal Dibuat).

Group	Tag	Value
ExifTool	ExifTool Version Number	12.69
File	File Name	Pengumuman_Seleksi_TPA_-_Calon_Staf_Humas_Marketing.pdf
File	Directory	D:/kiki/kuliah/kij/New folder
File	File Size	582 kB
File	File Modification Date/Time	2023:11:02 20:21:10+07:00
File	File Access Date/Time	2023:11:02 20:22:40+07:00
File	File Creation Date/Time	2023:11:02 20:21:10+07:00
File	File Permissions	-rw-rw-rw-
File	File Type	PDF
File	File Type Extension	pdf
File	MIME Type	application/pdf
PDF	PDF Version	1.7
PDF	Linearized	Yes
PDF	Author	
PDF	Create Date	2023:10:25 15:06:26+07:00
PDF	Modify Date	2023:11:02 20:21:10+07:00
PDF	Producer	Microsoft: Print To PDF
PDF	Title	Microsoft Word - Pengumuman Administrasi
PDF	Page Count	1
XMP	XMP Toolkit	Adobe XMP Core 9.1-c001 79.2a0d8d9, 2023/03/14-11:19:46
XMP	Format	application/pdf
XMP	Creator	
XMP	Title	Microsoft Word - Pengumuman Administrasi
XMP	Create Date	2023:10:25 15:06:26+07:00
XMP	Modify Date	2023:11:02 20:21:10+07:00
XMP	Metadata Date	2023:11:02 20:21:10+07:00
XMP	Producer	Microsoft: Print To PDF
XMP	Document ID	uuid:84ecc6c5-16d9-45d3-b8fa-0d6f00e8504b
XMP	Instance ID	uuid:594bea80-e0c2-4eb1-9dbe-379540a45911

Gambar 6: Hasil Analisis Metadata

Berdasarkan hasil peninjauan metadata yang ditunjukkan pada Gambar 6 terdapat beberapa bagian yang perlu diperhatikan tabel berikut:

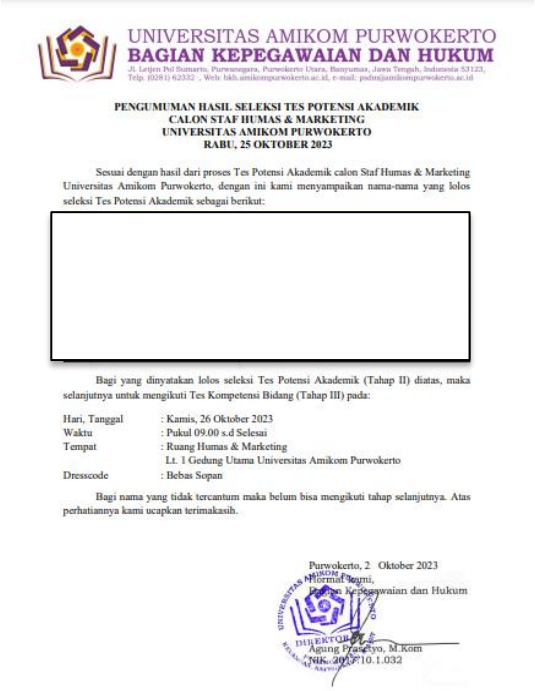
Tabel 2: Metadata

No	Jenis Metadata	Deskripsi
1	Birth Time (Create)	2023:10:25 15:06:26+07:00
2	Access Time	2023:11:02 20:22:40+07:00
3	Change Time (Modify)	2023:11:02 20:21:10+07:00
4	Metadata Date	2023:11:02 20:21:10+07:00
5	Producer	Microsoft Print To PDF

Berdasarkan metadata pada Gambar 6 dan Tabel 2, file yang bersangkutan dibuat pada tanggal 25 Oktober 2023 pukul 15:06:26+07:00 dan *modify date* terakhir pada tanggal 2 November 2023 pukul 20:21:10+07:00 dan dapat diasumsikan merupakan hasil scan dari *Microsoft print* to pdf.

4.2 Melakukan Pengamatan Fisik

Pada tahapan ini dilakukan untuk pengecekan awal apabila ditemukan kejanggalan pada bagian dokumen yang berasal dari website student.amikompurwokerto.ac.id pada tanggal 30 Oktober 2023 yang berisi Pengumuman Hasil Seleksi Tes Potensi Akademik Calon Staf Humas & Marketing Universitas Amikom Purwokerto. Hasil observasi fisik berupa temuan pendeteksian kejanggalan pada dokumen bukti disajikan pada Gambar 7:



UNIVERSITAS AMIKOM PURWOKERTO
BAGIAN KEPEGAWAIAN DAN HUKUM

PENGUMUMAN HASIL SELEKSI TES POTENSI AKADEMIK
CALON STAF HUMAS & MARKETING
UNIVERSITAS AMIKOM PURWOKERTO
RABU, 25 OKTOBER 2023

Sesuai dengan hasil dari proses Tes Potensi Akademik calon Staf Humas & Marketing Universitas Amikom Purwokerto, dengan ini kami menyampaikan nama-nama yang lolos seleksi Tes Potensi Akademik sebagai berikut:

Bagi yang dinyatakan lolos seleksi Tes Potensi Akademik (Tahap II) diatas, maka selanjutnya untuk mengikuti Tes Kompetensi Bidang (Tahap III) pada:

Hari, Tanggal : Kamis, 26 Oktober 2023
Waktu : Pukul 09.00 s.d Selesai
Tempat : Ruang Humas & Marketing
Lt. 1 Gedung Utama Universitas Amikom Purwokerto
Dresscode : Bebas Sopan

Bagi nama yang tidak tercantum maka belum bisa mengikuti tahap selanjutnya. Atas perhatiannya kami ucapkan terimakasih.

Purwokerto, 2 Oktober 2023
Hormat kami,
Kepala Kepegawaian dan Hukum

Agung Prasetyo, M.Kom
NIK. 2007.10.1.032

Gambar 7. Bukti Dokumen

Dari Gambar 7 terdapat beberapa kejanggalan pada dokumen tersebut yang berhasil diidentifikasi, untuk lebih lanjut terdapat penjelasan atas kejanggalan yang terdapat pada dokumen dilihat pada Tabel 3 :

Tabel 3: Pengamatan Fisik

Temuan Awal	**Objek Temuan**
Ada imbuhan tandatangan pada surat tersebut yang tidak diketahui oleh pemilik dan kemungkinan tandatangan tersebut merupakan hasil salinan elektronik dan bukan tandatangan langsung.	Paraf
Terdapat pemudaran warna pada kop surat tepatnya pada bagaian akhir nomor telefon den kemungkinan orang lain sengaja menutupi bagian nomor tersebut	Nomor Telefon

4.3 Proses Analisis Menggunakan PCA

Terdapat sebuah dokumen pdf yang bisa dianalisa untuk mencari tahu apakah terdapat manipulasi pada dokumen digital tersebut. Pada gambar dibawah ada beberapa bagian yang tidak konsisten setelah dilakukan *PCA* antara lain :

1. Terdapat titik putih yang menumpuk pada bagian stempel.
2. Warna pada akhir nomor telefon kop surat yang memudar.
3. Pada tanggal ditandatangani terdapat spasi yang lebih lebar dengan menggunakan 2 spasi dibandingkan dengan kata lain yang hanya terdapat 1 spasi hal ini bisa jadi terdapat perubahan dengan cara menghapus tanggal tersebut.
4. Dan pada bagian paraf terdapat garis lurus kesamping yang jika diperhatikan pada gambar garis tersebut tidak pecah hal ini bisa jadi terdapat penambahan garis pada paraf tersebut.

Untuk memperjelas hasil Analisa menggunakan *Principal Component Analysis (PCA)* dapat dilihat pada Gambar 8.

UNIVERSITAS AMIKOM PURWOKERTO
BAGIAN KEPEGAWAIAN DAN HUKUM

PENGUMUMAN HASIL SELEKSI TES POTENSI AKADEMIK
CALON STAF HUMAS & MARKETING
UNIVERSITAS AMIKOM PURWOKERTO
RABU, 25 OKTOBER 2023

Sesuai dengan hasil dari proses Tes Potensi Akademik calon Staf Humas & Marketing Universitas Amikom Purwokerto, dengan ini kami menyampaikan nama-nama yang lolos seleksi Tes Potensi Akademik sebagai berikut:

Bagi yang dinyatakan lolos seleksi Tes Potensi Akademik (Tahap II) diatas, maka selanjutnya untuk mengikuti Tes Kompetensi Bidang (Tahap III) pada:

Hari, Tanggal : Kamis, 26 Oktober 2023
Waktu : Pukul 09.00 s.d Selesai
Tempat : Ruang Humas & Marketing
Lt. 1 Gedung Utama Universitas Amikom Purwokerto
Dresscode : Bebas Sopan

Bagi nama yang tidak tercantum maka belum bisa mengikuti tahap selanjutnya. Atas perhatiannya kami ucapkan terimakasih.

Purwokerto, 2 Oktober 2023
Hormat kami,
Kepala Kepegawaian dan Hukum

Agung Prasetyo, M.Kom
NIK. 2007.10.1.032

Gambar 8. Hasil PCA

5. Reporting

Analisis forensik yang dilakukan mengungkapkan bahwa surat-surat tersebut diduga telah dimanipulasi berdasarkan prosedur dan teknik, antara lain pemeriksaan dan pengamatan fisik yang dilakukan menggunakan *software Adobe Acrobat Reader*, pemeriksaan

dan pengamatan metadata menggunakan *software Exiftools*, serta pemeriksaan analisis komponen utama menggunakan *imageforensic.org.*

4. KESIMPULAN

Hasil penelitian menunjukkan bahwa dengan mengadaptasi metode *National Institute of Justice (NIJ)* dan *Principal Component Analysis (PCA)* dapat digunakan untuk membuktikan keaslian suatu gambar atau image dan file, dibuktikan dengan simulasi menggunakan file PDF terlihat banyak titik putih menumpuk di beberapa tempat seperti stempel, warna pada akhir nomor telepon memudar, pada tanggal ditandatangani mempunyai spasi yang lebih luas dengan menggunakan 2 spasi dan pada bagian paraf terdapat garis lurus kesamping yang jika diperhatikan pada gambar garis tersebut tidak pecah. Hasil analisis dan investigasi yang dilakukan menunjukkan bahwa hasil pengujian yang dilakukan dengan Fotoforensik cukup memuaskan dengan ditemukannya beberapa kejanggalan yang berusaha memanipulasi file.

Kekurangan dari penggunaan metode NIJ adalah masih menggunakan pendekatan manual atau semi-otomatis dan penggunaan software yang cukup kuno, yang mana kurang efektif dibandingkan dengan metode digital yang menggunakan kecerdasan buatan atau AI untuk mendeteksi pemalsuan PDF. Penelitian selanjutnya dapat dikembangkan dengan melakukan perbandingan dengan alat forensik dan metode yang lain.

DAFTAR PUSTAKA

[1] M. Badri, "Analisis Forensik Originalitas Gambar Menggunakan Autopsy Dan Opencv," *J. Satya Inform.*, vol. 8, no. 01, pp. 43–49, 2023, doi: 10.59134/jsk.v8i01.236.

[2] I. Irwansyah and H. Yudiastuti, "Analisis Digital Forensik Rekayasa Image Menggunakan Jpegsnoop Dan Forensically Beta," *J. Ilm. Matrik*, vol. 21, no. 1, pp. 54–63, 2019, doi: 10.33557/jurnalmatrik.v21i1.518.

[3] K. N. Isnaini, H. Ashari, and A. P. Kuncoro, "Analisis Forensik untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode NIST," *J. Resist.*, vol. 3, no. 2, pp. 72–81, 2020, doi: https://doi.org/10.31598.

[4] I. Faisal, A. Budiman, and E. I. Fitiria, "Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Aplikasi Snack Video," vol. 2, no. 2, pp. 390–399.

[5] Ben Liu, "Apa Arti Format PDF," *KOFAX*. p. 1, 2021. [Online]. Available: https://www.kofax.com/learn/blog/what-does-pdf-format-mean

[6] N. Perdana, "11 perangkat lunak markup PDF gratis terbaik di pasaran pada tahun 2023," *FILESTAGE*. p. 1, 2023. [Online]. Available: https://filestage.io/blog/free-pdf-markup-software/

[7] P. B. Polri., "Rata-rata, Tujuh Kasus Pemalsuan Surat Ditangani Polri," *Pusiknas Bareskrim Polri.* p. 1, 2022. [Online]. Available: https://pusiknas.polri.go.id/detail_artikel/rata-rata,_tujuh_kasus_pemalsuan_surat_ditangani_polri

[8] R. M, "Forensic Document Forgery Analysis – A Landmark Approach To Curb Identity Fraud," *ShuftiPro*. p. 1, 2022. [Online]. Available: https://shuftipro.com/blog/forensic-document-forgery-analysis-a-landmark-approach-to-curb-identity-fraud/

[9] C. Khairunnisa and Zulfan, "Manfaat Ilmu Forensik dalam Hukum Pidana," *CENDEKIA J. Hukum, Sos. Hum.*, vol. 1, no. 1, pp. 1–12, 2023.

[10] W. Astuti and A. Adiwijaya, "Principal Component Analysis Sebagai Ekstraksi Fitur Data Microarray Untuk Deteksi Kanker Berbasis Linear Discriminant Analysis," *J. Media Inform. Budidarma*, vol. 3, no. 2, p. 72, 2019, doi: 10.30865/mib.v3i2.1161.

[11] D. A. Nugraha and A. S. Wiguna, "Seleksi Fitur Warna Citra Digital Biji Kopi Menggunakan Metode Principal Component Analysis," *Res. Comput. Inf. Syst. Technol. Manag.*, vol. 3, no. 1, p. 24, 2020, doi: 10.25273/research.v3i1.5352.

[12] F. Badri and S. U. R. Sari, "Penerapan Metode Principal Component Analysis (PCA) Untuk Identifikasi Faktor-Faktor yang Mempengaruhi Sikap Mahasiswa Memilih Melanjutkan Studi ke Kota Malang," *Build. Informatics, Technol. Sci.*, vol. 3, no. 3, pp. 426–431, 2021,

doi: 10.47065/bits.v3i3.1139.
[13] F. Harahap, "Deteksi Foto Manipulasi Dengan Tools Forensicallybeta dan Imageforensic . org Dengan Metode Error Level Analysis (ELA)," *TIN Terap. Inform. Nusant.*, vol. 2, no. 3, pp. 159–164, 2021, [Online]. Available: https://ejurnal.seminar-id.com/index.php/tin/article/view/859
[14] androideity, "ExifTool adalah editor metadata sumber terbuka dan lintas platform," *androideity*. p. 1, 2020. [Online]. Available: https://id.androideity.com/select-random-file-windows-explorer
[15] D. Mualfah, A. Viransa, and H. F. Amran, "Akuisisi Bukti Digital Pada Aplikasi Tamtam Messenger Menggunakan Metode National Institute of Justice," *J. Softw. Eng. Inf. Syst.*, vol. 3, no. 1, 2021, doi: 10.37859/seis.v3i1.4548.
[16] D. T. Yuwono, A. Fadlil, and S. Sunardi, "Performance Comparison of Forensic Software for Carving Files using NIST Method," *J. Teknol. dan Sist. Komput.*, vol. 7, no. 3, pp. 89–92, 2019, doi: 10.14710/jtsiskom.7.3.2019.89-92.
[17] E. P. Purwandari, A. Erlansari, A. Wijanarko, and E. A. Adrian, "Face sketch recognition using principal component analysis for forensics application," *J. Teknol. dan Sist. Komput.*, vol. 8, no. 3, pp. 178–184, 2020, doi: 10.14710/jtsiskom.2020.13422.
[18] S. Mamis, I. N. A. S. Putra, and I. M. M. Yusa, *Dasar-dasar Desain Komunikasi Visual*. 2023.
[19] M. A. Kustian, M. Informatika, and U. I. Indonesia, "Hash Dalam Menentukan Keaslian Video , Metadata Image Dan Magic," vol. 2, pp. 10–16, 2023.
[20] S. Marcellino, H. B. Seta, and I. W. Widi, "Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute of Justice (NIJ)," *Inform. J. Ilmu Komput.*, vol. 19, no. 2, pp. 141–156, 2023, doi: 10.52958/iftk.v19i2.4676.
[21] Y. Arif, E. I. Alwi, and M. A. Asis, "Analisis Bukti Digital Direct Message Pada Twitter Menggunakan Metode National Institute Of Justice (NIJ)," vol. 8, no. 2, pp. 165–174, 2023.
[22] S. Soni, Y. Fatma, and R. Anwar, "Akuisisi Bukti Digital Aplikasi Pesan Instan 'Bip'Menggunakan Metode National Institute Of Justice (NIJ)," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 3, no. 1, pp. 34–42, 2022, doi: 10.37859/coscitech.v3i1.3694.
[23] I. Gunawan, "Analisis Keamanan Aplikasi Android Non Playstore Dengan Metode Digital Forensik Pendekatan Statis Dan Dinamis," *Simetris*, vol. 15, no. 2, pp. 29–34, 2021, doi: 10.51901/simetris.v15i2.225.
[24] I. Riadi, J. Triyanto, and J. L. P. Soepomo, "Analisis Forensik Layanan Signal Private Messenger pada Smartwatch Menggunakan," *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 3, pp. 305–313, 2021.
[25] S. Sunardi, I. Riadi, and J. Triyanto, "Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice," *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 6, no. 2, p. 63, 2021, doi: 10.31328/jointecs.v6i2.2315.
[26] M. Syahrir and F. Fatimatuzzahra, "Association Rule Integrasi Pendekatan Metode Custom Hashing dan Data Partitioning untuk Mempercepat Proses Pencarian Frekuensi Item-set pada Algoritma Apriori," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 20, no. 1, pp. 149–158, 2020, doi: 10.30812/matrik.v20i1.833.