

Bab 4 Hasil dan Pembahasan

4.1 Implementasi Sistem

Dalam bab ini akan dilakukan implementasi sistem, yakni mulai pembuatan program aplikasi metadata forensik dengan membaca dan korelasi metadata file menggunakan bahasa pemrograman Java Kompiler Netbeans IDE 8.0. Program ini disebut metadata forensik, karena mampu membaca metadata setiap file dan mampu menemukan file berdasarkan korelasi setiap metadatanya. Hasil dari pembuatan program ini akan diimplementasikan pada beberapa file yang ada didalam komputer yang sudah ditentukan.

4.1.1 Jenis Komputer dan Sistem Operasi

Komputer / laptop yang digunakan dalam pengujian metode sistem metadata forensik ini adalah Laptop merk HP, berikut spesifikasinya:

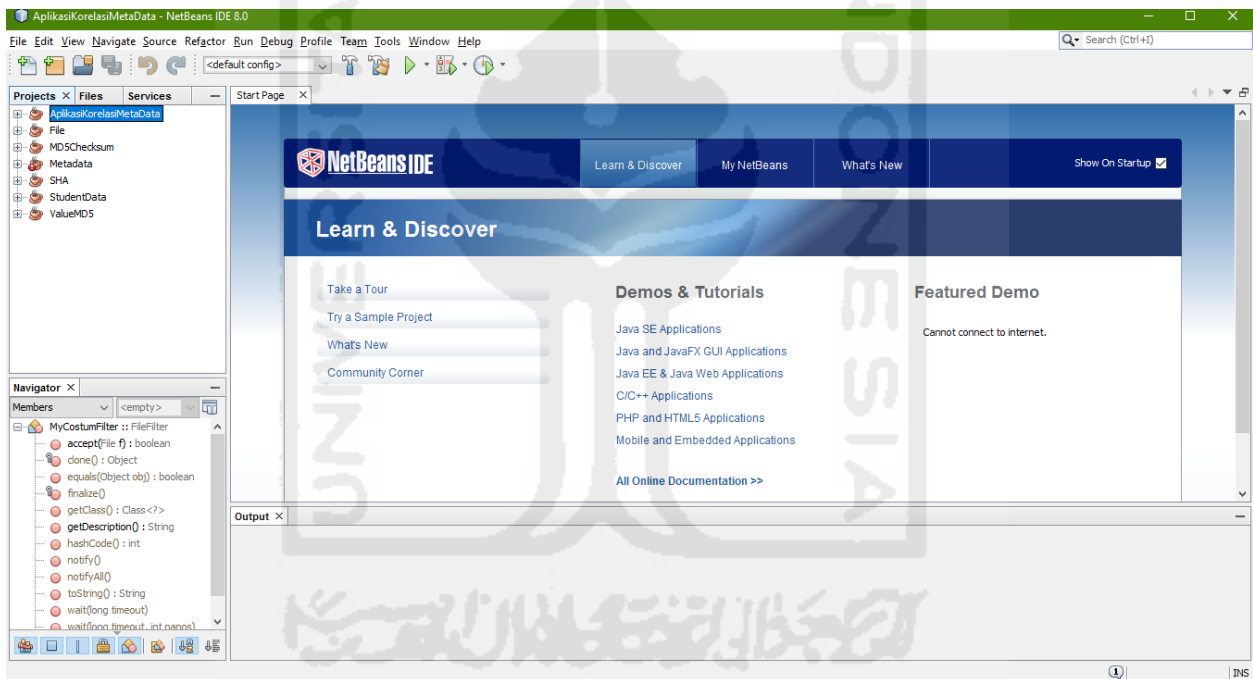
Tabel 4. 1 Spesifikasi Laptop HP

Resolusi Layar	1366 x 768
Ukuran Layar	14 FULL HD
Tipe Layar	Active Matrix TFT Color LCD
CPU	Intel® Core i3 2.40 GHz
Memori/RAM	6 GB DDR 3
Harddisk	500 GB
DVD	DVD Writer
Koneksi	Bluetooth 4.0 + HS, Wi-Fi, Gigabit Internet
Microphone	Ya
Port USB	USB 3.0 Terbaru!
Webcam	Ya Webcam terintegrasi
HDMI	Ya (untuk LCD projector)
Flash Kamera	Ya
Baterai	Lithium Ion (Li-Ion)
Berat	2.2 Kilogram

Sedangkan Sistem Operasi yang digunakan dalam komputer ini adalah jenis Sistem Operasi Windows 10. Sistem Operasi Windows 10 adalah Sistem Operasi yang dikembangkan oleh Microsoft Corporation yang menggunakan antarmuka dengan berbasis GUI (Graphical User Interface) atau tampilan antarmuka bergrafis pada umumnya sistem operasi ini banyak sekali digunakan oleh masyarakat, dari kalangan menengah ke atas hingga ke bawah.

4.1.2 Jenis Tools Aplikasi

Merupakan alat yang digunakan untuk menggambarkan bentuk logika model dari suatu sistem dengan menggunakan simbol-simbol, lambang-lambang, diagram-diagram ataupun GUI yang menunjukkan secara tepat arti dan fungsinya. Adapun tools aplikasi yang dijelaskan sebagai model sistem yang telah dirancang yaitu Netbeans IDE 8.0 untuk pemrograman Java.



Gambar 4. 1 Tampilan Pemrograman Java Netbeans IDE 8.0

4.1.3 Jenis File

Sistem metadata forensik yang telah dibangun ini bisa membaca semua macam tipe jenis file yang ada didalam komputer, contohnya pada laptop dengan merk HP, dimana didalamnya terdapat berbagai jenis macam file seperti file *Microsoft Office* (*word, excel, power point, acces, visio*, dan lain-lainnya), *txt, pdf, rar, py, html, php, jpg, bmp, png, apk, fbk, mp3, mp4*, dan berbagai macam extensi aplikasi yang masih banyak lagi yang ada didalam Laptop Merk HP yang semuanya bisa dibaca metadatanya, akan tetapi dalam tahap pengujian metode sistem ini, ada tujuh macam tipe jenis file yang akan diuji sebagai contoh yaitu DOCX, PDF, JPG, MP3, MP4, DD dan E01.

Ketujuh jenis file ini digunakan sebagai uji coba, karena didalam beberapa kasus yang sering terjadi didalam dunia forensika deigital yaitu seringnya melibatkan ketujuh jenis file ini, sebagai contoh seringnya pemalsuan dokumen (*docx, pdf*) yang terjadi didunia lelang e-procurement, gambar (*jpg*) yang sering menimpa artis tanah air, suara (*mp3*) sadapan yang sering digunakan oleh KPK untuk menjerat para Politikus yang Kuroptor, video-video (*mp4*) asusila yang akan dijadikan barang bukti oleh Polisi untuk menjerat para pelaku seperti video ariel yang sempat heboh beberapa tahun silam hingga kopi sianida mirna solihin yang masih hangat-hangatnya sekarang ini, dan file hasil akuisisi dd dan E01 untuk memastikan apakah dalam penanganan barang bukti sudah sesuai dengan SOP yang berlaku. Berikut masing-masing penjelasannya:

1. File Dokumen Ber-Extensi DOCX

Microsoft Word adalah aplikasi pengolah kata yang sangat populer pada saat ini, aplikasi yang dikembangkan oleh microsoft ini terdapat dalam satu paket microsoft office yang berisi microsoft word, microsoft excel, microsoft power point, microsoft office publisher microsoft office access dan lain-lain. Dalam perkembangannya microsoft word mengalami banyak perkembangan dari tahun ke tahun, dengan perkembangan tersebut microsoft telah menambahkan database dan tool yang baru untuk menyempurnakan agar microsoft word lebih mudah untuk digunakan. Dengan microsoft word dapat memudahkan kerja manusia dalam melakukan pengetikan surat maupun dokumen lain.



Gambar 4. 2 Icon File Extensi DOCX

2. File Ebook Ber-Extensi PDF

PDF atau Portable Document Format adalah sebuah format file yang diciptakan oleh Adobe System, Inc. File jenis ini sangat populer dan banyak digunakan terutama dalam bentuk ebook. Dokumen dengan format portable ini dibuat dan digunakan untuk tujuan kemudahan sekaligus keamanan dokumen.



Gambar 4. 3 Icon File Extensi PDF

3. File Gambar Ber-Extensi JPG

JPG adalah jenis data yang dikembangkan oleh *Joint Photographic Experts Assemble* (JPEG) yang dijadikan standar untuk para fotografer profesional. Setiap kali menyimpan ke tipe JPG dari tipe lain, ukuran gambar biasanya mengecil, dan kualitasnya turun dan tidak dapat dikembalikan lagi. Ukuran file BMP dapat turun menjadi seper sepuluh setelah dikonversi menjadi JPG. Meskipun dengan penurunan kualitas gambar, pada gambar-gambar tertentu (misalnya pemandangan), penurunan kualitas gambar hampir tidak akan terlihat oleh mata.



Gambar 4. 4 Icon File Extensi JPG

4. File Audio Ber-Extensi MP3

Mp3 merupakan format kompresi audio yang dikembangkan oleh Moving Picture Experts Group (MPEG). Format file ini menggunakan Layer 3 kompresi audio yang secara umum digunakan untuk menyimpan file–file musik dan audiobooks dalam hard drive.



Gambar 4. 5 Icon File Extensi MP3

5. File Video Ber-Extensi MP4

File MP4 yang dikembangkan oleh Organisasi Standarisasi Internasional (ISO) berjalan dengan baik dengan hampir semua jenis media player dan perangkat. Karena MP4 dikembangkan untuk MPEG4 dikodekan media, dapat juga ditemukan dalam MPEG-4 spesifikasi sebagai bagian 14 itu MP4 tidak format kontainer hanya dibawah MPEG-4 tetapi itu adalah turunan dari MPEG-4 bagian 12 spesifikasi yang lebih umum untuk menyimpan file MPEG-4.



Gambar 4. 6 Icon File Extensi MP4

6. File Akuisisi Ber-Extensi DD

Disk Image atau sering disebut Imaging dalam dunia digital forensic adalah suatu proses dari file tunggal atau suatu perangkat media penyimpanan seperti hardisk int/eks, usb flash drive, cd, dvd, dan lain-lain yang mengandung isi lengkap dengan strukturnya yang kemudian di *cloning* (perbanyak / penggandaan) dengan isi dan struktur yang sama persis sempurna dari yang asli tanpa selisih ukuran se-bit pun di dalamnya. Mudahnya *disk image* itu proses memetakan penggandaan barang bukti dengan metode *bit by bit copy*.



Gambar 4. 7 File Extensi DD

7. File Akuisisi Ber-Extensi E01

Encase Forensic adalah alat forensik yang paling banyak dikenal dan digunakan, yang telah diproduksi dan diluncurkan oleh Guidance Software Inc. Encase tertanam dengan berbagai fungsi forensik yang meliputi atribut seperti pencitraan disk dan pelestarian, pemulihan data

mutlak dalam bentuk aliran bit, dalam seri ini aplikasi *humongous*, ketika encase digunakan untuk membuat *backup* dari hard drive, CD, USB drive, dll, file yang dikenal sebagai “E01” diproduksi. Ini “.E01” ekstensi file terutama diakui sebagai “Encase Image File Format”. The E01 format file image juga dikenal sebagai EWF (singkatan Saksi Ahli Format). Konsep E01 image encase dikembangkan oleh perangkat lunak encase muncul sebagai hasil dari upaya efisien oleh Guidance Software untuk membantu penyelidikan forensik, analisis, dan ilmuwan forensik dalam menemukan data yang terorganisasi dan sistematis untuk penyelidikan.



Gambar 4. 8 File Extensi E01

4.1.4 Jenis Karakteristik Metadata File

Metadata mempunyai peranan dalam pencarian informasi yaitu memberikan informasi ketersediaan data (diperlukan untuk mengetahui ketersediaan data pada suatu lokasi geografis), kesesuaian pengguna (mengetahui suatu data telah memenuhi spesifikasi yang diinginkan), akses (memperoleh suatu data yang teridentifikasi) dan transfer (memperoleh, menggunakan dan memproses data) (SNI Metadata, 2008). Metadata terdiri dari komponen (role) dan elemen. Role merupakan header dari elemen, elemen berisi informasi mengenai data.

Metadata terdiri atas beberapa jenis standar dalam menampilkan data. Secara sederhana yang dimaksud dengan standar metadata adalah satu set terminologi serta definisi umum yang digunakan dalam metadata serta dipresentasikan dalam format terstruktur. Standar metadata spasial dibuat dan dikembangkan untuk mendefinisikan informasi yang diperlukan oleh seorang pengguna prospektif untuk mengetahui ketersediaan suatu set data spasial, mengetahui kesesuaian set data spasial untuk penggunaan yang diinginkan, mengetahui cara-cara pengaksesan data spasial serta untuk mentransfer set data spasial dengan sukses. Walaupun demikian standar tidak menetapkan tatacara bagaimana informasi diorganisasikan dalam suatu sistem komputer atau dalam suatu transfer data, tidak juga menetapkan tatacara bagaimana informasi tersebut ditransmisikan, dikomunikasikan atau disampaikan kepada pengguna. Jika standar metadata

geospasial terkesan sangat kompleks itu karena standar tersebut didesain untuk mendeskripsikan seluruh data geospasial yang bisa dideskripsikan.

Beberapa standar yang digunakan dalam pembuatan metadata spasial, yaitu: FGDC, ISO 19115, Dublin Core dan SNI Metadata. Standar metadata ISO 19115/19139 merupakan standar untuk pembuatan metadata data geospasial. Format ISO 19115 merupakan standar internasional untuk metadata informasi geografi dan format ISO 19139 merupakan skema implementasi untuk ISO 19115. ISO 19115 mempunyai 409 elemen dan terdapat 22 elemen inti (core element) yang dibutuhkan untuk mendeskripsikan data dan memiliki elemen compound (role) dibawahnya. Role tersebut terbagi menjadi 11 komponen utama, yaitu identifikasi, batasan, kualitas data, representasi spasial, sistem referensi, informasi data, referensi portal katalog, distribusi, informasi tambahan dan informasi skema aplikasi (ISO, 2003). Skema ISO 19139 digunakan untuk mendeskripsikan, melakukan validasi dan melakukan pertukaran metadata geospasial yang disiapkan dalam format XML (Extensible Markup Language).

Beberapa karakteristik metadata yang ditampilkan dalam sistem ini yaitu dibagi dalam 3 kategori:

1. Metadata General, yaitu lokasi file, nama file, type file, owner dan computer.
2. Metadata Detail, yaitu creationTime, lastAccessTime, lastModifiedTime, isDirectory, isOther, isRegularFile, isSymbolicLink dan Size.
3. Metadata Checksum, yaitu Nilai MD5 dan SHA-256.

4.1.5 Jenis Korelasi Metadata File

Secara sederhana, korelasi dapat diartikan sebagai hubungan. Namun ketika dikembangkan lebih jauh, korelasi tidak hanya dapat dipahami sebatas pengertian tersebut. Korelasi merupakan salah satu teknik analisis dalam statistik yang digunakan untuk mencari hubungan antara dua variabel yang bersifat kuantitatif. Hubungan dua variabel tersebut dapat terjadi karena adanya hubungan sebab akibat atau dapat pula terjadi karena kebetulan saja. Dua variabel dikatakan berkorelasi apabila perubahan pada variabel yang satu akan diikuti perubahan pada variabel yang lain secara teratur dengan arah yang sama (*korelasi positif*) atau berlawanan (*korelasi negatif*).

Komputer berisi data dan program, Program merupakan file komputer yang digunakan untuk melakukan tugas tertentu, sedangkan data merupakan file hasil kerja program komputer yang dapat diedit, dibuka, dihapus, dan sebagainya. Sementara itu, folder adalah suatu tempat untuk mengumpulkan file.

Dalam pengujian metode ini ada empat jenis korelasi metadata yang dijadikan sebagai contoh, yaitu metadata *file date, size, type file* dan *owner*. Seseorang investigasi bisa mencari semua jenis file (tidak hanya 7 macam jenis file yang telah dibahas diatas; Docx, Pdf, Jpg, Mp3, Mp4, DD dan E01) yang ada didalam komputer berdasarkan dari empat pilihan korelasi tersebut.

4.1.6 Live Data dalam Proses Investigasi Metadata

Live data adalah format data didalam sebuah sistem yang dapat diakses secara langsung oleh pengguna. Dalam pengumpulan barang bukti live data cenderung lebih mudah karena data yang didapatkan secara langsung dapat dilihat dan dianalisa lebih lanjut lagi.

Secara umum live data mempunyai nilai yang kuat untuk dijadikan barang bukti karena data yang diperoleh terbukti secara langsung dan dilihat secara langsung serta berhubungan dengan sesuatu maupun tindakan apa yang telah dilakukan terhadap file tersebut.

Selanjutnya karena live data dibuat dan dikelola oleh sistem operasi dan aplikasi perangkat lunak. Live data memiliki catatan waktu yang akurat, tergantung dengan kesesuaian jam yang ada dalam perangkat tersebut.

Proses yang terjadi dalam sebuah sistem mempunyai catatan waktu. Catatan waktu yang terjadi biasanya dikenal dengan istilah MAC (*Modified, Accessed, Created*).

1. **Modified** adalah catatan yang menampilkan waktu kapan terakhir kali data dimodifikasi, yaitu ketika terakhir kali disimpan. Modified menampilkan waktu terakhir perubahan file.
2. **Accessed** adalah catatan untuk menampilkan kapan waktu terakhir kali file tersebut diakses.
3. **Created** adalah catatan yang menampilkan kapan data tersebut dibuat pertama kalinya.

Untuk lebih jelasnya mari kita lihat gambar berikut ini:



Created:	01 Oktober 2015, 13:25:16
Modified:	08 Oktober 2015, 21:26:52
Accessed:	15 Oktober 2015, 16:25:22

Gambar 4.9 MAC (*Modified, Accessed, Created*)

Gambar tersebut menunjukkan kapan file tersebut dibuat pertama kali, kemudian menunjukkan juga kapan file dimodifikasi dan di simpan kembali dan yang terakhir menunjukkan kapan file tersebut di akses oleh pengguna.

Catatan waktu ini merupakan sebuah file metadata yang dapat menunjukkan urutan kejadian maupun kegiatan yang terjadi didalam sebuah sistem.

4.2 Source Code Metadata Forensik

Pada kali ini akan dibahas *source code* algoritma metadata forensik. *Source code* yang diambil hanya sebagian dari *coding* yang mempunyai peranan khusus untuk Melihat Karakteristik Metadata File dan Korelasi File berdasarkan metadata file dari Parameter *Date File*, *Size File*, *Type File* dan *Owner File*.

4.2.1 Source Code Membaca Karakteristik Metadata File

1. Source Code Melihat Metadata File Secara Umum

Tabel 4. 2 *Source Code Metadata General*

No.	Source Code
1	public void getMetaData(File f, String namafile) {
2	tModel = new DefaultTableModel(header, 0);
3	Path file = Paths.get(f.getAbsolutePath());
4	try {
5	txtLokasi.setText(f.getPath());
6	txtNamaFile2.setText(namafile);
7	txtTypeFile.setText(getFileExtension(f));
8	txtComputer.setText(getComputerName());
9	FileOwnerAttributeView ownerAttributeView = Files.getFileAttributeView(f.toPath(), FileOwnerAttributeView.class);
10	UserPrincipal owner = ownerAttributeView.getOwner();
11	txtAuthors.setText(owner.getName().substring(owner.getName().lastIndexOf("\\") + 1));
12	} catch (IOException ex) {
13	}
14	tabelMeta.setModel(tModel);
15	}

Pada baris 1 untuk memvalidasi bahwa method ini diakses dan mengembalikan nilai yang dikirim dari class Main, pada baris 2 untuk menaruh nilai yang dihasilkan pada sebuah tabel, pada baris 3 akan selalu mengembalikan pemisah direktori sesuai dengan platform pengguna, pada baris 5 mendefinisikan metadata Folder Path atau Lokasi File, pada baris 6 mendefinisikan metadata Name File, pada baris 7 mendefinisikan metadata Type File, pada baris 8 mendefinisikan metadata Computer yang dipakai, pada baris 9 dan 10 atribut yang di definisikan oleh interface untuk Owner File, pada baris 11 mendefinisikan metadata Owner atau pemilik file yang ada didalam komputer, pada baris 12 untuk *exception* yang berhubungan dengan *input* dan *output*, pada baris 14 di *set* langsung pada interface tabel metadata.

2. Source Code Melihat Metadata File Secara Jelas

Tabel 4. 3 Source Code Metadata Detail

No.	Source Code
1	<code>public void getMetaData(File f) {</code>
2	<code>tModel = new DefaultTableModel(header, 0);</code>
3	<code>Path file = Paths.get(f.getAbsolutePath());</code>
4	<code>try {</code>
5	<code>BasicFileAttributes attr = Files.readAttributes(file, BasicFileAttributes.class);</code>
6	<code>String data1[] = {"1", "creationTime: ", attr.creationTime().toString()};</code>
7	<code>tModel.addRow(data1);</code>
8	<code>String data8[] = {"2", "lastAccessTime: ", attr.lastAccessTime().toString()};</code>
9	<code>tModel.addRow(data8);</code>
10	<code>String data2[] = {"3", "lastModifiedTime: ", attr.lastModifiedTime().toString()};</code>
11	<code>tModel.addRow(data2);</code>
12	<code>lastmodifide=attr.lastModifiedTime().toMillis();</code>
13	<code>System.out.println("LONG File: "+lastmodifide);</code>
14	<code>String data3[] = {"4", "isDirectory: ", String.valueOf(attr.isDirectory())};</code>
15	<code>tModel.addRow(data3);</code>
16	<code>String data4[] = {"5", "isOther: ", String.valueOf(attr.isOther())};</code>
17	<code>tModel.addRow(data4);</code>
18	<code>String data5[] = {"6", "isRegularFile: ", String.valueOf(attr.isRegularFile())};</code>
19	<code>tModel.addRow(data5);</code>
20	<code>String data6[] = {"7", "isSymbolicLink: ", String.valueOf(attr.isSymbolicLink())};</code>
21	<code>tModel.addRow(data6);</code>
22	<code>String data7[] = {"8", "size: ", String.valueOf(attr.size())};</code>
23	<code>size = attr.size();</code>
24	<code>tModel.addRow(data7);</code>
25	<code>} catch (IOException ex) {</code>
26	<code>}</code>
27	<code>tabelMeta.setModel(tModel);</code>
28	<code>}</code>

Pada baris 1 untuk memvalidasi bahwa method ini diakses dan mengembalikan nilai yang dikirim dari class Main, pada baris 2 untuk menaruh nilai yang dihasilkan pada sebuah tabel, pada baris 3 akan selalu mengembalikan pemisah direktori sesuai dengan platform pengguna, pada baris 5 atribut yang di definisikan oleh interface, pada baris 6 dan 7 mendefinisikan metadata *creationTime* yang akan dibaca dan langsung memiliki sebuah baris tabel pada *interface*, begitu juga pada baris selanjutnya sampai dengan baris 24 mendefinisikan metadata *lastAccessTime*, *lastModifiedTime*, *isDirectory*, *isOther*, *isRegularFile*, *isSymbolicLink* dan *Size* serta memiliki sebuah baris tabel pada *interface*, pada baris 25 untuk *exception* yang berhubungan dengan *input* dan *output*, pada baris 27 di *set* langsung pada *interface* tabel metadata.

3. Source Code Melihat Metadata File Nilai Hashing

Tabel 4. 4 Source Code Metadata Checksum

No.	Source Code
1	public byte[] createChecksum(String filename, String type) throws Exception {
2	InputStream fis = new FileInputStream(filename);
3	byte[] buffer = new byte[1024];
4	MessageDigest complete = MessageDigest.getInstance(type);
6	int numRead;
7	do {
8	numRead = fis.read(buffer);
9	if (numRead > 0) {
10	complete.update(buffer, 0, numRead);
12	}
13	} while (numRead != -1);
14	fis.close();
15	return complete.digest();
16	}
17	public String getChecksum(String filename, String type) {
18	String result = "";
19	byte[] b;
20	try {
21	b = createChecksum(filename, type);
22	for (int i = 0; i < b.length; i++) {
23	result += Integer.toString((b[i] & 0xff) + 0x100, 16).substring(1);
24	}
25	} catch (Exception ex) {
26	JOptionPane.showMessageDialog(null, "GAGAL cek CheckSum");
27	}
28	return result;
29	}
30	public void getMetaData(File f, String namafile) {
31	tModel = new DefaultTableModel(header, 0);
32	Path file = Paths.get(f.getAbsolutePath());
33	try {
34	String checksum = "MD5 :\n" + getChecksum(f.getPath(), "MD5") + "\nSHA-256 :\n" +
35	getChecksum(f.getPath(), "SHA-256");
36	txtSUM.setText(checksum);
37	} catch (IOException ex) {
38	}
39	tabelMeta.setModel(tModel);
40	}

Pada baris 1 sampai dengan 16 *source coding* untuk mencari nilai MD5 dan pada baris 17 sampai dengan 29 *source coding* untuk mencari nilai SHA-256. Pada baris 30 untuk memvalidasi bahwa method ini diakses dan mengembalikan nilai yang dikirim dari class Main, pada baris 31 untuk menaruh nilai yang dihasilkan pada sebuah tabel, pada baris 32 akan selalu mengembalikan pemisah direktori sesuai dengan platform pengguna, pada baris 34 dan 35 untuk memanggil nilai Checksum MD5 dan SHA-256 yang ada pada baris 1 sampai dengan 16 dan baris 17 sampai dengan 29, pada baris 36 mendefinisikan metadata Checksum MD5 dan SHA-256, pada baris 37 untuk *exception* yang berhubungan dengan *input* dan *output*, pada baris 39 di *set* langsung pada *interface* tabel metadata.

4.2.2 Source Code Korelasi Metadata File

1. Source Code Korelasi Berdasarkan Tanggal File (Date)

Tabel 4. 5 Source Code Korelasi Berdasarkan Tanggal File (Date)

No.	Source Code
1	public void getHasilLastModified(String dirPath) {
2	try{
3	File dir = new File(dirPath);
4	File[] files = dir.listFiles(tglFilter);
5	if (files.length == 0) {
6	} else {
7	for (File aFile : files) {
8	String data[] = {aFile.getName(), String.valueOf(aFile.length()), sdf.format(new Date(aFile.lastModified())), aFile.getPath()};
9	tModelHasil.addRow(data);
10	}
11	tabelHasil.setModel(tModelHasil);
12	}
13	} catch(Exception ex){
14	}
15	}
16	FileFilter tglFilter = new FileFilter() {
17	public boolean accept(File file) {
18	if (file.isFile()) {
19	if (file.lastModified()== lastmodifide && perbandingan == 1) {
20	return true;
21	} else if (file.lastModified()< lastmodifide && perbandingan == 2) {
22	return true;
23	} else if (file.lastModified()> lastmodifide && perbandingan == 3) {

Lanjutan **Tabel 4.5** *Source Code* Korelasi Berdasarkan Tanggal File (*Date*)

No.	Source Code
24	return true;
25	} else if (file.lastModified()<= lastmodifide && perbandingan == 4) {
26	return true;
27	} else if (file.lastModified()>= lastmodifide && perbandingan == 5) {
28	return true;
29	} else {
30	return false;
31	}
32	} else {
33	return false;
34	}
35	}
36	}

Pada baris 1 untuk validasi hasil metadata lastModified yang dijadikan sebagai acuan korelasi metadata file, pada baris 3 berfungsi untuk melihat daftar file/folder yang berada di direktori atau folder tertentu, pada baris 4 direktori file yang dilihat berdasarkan tanggalnya, pada baris 5 sampai 8 sebuah kondisi yang akan menemukan file tertentu berdsarkan tanggalnya, pada baris 9 dan 11 direktori file yang di temukan akan memiliki baris dan di set langsung pada tabel korelasi di *interface*, pada baris 13 untuk *exception* yang berhubungan dengan *input* dan *output*, pada baris 16 akan memfilter file-file berdasarkan tanggal yang mau ditemukan, pada baris 17 validasi nilai *boolean* dipresentasikan dengan *true* untuk pernyataan bernilai benar dan *false* untuk pernyataan bernilai salah dari file-file yang akan ditemukan, pada baris 18 file yang di inputkan, pada baris 19 file-file direktori yang ditampilkan berdasarkan sama dengan file yang sudah di inputkan, pada baris 21 file-file direktori yang ditampilkan berdasarkan lebih kecil dengan file yang sudah di inputkan, pada baris 23 file-file direktori yang ditampilkan berdasarkan lebih besar dengan file yang sudah di inputkan, pada baris 25 file-file direktori yang ditampilkan berdasarkan lebih kecil sama dengan dengan file yang sudah di inputkan, pada baris 27 file-file direktori yang ditampilkan berdasarkan lebih besar sama dengan dengan file yang sudah di inputkan.

2. *Source Code* Korelasi Berdasarkan Ukuran File (*Size*)

Tabel 4. 6 *Source Code* Korelasi Berdasarkan Ukuran File (*Size*)

No.	Source Code
1	public void getHasilSize(String dirPath) {
2	try{

Lanjutan **Tabel 4. 6** *Source Code* Korelasi Berdasarkan Ukuran File (*Size*)

No.	Source Code
3	File dir = new File(dirPath);
4	File[] files = dir.listFiles(sizeFilter);
5	if (files.length == 0) {
6	} else {
7	for (File aFile : files) {
8	String data[] = {aFile.getName(), String.valueOf(aFile.length()), sdf.format(new Date(aFile.lastModified())), aFile.getPath()};
9	tModelHasil.addRow(data);
10	}
11	tabelHasil.setModel(tModelHasil);
12	}
13	}catch(Exception ex){
14	}
15	}
16	FileFilter sizeFilter = new FileFilter() {
17	public boolean accept(File file) {
18	if (file.isFile()) {
19	if (file.length() == size && perbandingan == 1) {
20	return true;
21	} else if (file.length() < size && perbandingan == 2) {
22	return true;
23	} else if (file.length() > size && perbandingan == 3) {
24	return true;
25	} else if (file.length() <= size && perbandingan == 4) {
26	return true;
27	} else if (file.length() >= size && perbandingan == 5) {
28	return true;
29	} else {
30	return false;
31	}
32	} else {
33	return false;
34	}
35	}
36	}

Pada baris 1 untuk validasi hasil metadata size yang dijadikan sebagai acuan korelasi metadata file, pada baris 3 berfungsi untuk melihat daftar file/folder yang berada di direktori atau folder tertentu, pada baris 4 direktori file yang dilihat berdasarkan ukuran filenya, pada baris 5

sampai 8 sebuah kondisi yang akan menemukan file tertentu berdasarkan ukuran filenya, pada baris 9 dan 11 direktori file yang di temukan akan memiliki baris dan di set langsung pada tabel korelasi di *interface*, pada baris 13 untuk *exception* yang berhubungan dengan *input* dan *output*, pada baris 16 akan memfilter file-file berdasarkan ukuran file yang mau ditemukan, pada baris 17 validasi nilai *boolean* dipresentasikan dengan *true* untuk pernyataan bernilai benar dan *false* untuk pernyataan bernilai salah dari file-file yang akan ditemukan, pada baris 18 file yang di inputkan, pada baris 19 file-file direktori yang ditampilkan berdasarkan sama dengan file yang sudah di inputkan, pada baris 21 file-file direktori yang ditampilkan berdasarkan lebih kecil dengan file yang sudah di inputkan, pada baris 23 file-file direktori yang ditampilkan berdasarkan lebih besar dengan file yang sudah di inputkan, pada baris 25 file-file direktori yang ditampilkan berdasarkan lebih kecil sama dengan dengan file yang sudah di inputkan, pada baris 27 file-file direktori yang ditampilkan berdasarkan lebih besar sama dengan dengan file yang sudah di inputkan.

3. Source Code Korelasi Berdasarkan Ektensi File (*Type File*)

Tabel 4. 7 Source Code Korelasi Berdasarkan Ektensi File (*Type File*)

No.	Source Code
1	FileFilter extensi = new FileFilter() {
2	public boolean accept(File file) {
3	if (file.isFile()) {
4	if (getFileExtension(file).equalsIgnoreCase(txtTypeFile.getText().trim())) {
5	return true;
6	} else {
7	return false;
8	}
9	} else {
10	return false;
11	}
12	}
13	};
14	private String getFileExtension(File file) {
15	String name = file.getName();
16	try {
17	return name.substring(name.lastIndexOf(".") + 1);
18	} catch (Exception e) {
19	return "";
20	}

Pada baris 1 untuk filter hasil metadata yang khusus ekstensi file, pada baris 2 validasi nilai *boolean* di presentasikan dengan *true* untuk pernyataan bernilai benar dan *false* untuk pernyataan bernilai salah dari file-file yang akan ditemukan, pada baris 3 sebuah kondisi yang akan menemukan file tertentu berdasarkan ekstensi filenya, pada baris 4 dan 5 jika file-file yang ditemukan berdasarkan file ekstensi maka akan ditampilkan, pada baris 6 dan 7 jika tidak ditemukan berdasarkan file ekstensi maka tidak akan ditampilkan, begitu juga dengan baris 9 dan 10. Pada baris 14 untuk validasi hasil metadata ekstensi file yang dijadikan sebagai acuan korelasi metadata file, pada baris 15 direktori file yang dilihat berdasarkan ekstensi filenya, pada baris 17 memilih file ekstensi yang dicari berdasarkan dari nilai metadata yang sudah ditemukan, pada baris 18 untuk *exception* yang berhubungan dengan *input* dan *output*.

4. Source Code Korelasi Berdasarkan Pemilik File (Owner)

Tabel 4. 8 Source Code Korelasi Berdasarkan Pemilik File (Owner)

No.	Source Code
1	FileFilter author = new FileFilter() {
2	public boolean accept(File file) {
3	FileOwnerAttributeView ownerAttributeView =
4	Files.getFileAttributeView(file.toPath(), FileOwnerAttributeView.class);
5	UserPrincipal owner = null;
6	try {
7	owner = ownerAttributeView.getOwner();
8	String dd = owner.getName().substring(owner.getName().lastIndexOf("\\") + 1);
9	if (file.isFile()) {
10	if (dd.equalsIgnoreCase(txtAuthors.getText().trim())) {
11	return true;
12	} else {
13	return false;
14	}
15	} else {
16	return false;
17	}
18	} catch (IOException ex) {
19	return false;
20	}
21	}
22	}

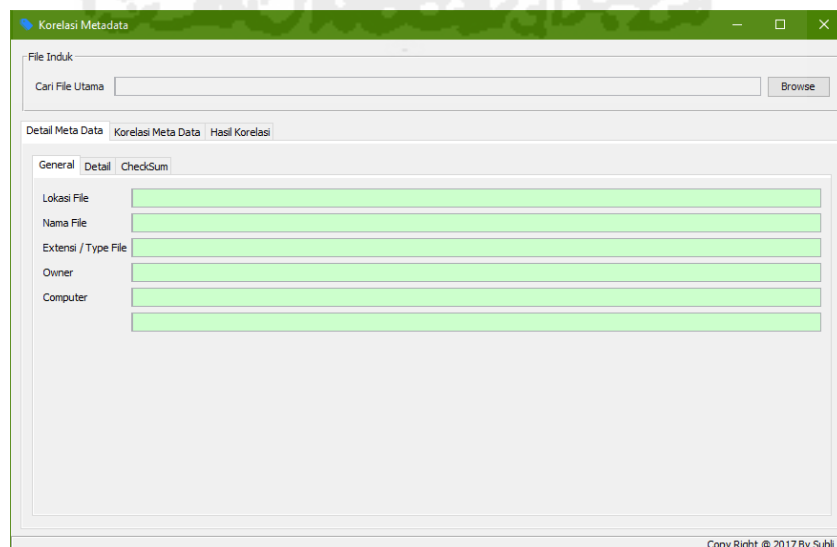
Pada baris 1 untuk filter hasil metadata yang khusus Owner atau pemilik file, pada baris 2 validasi nilai *boolean* di presentasikan dengan *true* untuk pernyataan bernilai benar dan *false* untuk

pernyataan bernilai salah dari file-file yang akan ditemukan, pada baris 3 dan 4 atribut yang di definisikan oleh *interface* untuk menemukan Owner file, pada baris 5 akan diseleksi pencarian dan yang ditampilkan berdasarkan owner file saja dan yang lainnya tidak akan ditampilkan, pada baris 7 direktori file yang dilihat berdasarkan owner filenya, pada baris 8 memilih file ekstensi yang dicari berdasarkan dari nilai metadata yang sudah ditemukan, pada baris 9 sebuah kondisi yang akan menemukan file tertentu berdasarkan Owner filenya, pada baris 10 dan 11 5 jika file-file yang ditemukan berdasarkan file owner maka akan ditampilkan, pada baris 12 dan 13 jika tidak ditemukan berdasarkan file ekstensi maka tidak akan ditampilkan, begitu juga dengan baris 15 dan 16, pada baris 18 untuk *exception* yang berhubungan dengan *input* dan *output*.

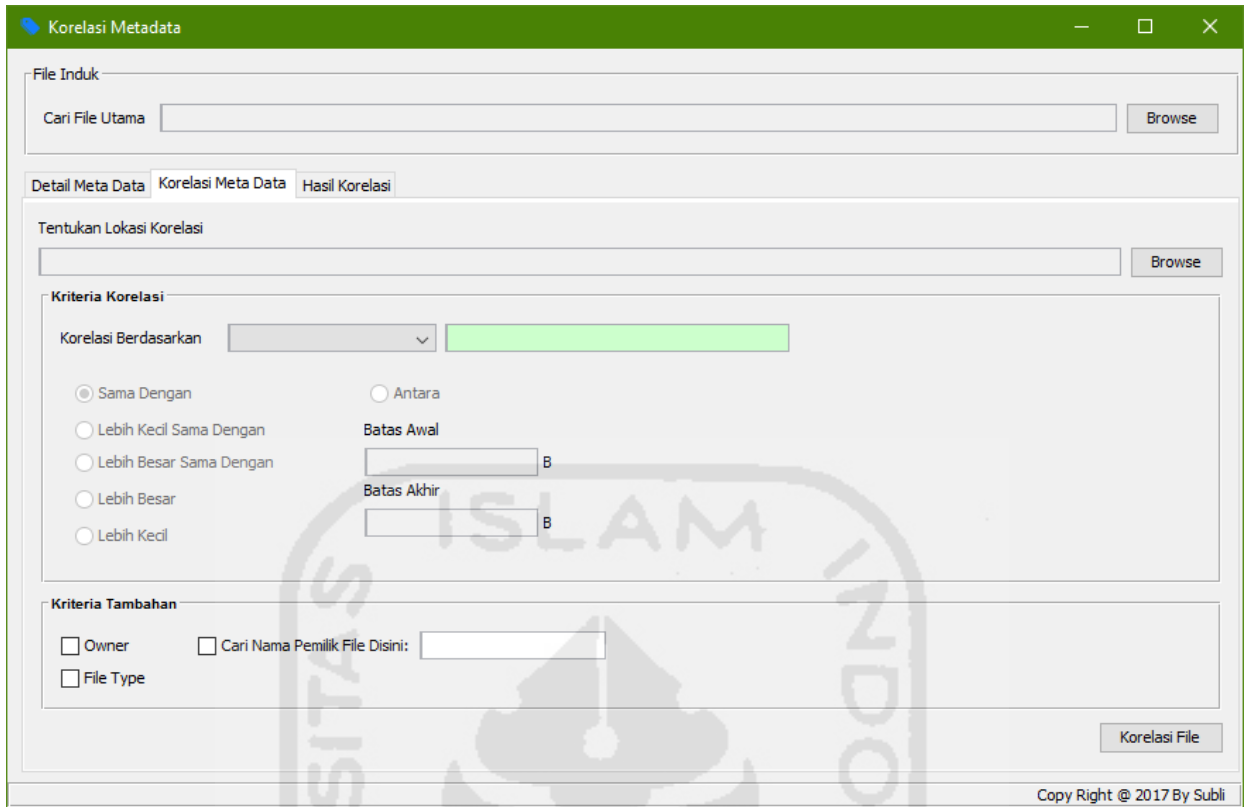
4.3 Pengujian Sistem Metadata Forensik

4.3.1 Awal Program

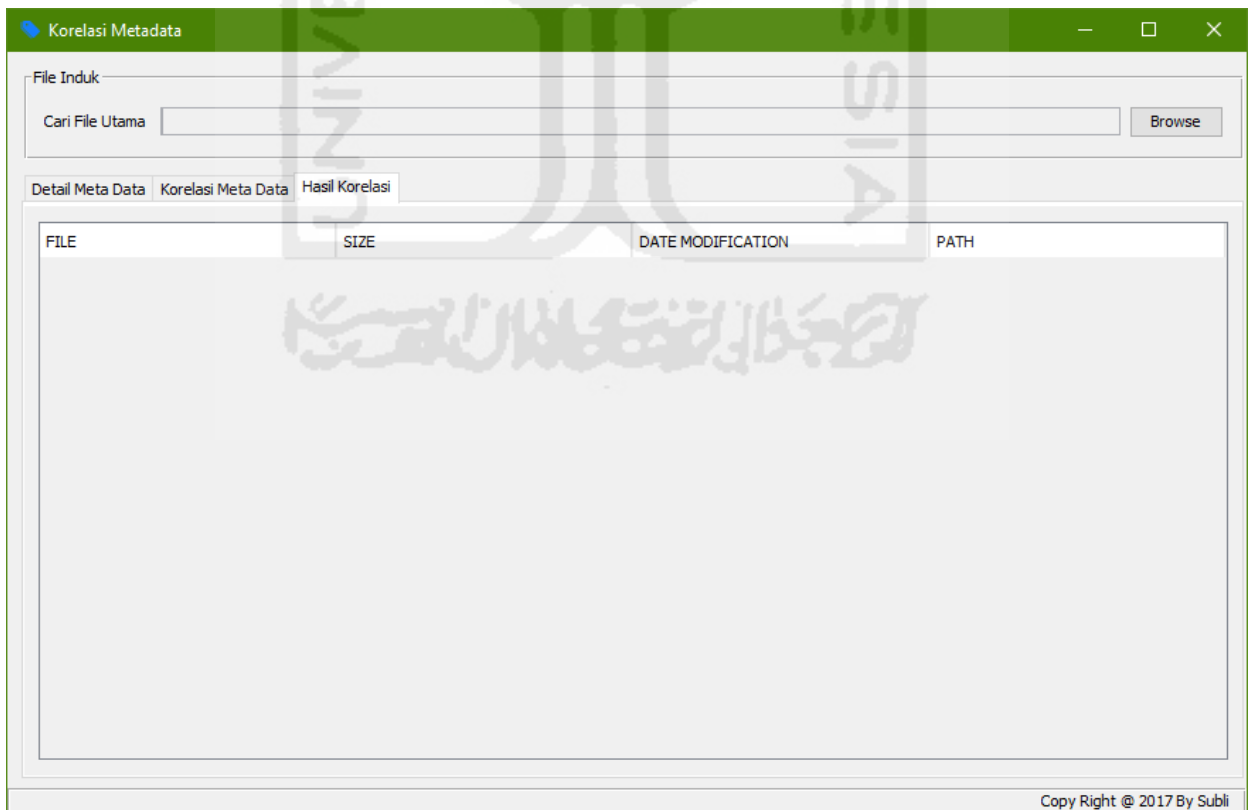
Tampilan awal program sistem metadata forensik ketika baru dijalankan yaitu akan menampilkan Menu File Induk (untuk mencari file utama yang akan di browse) dan Menu Detail Metadata (yang didalamnya ada Menu General untuk melihat metadata file secara umum, Menu Detail untuk melihat metadata file secara lebih jelas lagi dan Menu Checksum untuk melihat nilai hashing suatu file), selanjutnya ketika di select menu berikutnya yaitu Menu Korelasi Metadata (yang didalamnya akan menentukan lokasi tempat pencarian file dan pilihan korelasi file dari empat macam parameter metadata file yaitu tanggal, ukuran, ekstensi file dan nama pemilik file) dan Menu Hasil Korelasi (tempat yang sudah disediakan untuk file-file yang sudah ditemukan, berdasarkan pilihan dari menu korelasi file yang sudah ditentukan). Berikut adalah tempilan awal dari ketiga menu masing-masing program ketika baru dijalankan, seperti gambar dibawah ini:



Gambar 4. 10 Tampilan Awal Program Menu Detail Metadata



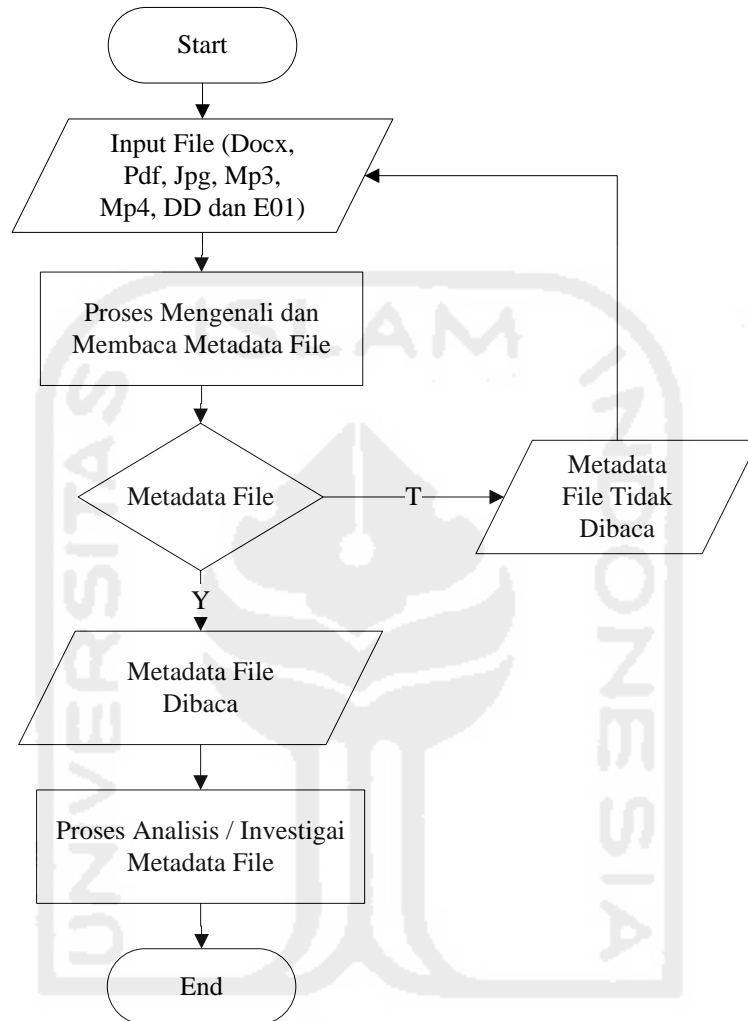
Gambar 4. 11 Tampilan Awal Program Menu Korelasi Metadata



Gambar 4. 12 Tampilan Awal Program Menu Hasil Korelasi

4.3.2 Melihat Karakteristik Metadata File

Berikut dijelaskan secara rinci langkah-langkah penggunaan program aplikasi ini dalam melihat karakteristik metadata file pada gambar *flowchart* dibawah:

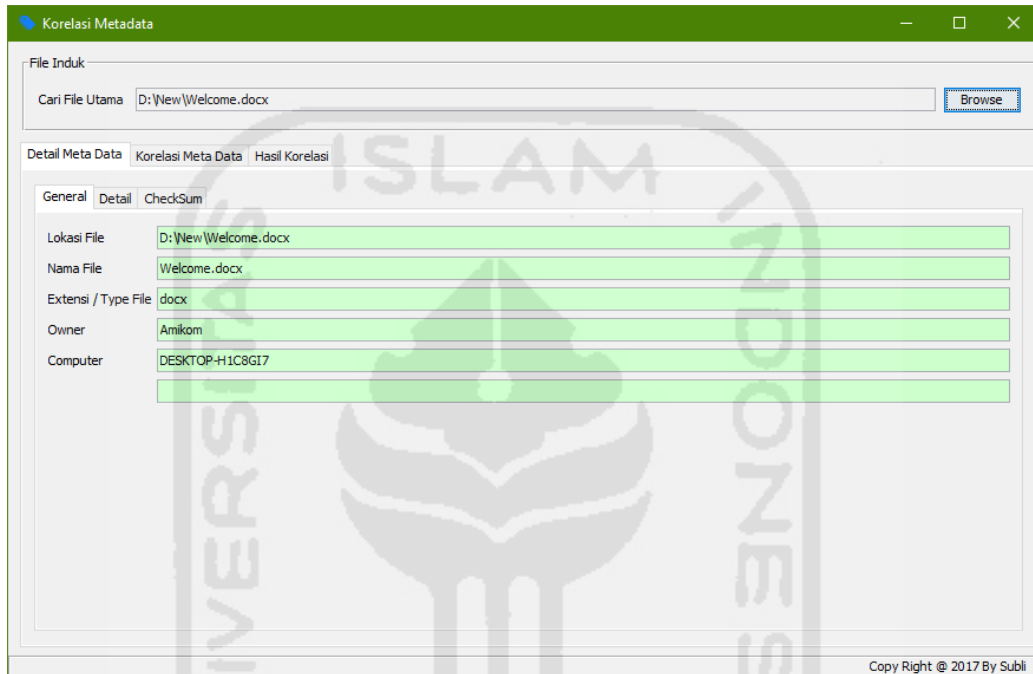


Gambar 4. 13 Flowchart Membaca Karakteristik Metadata File

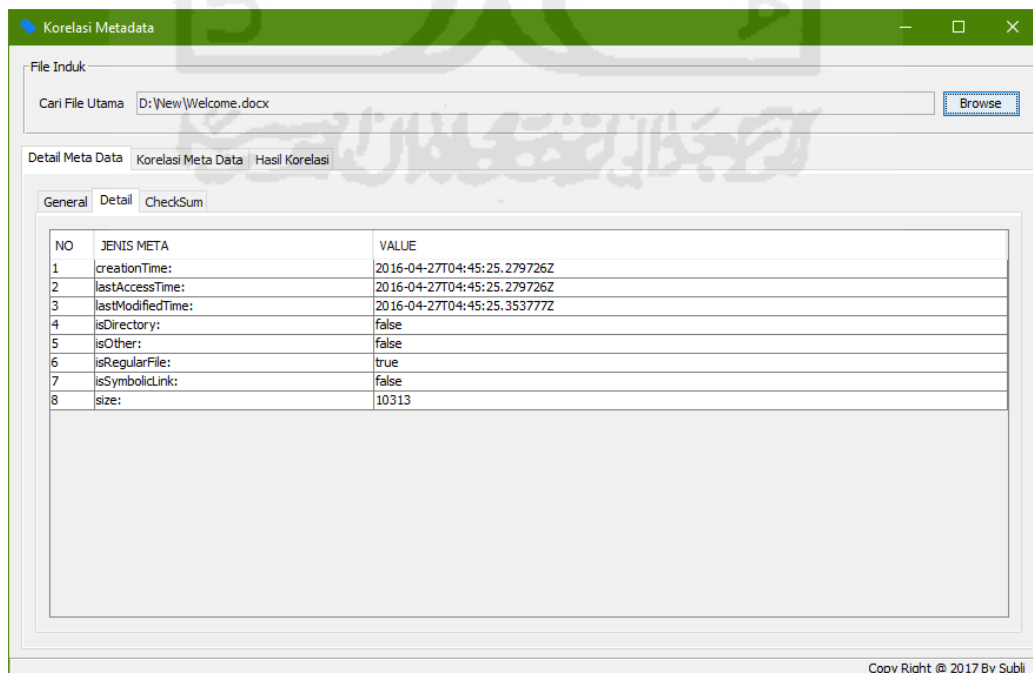
Berikut penjelasan gambar 4.12 *flowchart* dalam pengujian membaca karakteristik metadata file:

1. Pertama-tama dilakukan *start* atau sistem dijalankan
2. Setelah itu dilakukan penginputan file yang akan di baca atau di kenali metadatanya, dimana file yang akan dibaca yaitu file ber-extension Docx, Pdf, Jpg, Mp3, Mp4, DD dan E01
3. Kemudian program akan melakukan pemrosesan file yang telah di inputkan, terdapat kondisi, dimana metadata file yang tidak bisa dibaca akan kembali ke inputan file objek, tetapi metadata file yang dapat terbaca akan langsung ditampilkan metadata filenya
4. Selanjutnya dilakukan sebuah analisis / investigasi terhadap metadata file yang sudah dibaca, dan
5. Terakhir program di tutup atau selesai di jalankan

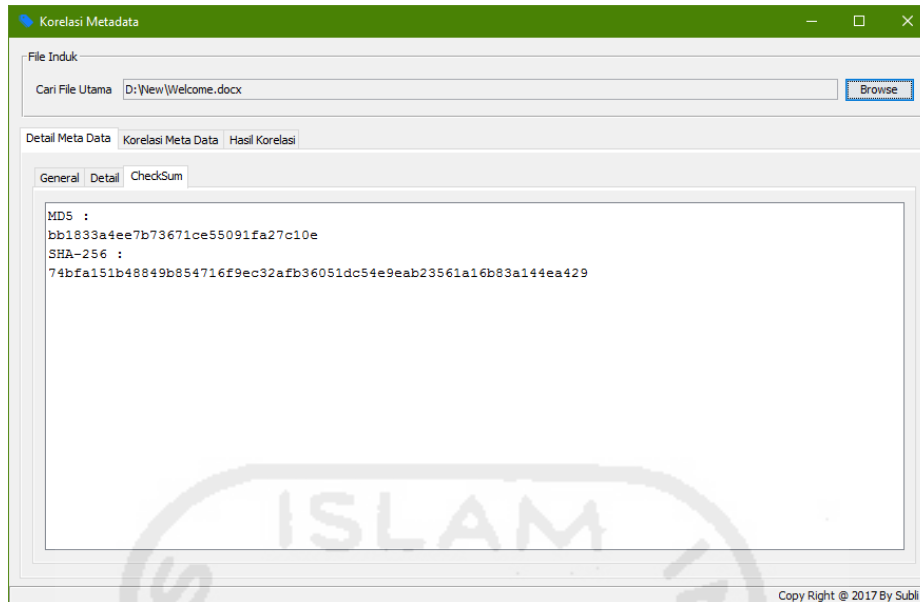
File yang mau di baca metadatanya, terlebih dahulu akan di browse atau di cari sebuah file yang akan diperiksa metadatanya, setelah itu baru kemudian program akan memproses file tersebut sampai ter-identifikasi metadatanya satu persatu, kemudian akan dimunculkan keterangan metadatanya di tabel detail metadata, seperti kita mencoba mem-browse sebuah file Welcome.docx yang ada didalam Folder New Data D Komputer, hasilnya bisa dilihat seperti gambar dibawah ini:



Gambar 4. 14 Metadata General



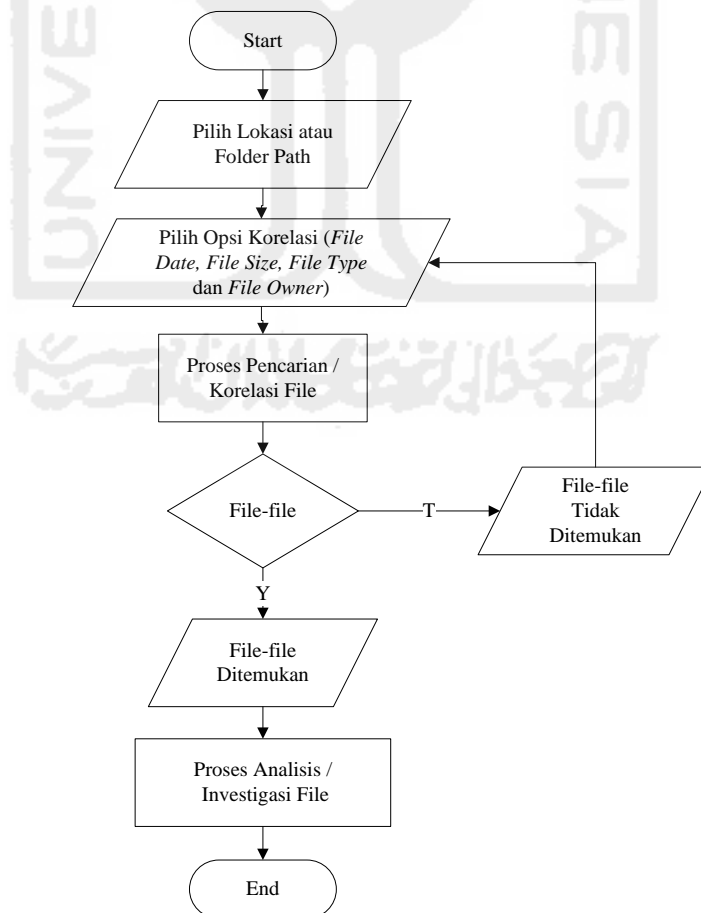
Gambar 4. 15 Metadata Detail



Gambar 4. 16 Metadata Checksum

4.3.3 Melakukan Korelasi File

Berikut dijelaskan secara rinci langkah-langkah penggunaan program aplikasi ini untuk melakukan korelasi file dalam gambar *flowchart* dibawah:



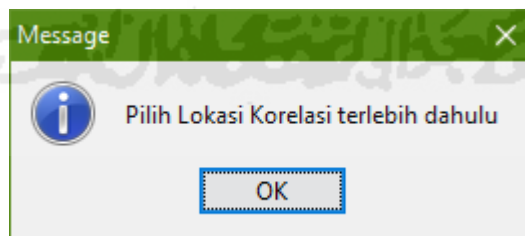
Gambar 4. 17 Flowchart Melakukan Korelasi Metadata File

Berikut penjelasan gambar 4.16 *flowchart* dalam pengujian melakukan korelasi metadata file:

1. Pertama-tama dilakukan *start* atau sistem yang sudah dijalankan tinggal menunggu perintah mulai lagi
2. Dilakukan penginputan lokasi korelasi terlebih dahulu (Data C, Data D atau Data E) atau Foder Path yang ada didalam komputer
3. Setelah itu dilakukan pemilihan metadata file berdasarkan korelasi parameter dari *File Date*, *File Size*, *File Type* dan *File Owner*, kemudian sistem akan melakukan proses menemukan korelasi metadata file yang telah dibuat
4. Terdapat pernyataan atau kondisi dimana terdapat banyak file-file, jika file-file masih belum ditemukan korelasi metadatanya maka sistem akan kembali memilih opsi korelasi metadata file seperti biasa, tetapi apabila file-file sudah ditemukan dari korelasi metadata filenya berdasarkan parameter yang telah dibangun maka akan dilanjutkan ke analisis / investigasi file-file yang sudah ditemukan tersebut, dan
5. Terakhir sistem ini selesai digunakan dan ditutup.

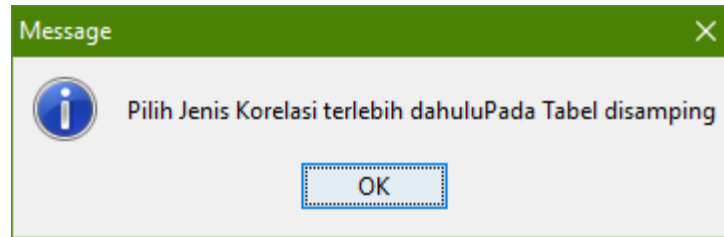
Untuk hasil korelasi metadata file itu sendiri, ada empat jenis yang ditampilkan dari file yaitu Nama sebuah file (*File Name*), Ukuran dari file (*Size*), Tanggal suatu file (*Date*) dan Tempat lokasi atau folder dari suatu file (*Path*).

Selanjutnya untuk melihat korelasi metadata, silahkan browse dulu letaknya, apakah mau di data mana (Data C / Data D) atau di folder mana di setiap data (Data C / Data D). Jika belum di browse dan langsung klik button Korelasi File, maka muncul pesan Pilih Lokasi Korelasi terlebih dahulu, hasilnya seperti gambar berikut:



Gambar 4. 18 Pilih Lokasi Korelasi

Jika sudah di browse lokasi korelasi metadata yang mau di lihat dan langsung klik button Korelasi File, maka muncul pesan Pilih Jenis Korelasi dahulu pada tabel disamping (parameter korelasi yang mau digunakan yaitu bisa tanggal/date, ukuran/size, ekstensi/type atau pemilik/owner), hasilnya seperti gambar berikut:



Gambar 4. 19 Pilih Jenis Korelasi

1. Korelasi Berdasarkan Tanggal (*File Date*)

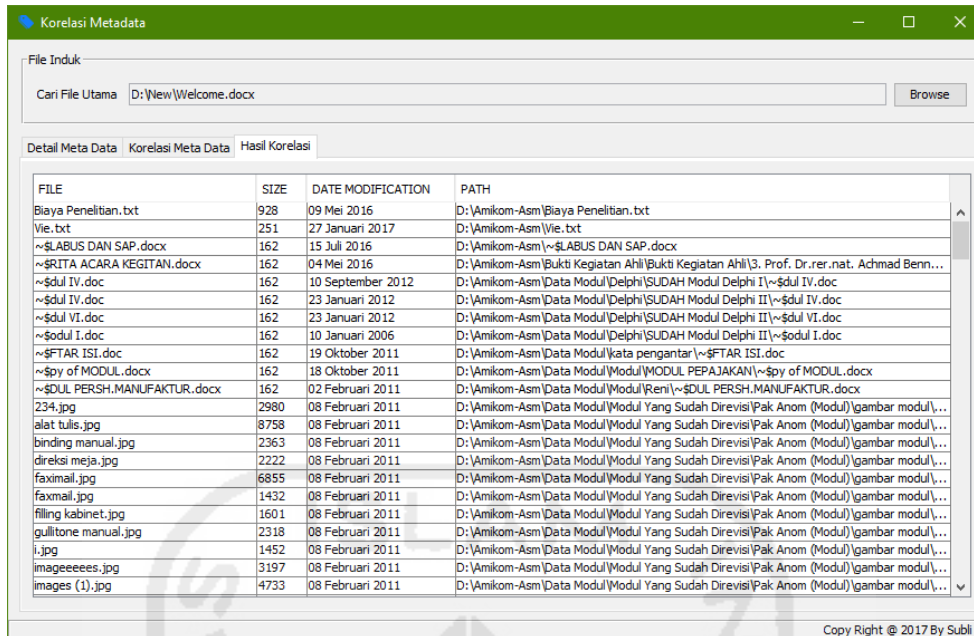
Jika sudah di pilih salah satunya, misal tanggal dan klik option file yang mau di munculin, apakah tanggalnya **Lebih Besar** dari file Welcome.docx yang sudah di browse, baru kemudian di klik button Korelasi File, maka file-file yang ada di Data D yang tanggalnya lebih besar dari file Welcome.docx akan segera di cari oleh sistem metadata forensik ini, setelah menunggu beberapa saat, maka akan ditemukan banyak sekali file-file yang ada di dalam folder-folder di Data D dan hasilnya seperti gambar berikut:

FILE	SIZE	DATE MODIFICATION	PATH
Biaya Penelitian.txt	928	09 Mei 2016	D:\Amikom-Asm\Biaya Penelitian.txt
borang re akreditasi revisi_8 ok.doc	1887744	11 Mei 2016	D:\Amikom-Asm\borang re akreditasi revisi_8 ok.doc
BUKU 3A-BORANG AKREDITASI PR...	1555968	07 Mei 2016	D:\Amikom-Asm\BUKU 3A-BORANG AKREDITASI PROGRAM DIPLOMA_v_NewEditing.doc
CONTOH PROPOSAL PENGABDIAN ...	278.28	11 Agustus 2016	D:\Amikom-Asm\CONTOH PROPOSAL PENGABDIAN MASYARAKAT.docx
Daftar Penelitian TK.docx	19307	24 Mei 2016	D:\Amikom-Asm\Daftar Penelitian TK.docx
Dosen Amikom.docx	12940	18 Juni 2016	D:\Amikom-Asm\Dosen Amikom.docx
KOP AMIKOM BARU.doc	167936	23 Juni 2016	D:\Amikom-Asm\KOP AMIKOM BARU.doc
NIK Dosen.xlsx	23734	25 Mei 2016	D:\Amikom-Asm\NIK Dosen.xlsx
SILABUS DAN SAP.docx	11596	15 Juli 2016	D:\Amikom-Asm\SILABUS DAN SAP.docx
Surat Undangan Rapat.docx	13805	13 Juni 2016	D:\Amikom-Asm\Surat Undangan Rapat.docx
Undangan Notulis.docx	13335	16 Juni 2016	D:\Amikom-Asm\Undangan Notulis.docx
Vie.txt	251	27 Januari 2017	D:\Amikom-Asm\Vie.txt
-SLABUS DAN SAP.docx	162	15 Juli 2016	D:\Amikom-Asm\SLABUS DAN SAP.docx
BERITA ACARA KEGIATAN.docx	83357	25 Mei 2016	D:\Amikom-Asm\Bukti Kegiatan Ahi\Bukti Kegiatan Ahi\1. Bambang Eka Purnama, M.Kom\...
Pengelolan Jurnal Ilmiah.pptx	4995284	18 Mei 2016	D:\Amikom-Asm\Bukti Kegiatan Ahi\Bukti Kegiatan Ahi\1. Bambang Eka Purnama, M.Kom\...
BERITA ACARA KEGIATAN.docx	84720	21 Mei 2016	D:\Amikom-Asm\Bukti Kegiatan Ahi\Bukti Kegiatan Ahi\10. Prof. Dr. ren.nat. Admad Ben...
BERITA ACARA KEGIATAN.docx	82802	21 Mei 2016	D:\Amikom-Asm\Bukti Kegiatan Ahi\Bukti Kegiatan Ahi\11. Prof. Dr. Richardus Eko Indraj...
E-Learning-dan-Pembelajaran-berba...	1115648	16 Mei 2016	D:\Amikom-Asm\Bukti Kegiatan Ahi\Bukti Kegiatan Ahi\11. Prof. Dr. Richardus Eko Indraj...
e-Learning.ppt	1299968	16 Mei 2016	D:\Amikom-Asm\Bukti Kegiatan Ahi\Bukti Kegiatan Ahi\11. Prof. Dr. Richardus Eko Indraj...
BERITA ACARA KEGIATAN.docx	83480	26 Mei 2016	D:\Amikom-Asm\Bukti Kegiatan Ahi\Bukti Kegiatan Ahi\12. Ir. Wayan Joniarta, MT\BERIT...
Program Penelitian dan Pengabdian...	184832	16 Mei 2016	D:\Amikom-Asm\Bukti Kegiatan Ahi\Bukti Kegiatan Ahi\12. Ir. Wayan Joniarta, MT\Prog...
Strategi-Perencanaan-Proposal-Peng...	154624	16 Mei 2016	D:\Amikom-Asm\Bukti Kegiatan Ahi\Bukti Kegiatan Ahi\12. Ir. Wayan Joniarta, MT\Strate...

Gambar 4. 20 Hasil Korelasi Tanggal

2. Korelasi Berdasarkan Ukuran (*File Size*)

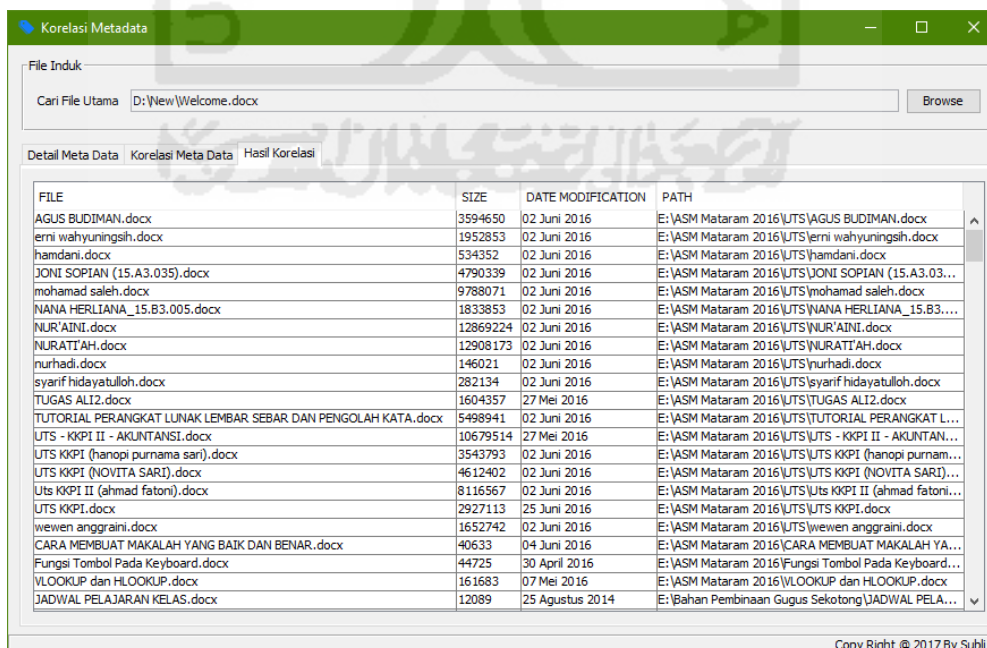
Sama seperti diatas, jika yang di pilih adalah size atau ukuran filenya, dan dibuat option yang dimunculin adalah **Lebih Kecil** dari file Welcome.docx yang sudah di browse, baru kemudian di klik button Korelasi File, maka file-file yang ada di Data D yang ukurannya lebih kecil dari file Welcome.docx akan segera di cari oleh sistem metadata forensik ini, kemudian menunggu beberapa saat, maka akan ditemukan banyak sekali file-file yang ada di dalam folder-folder di Data D dan hasilnya seperti gambar berikut:



Gambar 4. 21 Hasil Korelasi Ukuran

3. Korelasi Berdasarkan Ektensi (File Type)

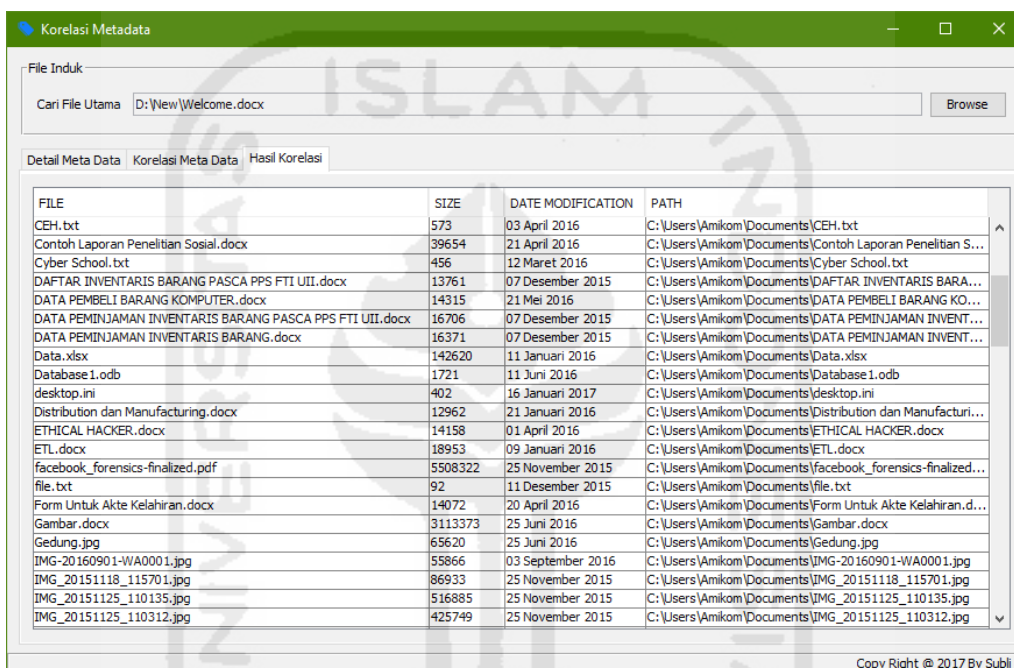
Untuk melihat hasil pencarian berdasarkan korelasi ekstensi file yaitu pilih lokasi korelasi dulu, misal di Data E dan langsung dipilih option **File Type**, maka file Welcome.docx yang sudah di browse yang berektensi **.docx** akan segera di cari oleh sistem metadata forensik ini, setelah menunggu beberapa saat, maka akan ditemukan banyak sekali file-file berektensi docx yang ada di dalam folder-folder di Data E dan hasilnya seperti gambar berikut:



Gambar 4. 22 Hasil Korelasi Ektensi File

4. Korelasi Berdasarkan Pemilik (*File Owner*)

Selanjutnya untuk melihat hasil pencarian berdasarkan korelasi pemilik file yaitu pilih lokasi korelasi dulu, misalnya di Documents yang ada di Data C dan langsung dipilih option **Owner**, maka file Welcome.docx yang sudah di browse sebelumnya yang pemilik filenya bernama **Amikom** akan segera di cari oleh sistem metadata forensik ini, kemudian menunggu beberapa saat, maka akan ditemukan banyak sekali file-file atas nama pemilik Amikom yang ada di dalam folder-folder yang di Documents Data C dan hasilnya bisa dilihat seperti gambar berikut:



FILE	SIZE	DATE MODIFICATION	PATH
CEH.txt	573	03 April 2016	C:\Users\Amikom\Documents\CEH.txt
Contoh Laporan Penelitian Sosial.docx	39654	21 April 2016	C:\Users\Amikom\Documents\Contoh Laporan Penelitian S...
Cyber School.txt	456	12 Maret 2016	C:\Users\Amikom\Documents\Cyber School.txt
DAFTAR INVENTARIS BARANG PASCA PPS FTI UII.docx	13761	07 Desember 2015	C:\Users\Amikom\Documents\DAFTAR INVENTARIS BARA...
DATA PEMBELI BARANG KOMPUTER.docx	14315	21 Mei 2016	C:\Users\Amikom\Documents\DATA PEMBELI BARANG KO...
DATA PEMINJAMAN INVENTARIS BARANG PASCA PPS FTI UII.docx	16706	07 Desember 2015	C:\Users\Amikom\Documents\DATA PEMINJAMAN INVENT...
DATA PEMINJAMAN INVENTARIS BARANG.docx	16371	07 Desember 2015	C:\Users\Amikom\Documents\DATA PEMINJAMAN INVENT...
Data.xlsx	142620	11 Januari 2016	C:\Users\Amikom\Documents\Data.xlsx
Database1.odt	1721	11 Juni 2016	C:\Users\Amikom\Documents\Database1.odt
desktop.ini	402	16 Januari 2017	C:\Users\Amikom\Documents\desktop.ini
Distribution dan Manufacturing.docx	12962	21 Januari 2016	C:\Users\Amikom\Documents\Distribution dan Manufacturi...
ETHICAL HACKER.docx	14158	01 April 2016	C:\Users\Amikom\Documents\ETHICAL HACKER.docx
ETL.docx	18953	09 Januari 2016	C:\Users\Amikom\Documents\ETL.docx
facebook_forensics-finalized.pdf	5508322	25 November 2015	C:\Users\Amikom\Documents\facebook_forensics-finalized...
file.txt	92	11 Desember 2015	C:\Users\Amikom\Documents\file.txt
Form Untuk Akte Kelahiran.docx	14072	20 April 2016	C:\Users\Amikom\Documents\Form Untuk Akte Kelahiran.d...
Gambar.docx	3113373	25 Juni 2016	C:\Users\Amikom\Documents\Gambar.docx
Gedung.jpg	65620	25 Juni 2016	C:\Users\Amikom\Documents\Gedung.jpg
IMG-20160901-WA0001.jpg	55866	03 September 2016	C:\Users\Amikom\Documents\IMG-20160901-WA0001.jpg
IMG_20151118_115701.jpg	86933	25 November 2015	C:\Users\Amikom\Documents\IMG_20151118_115701.jpg
IMG_20151125_110135.jpg	516885	25 November 2015	C:\Users\Amikom\Documents\IMG_20151125_110135.jpg
IMG_20151125_110312.jpg	425749	25 November 2015	C:\Users\Amikom\Documents\IMG_20151125_110312.jpg

Gambar 4. 23 Hasil Korelasi Pemilik File

4.4 Analisis Hasil Sistem Metadata Forensik

Untuk melihat sejauh mana hasil kemampuan sistem yang dibangun, perlu dilihat dan dianalisa hasil pengujian metode tersebut. Berikut adalah hasil pengujian dan analisa sistem yang sudah di uji cobakan.

4.4.1 Analisis Hasil Membaca Karakteristik Metadata File

1. File Dokumen ber-Extensi DOCX

Nama file yang di uji coba dengan sistem metadata forensik ini adalah file Welcome.docx yang berlokasi didalam Folder New yang ada di Data D, kemudian dari pengujian tersebut di dapat hasil analisa metadatanya, berikut bisa di lihat di tabel berikut:

Tabel 4. 9 Hasil Membaca Metadata File Dokumen Welcome.docx

No.	Jenis Metadata	Value
1	Folder Path	D:\New>Welcome.docx
2	Name File	Welcome.docx
3	Type File	docx
4	Owner	Amikom
5	Computer	DESKTOP-H1C8GI7
6	Creation Time	2016-04-27T04:45:25.279726Z
7	Last Access Time	2016-04-27T04:45:25.279726Z
8	Last Modified Time	2016-04-27T04:45:25.353777Z
9	Is Directory	false
10	Is Other	false
11	Is Regular File	true
12	Is Symbolic Link	false
13	Size	10313
14	Checksum MD5	bb1833a4ee7b73671ce55091fa27c10e
15	Checksum SHA-256	74bfa151b48849b854716f9ec32afb3 6051dc 54e9eab23561 a16b83a144ea429

2. File Ebook ber-Extensi PDF

Nama file yang di uji coba dengan sistem metadata forensik ini adalah file Contoh-LR-FD.pdf yang berlokasi di Folder Tesis UII yang ada di Data D, kemudian dari pengujian tersebut di dapat hasil analisa metadatanya, berikut bisa di lihat di tabel berikut:

Tabel 4. 10 Hasil Membaca Metadata File Ebook Contoh-LR-FD.pdf

No.	Jenis Metadata	Value
1	Folder Path	D:\Tesis UII\Contoh-LR-FD.pdf
2	Name File	Contoh-LR-FD.pdf
3	Type File	pdf
4	Owner	Amikom
5	Computer	DESKTOP-H1C8GI7
6	Creation Time	2016-09-18T15:42:27.799967Z
7	Last Access Time	2016-09-18T15:42:27.799967Z
8	Last Modified Time	2016-06-23T02:58:32Z
9	Is Directory	false
10	Is Other	false
11	Is Regular File	true

Lanjutan **Tabel 4. 10** Hasil Membaca Metadata File Ebook Contoh-LR-FD.pdf

No.	Jenis Metadata	Value
12	Is Symbolic Link	false
13	Size	3290304
14	Checksum MD5	35a66b998cd21306211cdbcdf23419c3
15	Checksum SHA-256	fad9bdc81b174492304ea6f5753646f65eda936f623d05e0fbb8aa3c59f5ad04

3. File Gambar ber-Extensi JPG

Nama file yang di uji coba dengan sistem metadata forensik ini adalah file Subli.jpg yang berlokasi di Folder Foto yang ada di Data E, kemudian dari pengujian tersebut di dapat hasil analisa metadatanya, berikut bisa di lihat di tabel berikut:

Tabel 4. 11 Hasil Membaca Metadata File Gambar Subli.jpg

No.	Jenis Metadata	Value
1	Folder Path	E:\Foto\Subli.jpg
2	Name File	Subli.jpg
3	Type File	jpg
4	Owner	S-1-5-21-2838851640-846236458-583387153-1001
5	Computer	DESKTOP-H1C8GI7
6	Creation Time	2015-10-08T03:00:25.719788Z
7	Last Access Time	2015-10-08T03:00:25.719788Z
8	Last Modified Time	2013-05-27T14:05:33.458215Z
9	Is Directory	false
10	Is Other	false
11	Is Regular File	true
12	Is Symbolic Link	false
13	Size	5117665
14	Checksum MD5	3858ca9b670e9d4577465ab2774a0fa6
15	Checksum SHA-256	26b1b0b0e52e085e30e7e149a2940fb3f198d44eddf \40f822e201b99c511fb94

4. File Audio ber-Extensi MP3

Nama file yang di uji coba dengan sistem metadata forensik ini adalah file Opick-Alhamdulillah.mp3 yang berlokasi di Folder Mp3\ISLAMI\Opick yang ada di Data E, kemudian dari pengujian tersebut di dapat hasil analisa metadatanya, berikut bisa di lihat di tabel berikut:

Tabel 4. 12 Hasil Membaca Metadata File Audio Opick-Alhamdulillah.mp3

No.	Jenis Metadata	Value
1	Folder Path	E:\Mp3\ISLAMI\Opick\Opick-Alhamdulillah.mp3
2	Name File	Opick-Alhamdulillah.mp3
3	Type File	mp3
4	Owner	S-1-5-21-2838851640-846236458-583387153-1001
5	Computer	DESKTOP-H1C8GI7
6	Creation Time	2014-06-11T08:24:51.186661Z
7	Last Access Time	2014-06-11T08:24:51.186661Z
8	Last Modified Time	2006-06-07T10:32:06Z
9	Is Directory	false
10	Is Other	false
11	Is Regular File	true
12	Is Symbolic Link	false
13	Size	1850203
14	Checksum MD5	edc517e19bb627b7b4804f057b577ae3
15	Checksum SHA-256	952594a2b8864bc1974fa11dd951dba25831dd4 cb657d989 32e7d309377e8ae0

5. File Video ber-Extensi MP4

Nama file yang di uji coba dengan sistem metadata forensik ini adalah file Dewa19-LaskarCinta.mp4 yang berlokasi di Folder MP4 yang ada di Data E, kemudian dari pengujian tersebut di dapat hasil analisa metadatanya, berikut bisa di lihat di tabel berikut:

Tabel 4. 13 Hasil Membaca Metadata File Video Dewa19-LaskarCinta.mp4

No.	Jenis Metadata	Value
1	Folder Path	E:\MP4\Dewa19-LaskarCinta.mp4
2	Name File	Dewa19-LaskarCinta.mp4
3	Type File	mp4
4	Owner	S-1-5-21-2838851640-846236458-583387153-1001
5	Computer	DESKTOP-H1C8GI7
6	Creation Time	2015-05-20T09:36:56.003425Z
7	Last Access Time	2015-05-21T02:40:53.715456Z
8	Last Modified Time	2015-05-20T10:32:02.647291Z
9	Is Directory	false
10	Is Other	false
11	Is Regular File	true
12	Is Symbolic Link	false

Lanjutan **Tabel 4. 13** Hasil Membaca Metadata File Video Dewa19-LaskarCinta.mp4

No.	Jenis Metadata	Value
13	Size	17522975
14	Checksum MD5	d3a0a69207a387db31df0a994c1d203a
15	Checksum SHA-256	74afeff05741861c91bae970d7cbc9dfef03588a8 5760afdf0468bb2ca7ea55

6. File Akuisisi ber-Extensi DD

Nama file yang di uji coba dengan sistem metadata forensik ini adalah file Metadata.dd yang berlokasi di Folder ProsesImaging yang ada di Data D, kemudian dari pengujian tersebut di dapat hasil analisa metadatanya, berikut bisa di lihat di tabel berikut:

Tabel 4. 14 Hasil Membaca Metadata File Akuisisi Metadata.dd

No.	Jenis Metadata	Value
1	Folder Path	D:\ProsesImaging\Metadata.dd
2	Name File	Metadata.dd
3	Type File	dd
4	Owner	Administrators
5	Computer	DESKTOP-H1C8GI7
6	Creation Time	2017-01-16T15:12:58.767359Z
7	Last Access Time	2017-01-16T15:12:58.767359Z
8	Last Modified Time	2017-01-16T15:17:13.10053Z
9	Is Directory	false
10	Is Other	false
11	Is Regular File	true
12	Is Symbolic Link	false
13	Size	3868623360
14	Checksum MD5	56ec0c24bb966d3a035f0696a1286dbb
15	Checksum SHA-256	a27a203679c3628a9a3413effa42208e48b597c60 a9d067e535 df091fa9643ab

7. File Akuisisi ber-Extensi E01

Nama file yang di uji coba dengan sistem metadata forensik ini adalah file Imaging.E01 yang berlokasi di Folder ProsesImaging yang ada di Data D, kemudian dari pengujian tersebut di dapat hasil analisa metadatanya, berikut bisa di lihat di tabel berikut:

Tabel 4. 15 Hasil Membaca Metadata File Akuisisi Imaging.E01

No.	Jenis Metadata	Value
1	Folder Path	D:\ProsesImaging\Imaging.E01
2	Name File	Imaging.E01
3	Type File	E01
4	Owner	Administrators
5	Computer	DESKTOP-H1C8GI7
6	Creation Time	2017-01-16T15:43:40.929069Z
7	Last Access Time	2017-01-16T15:43:40.929069Z
8	Last Modified Time	2017-01-16T15:48:08.291819Z
9	Is Directory	false
10	Is Other	false
11	Is Regular File	true
12	Is Symbolic Link	false
13	Size	3718986211
14	Checksum MD5	052fe2ccea953ad4e38f720f631deb4e
15	Checksum SHA-256	af6931acd22d13f98515a25186fb3f3cbd7a3505fd4e955effe6685087488442

Untuk melihat sejauh mana kemampuan aplikasi sistem yang telah dibangun ini, metadata file yang mampu dibaca karakteristiknya tidak hanya pada sebatas tujuh jenis file diatas, tetapi mampu membaca dan mengenali karakteristik metadata jenis file lainnya juga. Berikut dibuat juga tiga macam jenis file yang sudah dibaca karakteristik metadatanya selain dari ketujuh jenis file diatas, yaitu TXT, RAR dan HTML yang dilanjutkan dengan nomor delapan sebagai berikut:

8. File Akuisisi ber-Extensi TXT

Nama file yang di uji coba dengan sistem metadata forensik ini adalah file CEH.txt yang berlokasi di Folder ProsesImaging yang ada di Documents Data C, kemudian dari pengujian tersebut di dapat hasil analisa metadatanya, berikut bisa di lihat di tabel berikut:

Tabel 4. 16 Hasil Membaca Metadata File Text CEH.txt

No.	Jenis Metadata	Value
1	Folder Path	C:\Users\Amikom\Documents\CEH.txt
2	Name File	CEH.txt
3	Type File	txt
4	Owner	Amikom
5	Computer	DESKTOP-H1C8GI7

Lanjutan **Tabel 4. 16** Hasil Membaca Metadata File Text CEH.txt

No.	Jenis Metadata	Value
6	Creation Time	2016-04-03T07:00:16.237292Z
7	Last Access Time	2016-04-03T07:00:16.368379Z
8	Last Modified Time	2016-04-03T07:00:16.368379Z
9	Is Directory	false
10	Is Other	false
11	Is Regular File	true
12	Is Symbolic Link	false
13	Size	573
14	Checksum MD5	248fd1c76cad263cba3ce019eb6dbd06
15	Checksum SHA-256	9a8b6fc593cfbd09c303ef508a4dc0eae68d3a0f6d9948d92fa48e4b53d8b2d8

9. File Akuisisi ber-Extensi RAR

Nama file yang di uji coba dengan sistem metadata forensik ini adalah file Subli.rar yang berlokasi di Folder Tesis UII yang ada di Data D, kemudian dari pengujian tersebut di dapat hasil analisa metadatanya, berikut bisa di lihat di tabel berikut:

Tabel 4. 17 Hasil Membaca Metadata File Winrar Subli.rar

No.	Jenis Metadata	Value
1	Folder Path	D:\Tesis UII\Subli.rar
2	Name File	Subli.rar
3	Type File	rar
4	Owner	Amikom
5	Computer	DESKTOP-H1C8GI7
6	Creation Time	2017-03-14T00:31:38.257399Z
7	Last Access Time	2017-03-14T00:31:38.257399Z
8	Last Modified Time	2017-03-14T00:31:38.549597Z
9	Is Directory	false
10	Is Other	false
11	Is Regular File	true
12	Is Symbolic Link	false
13	Size	964224
14	Checksum MD5	ac843814dc81d8f75aa66f1773b5cbb8
15	Checksum SHA-256	37c011aafabe8946361fb40183470a0e24c137586b4f92415786e28af711ed22

10. File Akuisisi Ber-Extensi HTML

Nama file yang di uji coba dengan sistem metadata forensik ini adalah file Table.html yang berlokasi di Folder XML yang ada di Data D, kemudian dari pengujian tersebut di dapat hasil analisa metadatanya, berikut bisa di lihat di tabel berikut:

Tabel 4. 18 Hasil Membaca Metadata File HTML Table.html

No.	Jenis Metadata	Value
1	Folder Path	D:\XML\Table.html
2	Name File	Table.html
3	Type File	html
4	Owner	Amikom
5	Computer	DESKTOP-H1C8GI7
6	Creation Time	2015-12-07T02:48:32.830417Z
7	Last Access Time	2015-12-07T02:48:32.830417Z
8	Last Modified Time	2015-12-08T16:21:17.570859Z
9	Is Directory	false
10	Is Other	false
11	Is Regular File	true
12	Is Symbolic Link	false
13	Size	694
14	Checksum MD5	8ebfa04c6bbbf64b8a7967ec54546c0e
15	Checksum SHA-256	1f209514b3583b2d90af48e9c9f3b02d80702b5bf31a70a347f8881fe0d6eb37

4.4.2 Analisis Hasil Melakukan Korelasi File

1. Korelasi Berdasarkan Tanggal (*File Date*)

Option Sama Dengan

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata tanggalnya berupa “27 April 2016”, yang dilakukan pencarian file-file yang berlokasi di Data D dengan pilihan “Sama Dengan”, maka ditemukan hanya satu file yang tanggalnya sama dengan 27 April 2016 dari metadata tanggal file Welcome.docx yang ada di Data D tersebut. Berikut bisa di lihat hasil analisisnya dari tabel 4.19 di bawah ini:

Tabel 4. 19 Hasil Korelasi File Tanggal Opsi Sama Dengan

No.	File Name	Size	Date	Path
1	Welcome.docx	10313	27 April 2016	D:\Welcome.docx

Option Lebih Besar

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata tanggalnya berupa “27 April 2016”, yang dilakukan pencarian file-file yang berlokasi di Data D dengan pilihan “Lebih Besar”, maka ditemukan banyak sekali file-file yang tanggalnya lebih besar 27 April 2016 dari metadata tanggal file Welcome.docx yang ada di Data D tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel di jadikan sebagai analisa pencarian file berdasarkan korelasi tanggal. Berikut bisa di lihat hasil analisisnya dari tabel 4.20 di bawah ini:

Tabel 4. 20 Hasil Korelasi File Tanggal Opsi Lebih Besar

No.	File Name	Size	Date	Path
1	COVER.doc	91648	28 Oktober 2016	D:\COVER.doc
2	File	38	08 September 2016	D:\File
3	File Backup.txt	26666	03 Januari 2017	D:\File Backup.txt
4	loging.log	7	05 September 2016	D:\loging.log
5	Membuat dan Membaca File dari Java.docx	202856	08 September 2016	D:\Membuat dan Membaca File dari Java.docx
6	metadata.php	261	10 September 2016	D:\metadata.php
7	TESIS PENGARUH PENERAPAN SISTEM INFORMASI MANAJEMEN.pdf	317296	26 September 2016	D:\TESIS PENGARUH PENERAPAN SISTEM INFORMASI MANAJEMEN.pdf
8	TESIS PERENCANAAN STRATEGIS SISTEM INFORMASI.pdf	1334110	17 September 2016	D:\TESIS PERENCANAAN STRATEGIS SISTEM INFORMASI.pdf

Lanjutan **Tabel 4. 20** Hasil Korelasi File Tanggal Opsi Lebih Besar

No.	File Name	Size	Date	Path
9	TESIS SISTEM INFORMASI.txt	271	26 September 2016	D:\TESIS SISTEM INFORMASI.txt
10	Buku Wisuda 2016 Hal 30-45 baru.cdr	27020269	30 Juni 2016	D:\AMIKOM BOOK \BAH TIAR\Buku Wisuda.cdr

Option Lebih Kecil

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata tanggalnya berupa “27 April 2016”, yang dilakukan pencarian file-file yang berlokasi di Data D dengan pilihan “Lebih Kecil”, maka ditemukan banyak sekali file-file yang tanggalnya lebih kecil 27 April 2016 dari metadata tanggal file Welcome.docx yang ada di Data D tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel di jadikan sebagai analisa pencarian file berdasarkan korelasi tanggal. Berikut bisa di lihat hasil analisisnya dari tabel 4.21 di bawah ini:

Tabel 4. 21 Hasil Korelasi File Tanggal Opsi Lebih Kecil

No.	File Name	Size	Date	Path
1	Absen TK.xlsx	302532	14 April 2016	D:\Amikom-Asm\Absen TK.xlsx
2	BUKU 3A PRODI TK-2016 fix-2.docx	695319	25 April 2016	D:\Amikom-Asm\BUKU 3A PRODI TK-2016 fix-2.docx
3	Contoh surat pengantar SMA.doc	481792	11 Maret 2016	D:\Amikom-Asm\Contoh surat pengantar SMA.doc
4	KOP ASM BARU.doc	550912	14 Desember 2015	D:\Amikom-Asm\KOP ASM BARU.doc
5	surat tanpa tes.docx	423143	12 Maret 2016	D:\Amikom-Asm\surat tanpa tes.docx
6	Tesis FIX - ANggun.rar	9871547	21 April 2016	D:\Amikom-Asm\Tesis FIX - ANggun.rar
7	TK SAP N TERBARU.rar	1852891	24 Maret 2016	D:\Amikom-Asm\TK SAP N TERBARU.rar
8	AMIKOM 2015-2016.xls	104960	17 Januari 2016	D:\Amikom-Asm\Absen AMIKOM\AMIKOM 2015-2016.xls
9	Absen AMIKOM-2013-2014.xls	144384	17 Februari 2016	D:\Amikom-Asm\Absen AMIKOM\Absen AMIKOM- 2013-2014.xls
10	Absen AMIKOM-2014-2015.xls	114688	17 Januari 2016	D:\Amikom-Asm\Absen AMIKOM\Absen AMIKOM- 2014-2015.xls

Option Lebih Kecil Sama Dengan

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata tanggalnya berupa “27 April 2016”, yang dilakukan pencarian file-file yang berlokasi di Data D dengan pilihan “Lebih Kecil Sama Dengan”, maka ditemukan banyak sekali file-file yang tanggalnya lebih kecil sama dengan 27 April 2016 dari metadata tanggal file Welcome.docx yang ada di Data D tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel yang dijadikan sebagai analisa pencarian file berdasarkan korelasi tanggal. Berikut bisa di lihat hasil analisisnya dari tabel 4.22 di bawah ini:

Tabel 4. 22 Hasil Korelasi File Tanggal Opsi Lebih Kecil Sama Dengan

No.	File Name	Size	Date	Path
1	file.txt	92	07 Oktober 2015	D:\New\file.txt
2	hash.py	19451	10 Oktober 2015	D:\New\hash.py
3	hashing.py	7491	10 Oktober 2015	D:\New\hashing.py
4	Hasil.E03	391248949	29 Mei 2015	D:\New\Hasil.E03
5	image.py	1830	10 Oktober 2015	D:\New\image.py
6	read.py	413	07 Oktober 2015	D:\New\read.py
7	Reference.py	1312	21 Desember 2015	D:\New\Reference.py
8	subli.jpg	5117665	27 Mei 2013	D:\New\subli.jpg
9	Tabel.py	2586	21 Desember 2015	D:\New\Tabel.py
10	Welcome.docx	10313	27 April 2016	D:\New>Welcome.docx

Option Lebih Besar Sama Dengan

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata tanggalnya berupa “27 April 2016”, yang dilakukan pencarian file-file yang berlokasi di Data D dengan option pilihan “Lebih Besar Sama Dengan”, maka ditemukan banyak sekali file-file yang tanggalnya lebih besar sama dengan 27 April 2016 dari metadata tanggal file Welcome.docx yang ada di Data D tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel yang dijadikan sebagai analisa pencarian file berdasarkan korelasi tanggal. Berikut bisa di lihat hasil analisisnya dari tabel 4.23 di bawah ini:

Tabel 4. 23 Hasil Korelasi File Tanggal Opsi Lebih Besar Sama Dengan

No.	File Name	Size	Date	Path
1	COVER.doc	91648	28 Oktober 2016	D:\New\COVER.doc
2	File	38	08 September 2016	D:\New\File
3	File Backup.txt	26666	03 Januari 2017	D:\New\File Backup.txt
4	loging.log	7	05 September 2016	D:\New\loging.log
5	Membuat dan Membaca File dari Java.docx	202856	08 September 2016	D:\New\Membuat dan Membaca File dari Java.docx
6	metadata.php	261	10 September 2016	D:\New\metadata.php
7	TESIS PENGARUH PENERAPAN SISTEM INFORMASI MANAJEMEN.pdf	317296	26 September 2016	D:\New\TESIS PENGARUH PENERAPAN SISTEM INFORMASI MANAJEMEN.pdf
8	TESIS PERENCANAAN STRATEGIS SISTEM INFORMASI.pdf	1334110	17 September 2016	D:\New\TESIS PERENCANAAN STRATEGIS SISTEM INFORMASI.pdf
9	TESIS SISTEM INFORMASI.txt	271	26 September 2016	D:\New\TESIS SISTEM INFORMASI.txt
10	Welcome.docx	10313	27 April 2016	D:\New>Welcome.docx

2. Korelasi Berdasarkan Ukuran (*File Size*)

Option Sama Dengan

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata ukuran filenya berupa “10.313 byte”, yang dilakukan pencarian file-file yang berlokasi di Data D dengan pilihan “Sama Dengan”, maka ditemukan hanya dua file yang ukuran filenya sama dengan 10.313 byte dari metadata ukuran file Welcome.docx yang ada di Data D tersebut. Berikut bisa dilihat hasil analisisnya dari tabel 4.24 di bawah ini:

Tabel 4. 24 Hasil Korelasi File Ukuran Opsi Sama Dengan

No.	File Name	Size	Date	Path
1	7seg.lss	10313	04 November 2010	D:\Jadi Satu\Seven Segments\default\7seg.lss
2	Welcome.docx	10313	27 April 2016	D:\New>Welcome.docx

Option Lebih Besar

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata ukuran filenya berupa “10.313 byte”, yang dilakukan pencarian file-file yang berlokasi di Data E dengan pilihan “Lebih Besar”, maka ditemukan banyak sekali file-file yang ukuran filenya lebih besar 10.313 byte dari metadata ukuran file Welcome.docx yang ada di Data E tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel yang dijadikan sebagai analisa pencarian file berdasarkan korelasi ukuran file. Berikut bisa di lihat hasil analisisnya dari tabel 4.25 di bawah ini:

Tabel 4. 25 Hasil Korelasi File Ukuran Opsi Lebih Besar

No.	File Name	Size	Date	Path
1	Akhlakul Rasulullah SAW.pptx	1155864 6	13 Desember 2015	E:\Akhlakul Rasulullah SAW.pptx
2	IMG_20160604_174441.jpg	371024	25 September 2016	E:\IMG_20160604_174441.jpg
3	Kata-Motivasi-Hidup.jpeg	90719	25 September 2016	E:\Kata-Motivasi-Hidup.jpeg
4	Amikom-Asm Mataram.ppt	2509312	02 April 2016	E:\Amikom-Asm Mataram.ppt
5	Koperasi.accdb	520192	16 Juli 2016	E:\Koperasi.accdb
6	[1] PAI.doc	233984	20 September 2010	E:\1. PAI-Prangkat PmbIjran karakter [KTSP]\[1] PAI.doc
7	100 TOKOH.chm	1281966	02 Desember 2005	E:\AGAMA\AL-QURAN dan al-HADITS\100 TOKOH.chm
8	Abu Hanifah.mp3	8620784 2	11 September 2009	E:\AGAMA\BIOGRAFI 4 IMAM (MP3)\Biografi Imam Abu Hanifah rahimahullah\Abu Hanifah.mp3
9	100_tokoh yg berpengaruh dlm sejarah.chm	1281966	04 Desember 2005	E:\AGAMA\Buku Islami\100_tokoh yg berpengaruh dlm sejarah.chm
10	10 Sebab Di Cintai Allah.ppt	126976	28 Desember 2006	E:\AGAMA\dari akh Riza\10 Sebab Di Cintai Allah.ppt

Option Lebih Kecil

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata ukuran filenya berupa “10.313 byte”, yang dilakukan pencarian file-file yang berlokasi di Data E dengan pilihan “Lebih Kecil”, maka ditemukan banyak sekali file-file yang ukuran filenya lebih kecil 10.313 byte dari metadata ukuran file Welcome.docx yang ada di Data E tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel yang dijadikan sebagai analisa pencarian file berdasarkan korelasi ukuran file. Berikut bisa di lihat hasil analisisnya dari tabel 4.26 di bawah ini:

Tabel 4. 26 Hasil Korelasi File Ukuran Opsi Lebih Kecil

No.	File Name	Size	Date	Path
1	desktop.ini	129	23 November 2015	E:\\$RECYCLE.BIN\S-1-5-21-316737675-2236937756-87291139-1001\desktop.ini
2	banner_islami cshop.gif	64	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\banner_islamicshop.gif
3	cvjasatama.gif	2539	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\cvjasatama.gif
4	digiquran.gif	2052	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\digiquran.gif
5	frames.js	3098	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\frames.js
6	online.gif	1102	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\online.gif
7	QuranDigital.gif	3072	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\QuranDigital.gif
8	smartquran.gif	2767	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\smartquran.gif
9	spacer.png	218	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\spacer.png
10	top_bar.jpg	589	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\top_bar.jpg

Option Lebih Kecil Sama Dengan

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata ukuran filenya berupa “10.313 byte”, yang dilakukan pencarian file-file yang berlokasi di Data E dengan pilihan “Lebih Kecil Sama Dengan”, maka ditemukan banyak sekali file-file yang ukuran filenya lebih kecil sama dengan 10.313 byte dari metadata ukuran file Welcome.docx yang ada di Data E tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel yang dijadikan sebagai

analisa pencarian file berdasarkan korelasi ukuran file. Berikut bisa di lihat hasil analisisnya dari tabel 4.27 di bawah ini:

Tabel 4. 27 Hasil Korelasi File Ukuran Opsi Lebih Kecil Sama Dengan

No.	File Name	Size	Date	Path
1	QuranDigital.gif	3072	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\QuranDigital.gif
2	smartquran.gif	2767	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\smartquran.gif
3	spacer.png	218	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\spacer.png
4	top_bar.jpg	589	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\top_bar.jpg
5	Desktop.ini	78	20 Oktober 2007	E:\AGAMA\Nasehat 1\Desktop.ini
6	Risalah Ramadhan.pdf	0	16 Juli 2012	E:\AGAMA\Ramadhan & Zakat\Risalah Ramadhan.pdf
7	1_1.gif	832	13 Juni 2003	E:\Al Qur'an\Al-quran digital\0-Al-Qur'an & Nabi\AL-QUR'AN DIGITAL\GIF\1\1_1.gif
8	1_2.gif	789	13 Juni 2003	E:\Al Qur'an\Al-quran digital\0-Al-Qur'an & Nabi\AL-QUR'AN DIGITAL\GIF\1\1_2.gif
9	1_3.gif	699	13 Juni 2003	E:\Al Qur'an\Al-quran digital\0-Al-Qur'an & Nabi\AL-QUR'AN DIGITAL\GIF\1\1_3.gif
10	1_4.gif	689	13 Juni 2003	E:\Al Qur'an\Al-quran digital\0-Al-Qur'an & Nabi\AL-QUR'AN DIGITAL\GIF\1\1_4.gif

Option Lebih Besar Sama Dengan

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata ukuran filenya berupa “10.313 byte”, yang dilakukan pencarian file-file yang berlokasi di Data E dengan pilihan “Lebih Besar Sama Dengan”, maka ditemukan banyak sekali file-file yang ukuran filenya lebih besar sama dengan 10.313 byte dari metadata ukuran file Welcome.docx yang ada di Data E tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel yang dijadikan sebagai analisa pencarian file berdasarkan korelasi ukuran file. Berikut bisa di lihat hasil analisisnya dari tabel 4.28 di bawah ini:

Tabel 4. 28 Hasil Korelasi File Ukuran Opsi Lebih Besar Sama Dengan

No.	File Name	Size	Date	Path
1	Toleransi Seorang Shalahuddin al.doc	33280	23 Oktober 2008	E:\Religius\Islam\DAQWAH\Toleransi Seorang Shalahuddin al.doc
2	TUJUH GOLONGAN YANG AKAN BERNAUNG DI BAWAH.doc	26112	21 November 2008	E:\Religius\Islam\DAQWAH\TUJUH GOLONGAN YANG AKAN BERNAUNG DI BAWAH.doc
3	TUJUH HAL YANG MERUPAKAN SEBAB AKIBAT.doc	30208	08 Januari 2011	E:\Religius\Islam\DAQWAH\TUJUH HAL YANG MERUPAKAN SEBAB AKIBAT.doc
4	Tujuh Macam Pahala.doc	64512	28 Mei 2009	E:\Religius\Islam\DAQWAH\Tujuh Macam Pahala.doc
5	TUJUH POIN SABDA NABI TENTANG DUNIA.doc	28160	08 Januari 2011	E:\Religius\Islam\DAQWAH\TUJUH POIN SABDA NABI TENTANG DUNIA.doc
6	Yaa Allah Berkahilah Kami di Bulan Rajab.doc	35328	19 April 2009	E:\Religius\Islam\DAQWAH\Yaa Allah Berkahilah Kami di Bulan Rajab.doc
7	Yang Manakah Anda.doc	27136	06 Mei 2009	E:\Religius\Islam\DAQWAH\Yang Manakah Anda.doc
8	yyidina muhammad wa aalihi washohbihi wassalim.docx	80715	15 Januari 2011	E:\Religius\Islam\DAQWAH\yyidina muhammad wa aalihi washohbihi wassalim.docx
9	bagaimana_seorang muslim_berpikir.rtf	272040	02 Maret 2004	E:\Religius\Islam\Harun Yahya E-book\bagaimana_seorang muslim_berpikir.rtf
10	Bagaimana_seorangmuslim_berpikir.pdf	2464332	02 Maret 2004	E:\Religius\Islam\Harun Yahya E-book\Bagaimana seorang muslim_berpikir.pdf

Option Antara

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata ukuran filenya berupa “10.313 byte”, yang dilakukan pencarian file-file yang berlokasi di Data E dengan pilihan “Antara”, dimana ukuran file yang di inputkan dari yang ukuran file yang bernilai batas minimal sampai dengan ukuran file yang bernilai batas maksimal, sehingga file-file yang akan di cari yaitu ukuran file yang ada diantara nilai batas minimal sampai dengan batas maksimal yang telah di inputkan. Dalam pengujian dan analisa ini, di inputkan ukuran file 10.000 byte untuk nilai batas

minimal dan 50.000 byte untuk nilai batas maksimal. Maka ditemukan banyak sekali file-file yang ukuran filenya diantara 10.000 byte sampai dengan 50.000 byte yang ada di Data E tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel yang dijadikan sebagai analisa pencarian file berdasarkan korelasi ukuran file opsi antara. Berikut bisa di lihat hasil analisisnya dari tabel 4.29 di bawah ini:

Tabel 4. 29 Hasil Korelasi File Ukuran Opsi Antara

No.	File Name	Size	Date	Path
1	Al Quran Digital.chw	20318	28 Februari 2012	E:\AGAMA\AL-QURAN dan al-HADITS\Al Quran Digital.chw
2	Share-e qurban.xls	13824	02 November 2012	E:\AGAMA\dari akh Riza\Share-e qurban.xls
3	Peserta HIT.xls	13824	02 November 2012	E:\AGAMA\dari akh Riza\Peserta HIT.xls
4	Orang Tayli.PDF	38074	11 Januari 2001	E:\AGAMA\Fiqih dan Mutiara Hikmah\Orang Tayli.PDF
5	Pic06868.jpg	39479	06 Mei 2002	E:\AGAMA\Islam & Science\Pic06868.jpg
6	Gender Equity In Islam.pdf	45213	27 Mei 2002	E:\AGAMA\Islam, Women & Family\Gender Equity In Islam.pdf
7	Ro'yu ttg muh bin ishaq.pdf	42339	11 Januari 2001	E:\AGAMA\Kajian Islami\Ro'yu ttg muh bin ishaq.pdf
8	Kami Berikan Cobaan Kepadamu.pdf	29045	11 Januari 2001	E:\AGAMA\Kajian Islami\Kami Berikan Cobaan Kepadamu.pdf
9	el-haji.gif	12639	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\el-haji.gif
10	template_css.css	10874	21 November 2006	E:\AGAMA\Keluarga Islami\Keluarga Sakinah_files\template_css.css

3. Korelasi Berdasarkan Ektensi (*File Type*)

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata ekstensi filenya berupa “docx”, yang dilakukan pencarian file-file yang berlokasi di Data E dengan option File Type, maka ditemukan banyak sekali file-file yang ekstensi filenya docx dari metadata file type Welcome.docx yang ada di Data E tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel yang dijadikan sebagai analisa pencarian file berdasarkan korelasi file type. Berikut bisa di lihat hasil analisisnya dari tabel 4.30 di bawah ini:

Tabel 4. 30 Hasil Korelasi File Berdasarkan Ektensi File

No.	File Name	Size	Date	Path
1	CARA MEMBUAT MAKALAH YANG BAIK.docx	40633	04 Juni 2016	E:\ASM Mataram 2016\CARA MEMBUAT MAKALAH YANG BAIK.docx
2	Fungsi Tombol Pada Keyboard.docx	44725	30 April 2016	E:\ASM Mataram 2016\Fungsi Tombol Pada Keyboard.docx
3	VLOOKUP dan HLOOKUP.docx	161683	07 Mei 2016	E:\ASM Mataram 2016\VLOOKUP dan HLOOKUP.docx
4	409875558039646.docx	8691	17 September 2016	E:\Backup Android\Telegram\Telegram Documents\409875558039646.docx
5	JADWAL PELAJARAN KELAS.docx	12089	25 Agustus 2014	E:\Bahan Pembinaan Gugus Sekotong\JADWAL PELAJARAN KELAS.docx
6	KALDIK TH. 2014-2015 LOBAR.docx	69002	13 Juni 2014	E:\Bahan Pembinaan Gugus Sekotong\KALDIK TH. 2014-2015 LOBAR.docx
7	Kalender Pendidikan.docx	12321	25 Agustus 2014	E:\Bahan Pembinaan Gugus Sekotong\Kalender Pendidikan.docx
8	PROGRAM SEMESTER GANJIL.docx	13852	25 Agustus 2014	E:\Bahan Pembinaan Gugus Sekotong\PROGRAM SEMESTER GANJIL.docx
9	PROGRAM SEMESTER GENAP.docx	13854	25 Agustus 2014	E:\Bahan Pembinaan Gugus Sekotong\PROGRAM SEMESTER GENAP.docx
10	PROGRAM TAHUNAN.docx	12209	25 Agustus 2014	E:\Bahan Pembinaan Gugus Sekotong\PROGRAM TAHUNAN.docx

4. Korelasi Berdasarkan Pemilik (*File Owner*)

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata owner atau pemilik filenya berupa “Amikom”, yang dilakukan pencarian file-file yang berlokasi di Data D dengan option Owner, maka ditemukan banyak sekali file-file yang owner atau pemilik filenya Amikom dari metadata owner file Welcome.docx yang ada di Data D tersebut, tetapi dari sekian banyak file yang sudah ditemukan, diambil sepuluh sampel yang dijadikan sebagai analisa pencarian file berdasarkan korelasi owner file. Berikut bisa di lihat hasil analisisnya dari tabel 4.31 di bawah ini:

Tabel 4. 31 Hasil Korelasi File Berdasarkan Pemilik File

No.	File Name	Size	Date	Path
1	Tugas CHFI.docx	706260	27 Mei 2016	D:\S2 UII\Tugas CHFI.docx
2	indo_06_13.xls	47616	14 Januari 2016	D:\S2 UII\Semester I\SPK & Business Intelligence\tugas2-14917148\indo_06_13.xls
3	JUMLAH TENAGA MEDIS 2003-2012 (Data yang diolah).xlsx	994225	14 Januari 2016	D:\S2 UII\Semester I\Visualisasi Data BI\JUMLAH TENAGA MEDIS 2003-2012 (Data yang diolah).xlsx
4	Laporan Visualisasi Data.docx	2145635	14 Januari 2016	D:\S2 UII\Semester I\Visualisasi Data BI\Laporan Visualisasi Data.docx
5	tenaga-kesehatan-per-provinsi-2000-2012.csv	176519	12 Januari 2016	D:\S2 UII\Semester I\Visualisasi Data BI\tenaga-kesehatan-per-provinsi-2000-2012.csv
6	JUMLAH TENAGA MEDIS 2003-2012.xlsx	1054086	14 Januari 2016	D:\S2 UII\Semester I\JUMLAH TENAGA MEDIS 2003-2012).xlsx
7	Laporan Visualisasi Data.docx	2868488	14 Januari 2016	D:\S2 UII\Semester I\Laporan Visualisasi Data.docx
8	Pelengkap Laporan.docx	13160	18 Januari 2016	D:\S2 UII\Semester III\Olah TKP\Ex UAS Laporan Olah TKP\Pelengkap Laporan.docx
9	Laporan Olah TKP.docx	4448169	31 Januari 2016	D:\S2 UII\Semester III\Olah TKP\Laporan FINAL O-TKP\Laporan Olah TKP.docx
10	Laporan Olah TKP.pdf	2102989	31 Januari 2016	D:\S2 UII\Semester III\Olah TKP\Laporan FINAL O-TKP\Laporan Olah TKP.pdf

5. Korelasi File dari Gabungan Beberapa Jenis Korelasi

Untuk hasil metadata file yang dikorelasi yaitu file Welcome.docx yang metadata ukuran filenya “10313 byte”, pemilik filenya berupa “Amikom” dan ekstensi file “docx” yang dilakukan pencarian file-file yang berlokasi di Documents Data C dengan option korelasi mulai dari Size dengan option Lebih Besar Sama Dengan, Owner dan File Type maka ditemukan banyak sekali file-file yang metadata size filenya “10313 byte” dengan option Lebih Besar Sama Dengan, pemilik filenya berupa “Amikom” dan ekstensi file “docx” dari metadata file Welcome.docx yang ada di Documents Data C, tetapi dari sekian banyak file yang sudah ditemukan, diambil hanya sepuluh

sampel yang dijadikan sebagai analisa pencarian file berdasarkan gabungan dari beberapa jenis korelasi tersebut. Berikut bisa di lihat hasil analisisnya dari tabel 4.32 di bawah ini:

Tabel 4. 32 Korelasi File dari Gabungan Beberapa Jenis Korelasi

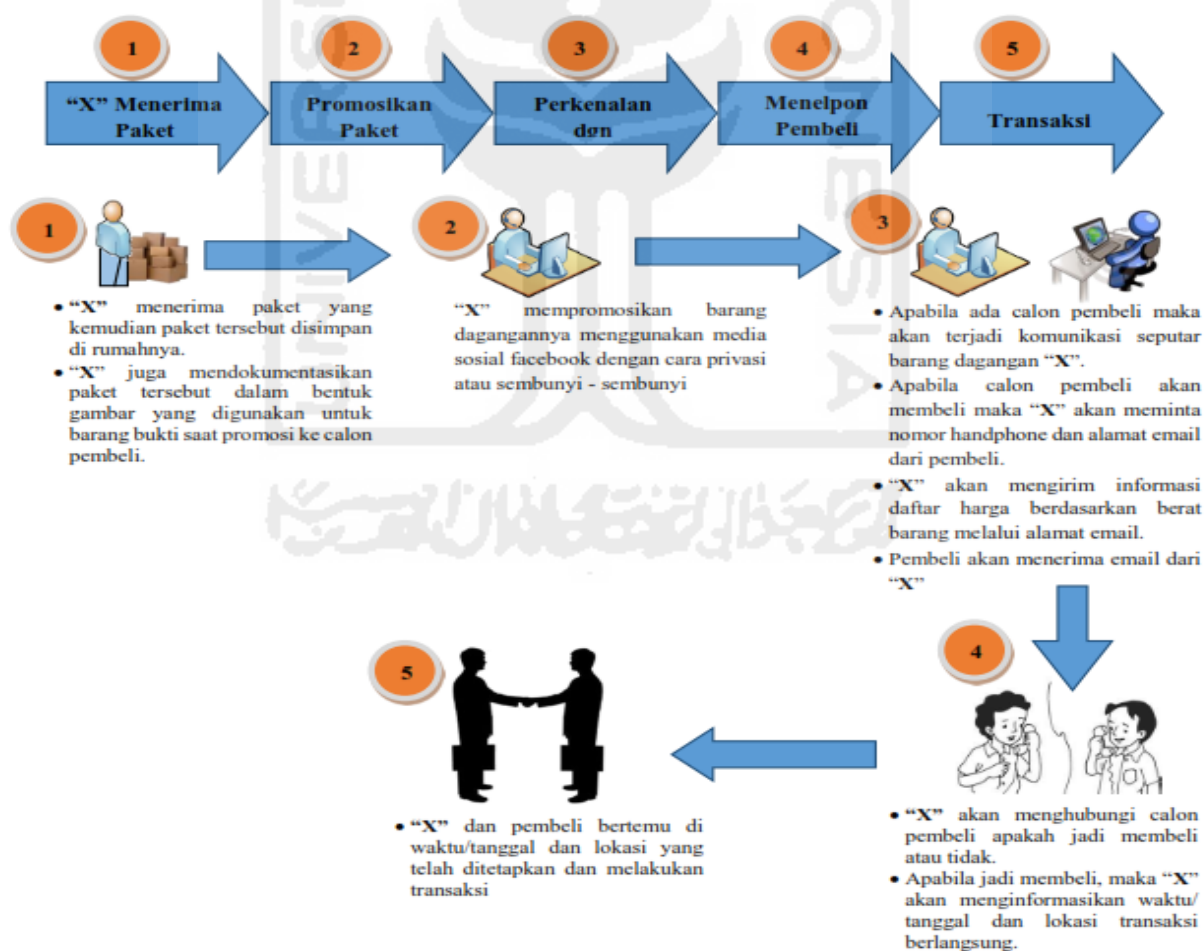
No.	File Name	Size	Date	Path
1	PELATIHAN CEH DAN CHFI.docx	17906	22 Januari 2016	C:\Users\Amikom\Documents\PELATIHAN CEH DAN CHFI.docx
2	ACARA MAULID.docx	10517077	02 Juli 2016	C:\Users\Amikom\Documents\ACARA MAULID.docx
3	ACARA NUZULUL.docx	25702032	01 Juli 2016	C:\Users\Amikom\Documents\ACARA NUZULUL.docx
4	Algoritma SHA Dengan Java.docx	36233	03 September 2016	C:\Users\Amikom\Documents\Algoritma SHA Dengan Java.docx
5	Backpacker Jogja-Lombok.docx	17112	19 Desember 2015	C:\Users\Amikom\Documents\Backpacker Jogja-Lombok.docx
6	Belajar Basic OOP di Python.docx	20164	10 Desember 2015	C:\Users\Amikom\Documents\Belajar Basic OOP di Python.docx
7	Business Intelegence in Blue Bird Corporation.docx	16142	10 Desember 2015	C:\Users\Amikom\Documents\Business Intelegence in Blue Bird Corporation.docx
8	VM VirtualBox dan VirtualBox Extensions Pack.docx	805697	23 November 2015	C:\Users\Amikom\Documents\ VM VirtualBox dan VirtualBox Extensions Pack.docx
9	Cara Membagi Partisi Hardisk External Tanpa Software.docx	358375	15 Desember 2015	C:\Users\Amikom\Documents\Cara Membagi Partisi Hardisk External Tanpa Software.docx
10	Partisi Hardisk EASEUS Partition Master.docx	293177	15 Desember 2015	C:\Users\Amikom\Documents\Partisi Hardisk EASEUS Partition Master.docx

Semua hasil analisa yang sudah ditampilkan dalam tabel-tabel diatas, di dapatkan sebuah metadata file yang dibaca secara umum yang tidak terlaui spesifikasikan dalam pembacaan metadatanya, contohnya file JPG mempunyai nilai metadata merk kamera waktu pemoretannya dan file MP4 mempunyai nilai metadata *frame rate*, ini tentunya mempunyai nilai metadata yang berbeda dan lebih spesifik lagi, tetapi dalam analisa pembacaan metadata ini yang ditampilkan sama semua yaitu pembacaan metadata file secara umum dan ditemukan juga beberapa file dalam proses korelasi metadata file tersebut dari tampilan hasil korelasi yang dimunculkan itu adalah Nama File (*File Name*), Ukuran File (*Size*), Tanggal File (*Date*) dan Lokasi File (*Path*).

4.5 Studi Kasus dengan Melakukan Pendekatan Metadata

Pada tanggal 28 Agustus 2015 “X” mendapat kiriman paket narkoba jenis sabu-sabu untuk di edarkan dan dijual ke wilayah Jawa Barat. Beberapa bulan kemudian transaksi yang dilakukan oleh “X” mulai menembus wilayah Jawa Tengah dan Jawa Timur, karena jarak antara wilayah yang sangat jauh sehingga “X” terpikir untuk melibatkan teknologi informasi dalam aksinya.

Pada bulan September 2015 “X” mulai melibatkan jaringan internet lewat media sosial Facebook untuk memperkenalkan dagangannya kepada calon pembeli secara privasi atau sembunyi-sembunyi. Berawal dari komunikasi media facebook transaksi dilakukan dan apabila calon pembeli tertarik untuk membeli maka “X” akan meminta nomor telepon/handphone dari calon pembeli untuk membahas lebih lanjut tentang harga jual, berat barang yang akan dibeli, dan lokasi transaksi serta untuk memudahkannya maka “X” akan meminta alamat email calon pembeli untuk mengirimkan data-data tersebut adapun dalam kiriman tersebut juga dilampirkan foto dari barang yang akan dibeli oleh calon. Berikut adalah gambar alur proses kasus transaksi narkoba:



Gambar 4. 24 Alur Proses Kasus Transaksi Narkoba

Barang Bukti

Pada kasus transaksi narkoba tersebut, dapat diketahui berbagai jenis barang bukti teknologi informasi yang digunakan, barang bukti tersebut dapat digolongkan menjadi 2 bagian yaitu :

1. Barang Bukti Elektronik

Barang bukti elektronik yang digunakan adalah :

- a. Handphone berfungsi sebagai alat komunikasi.
- b. Laptop sebagai media untuk mengetik data, edit gambar dan melakukan komunikasi media sosial facebook
- c. Modem sebagai perangkat jaringan internet
- d. Sim Card yang digunakan untuk modem dan Handphone
- e. Thumbdrive Toshiba tempat penyimpanan bukti-bukti kasus transaksi narkoba

2. Barang Bukti Digital

Barang bukti digital yang digunakan adalah :

- a. Facebook
- b. Email
- c. Dokumen
- d. Gambar

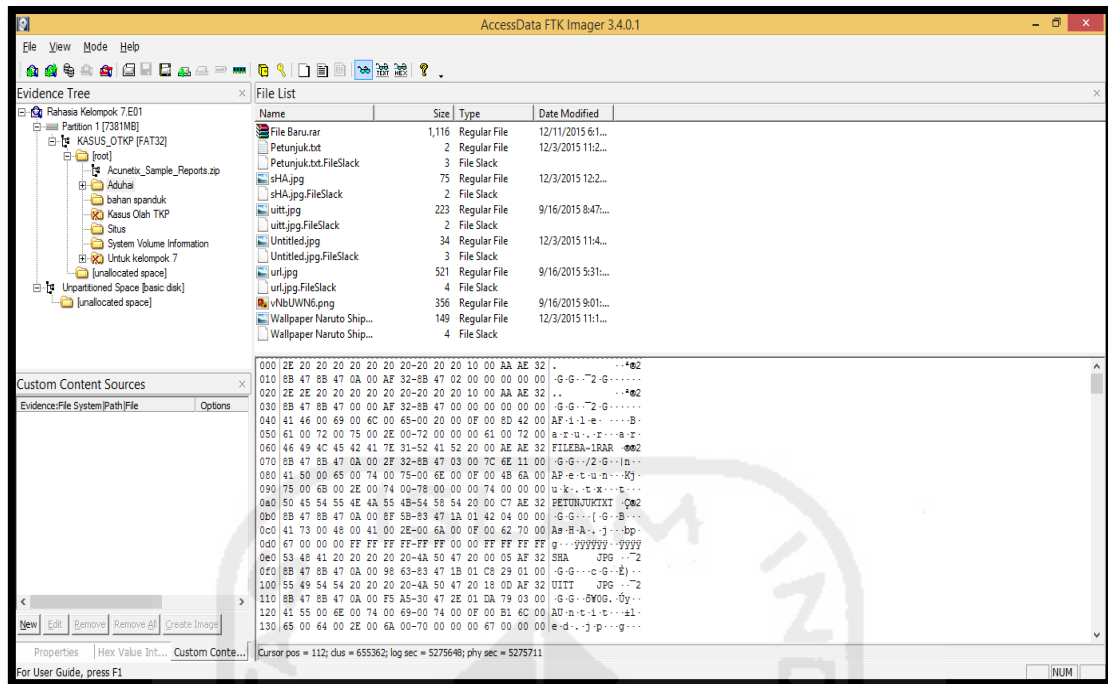
Pekerjan Investigasi

Menemukan keterlibatan “X” yang dapat memberatkannya di Pengadilan, barang bukti yang harus ditemukan adalah :

1. Temukan password di setiap barang bukti
2. File dokumen berupa daftar harga sabu-sabu
3. Gambar sabu-sabu sebagai contoh ilustrasi bukti sabu-sabu dari penjual kepada pembeli

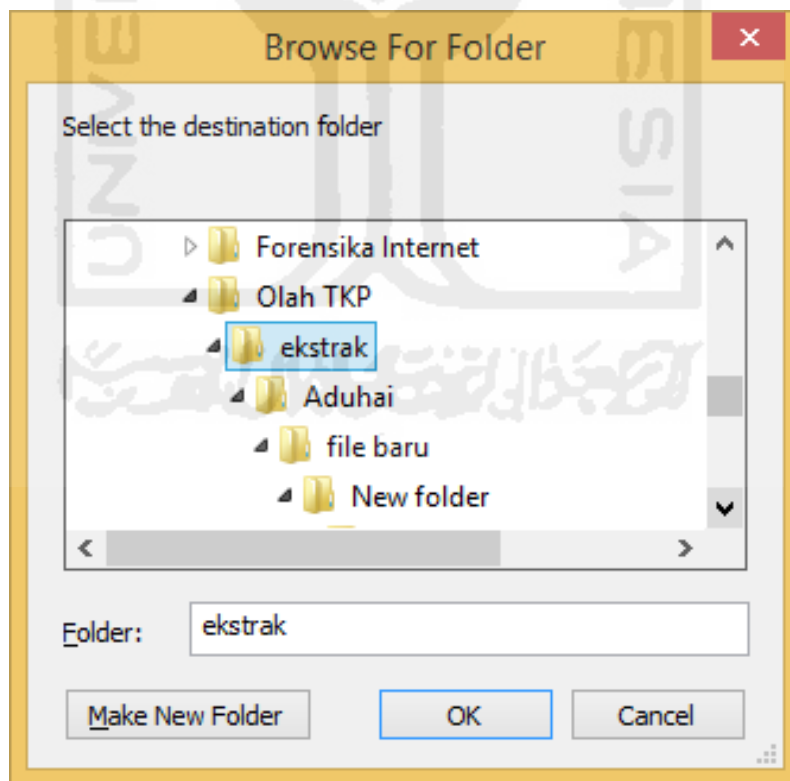
Analisa

1. Langkah pertama membuka bukti digital “Rahasia Kelompok 7.E01” dari barang bukti elektronik *Thumbdrive* Toshiba pada tools FTK Imager 3.4.0.1 seperti gambar 4.25 di bawah ini:



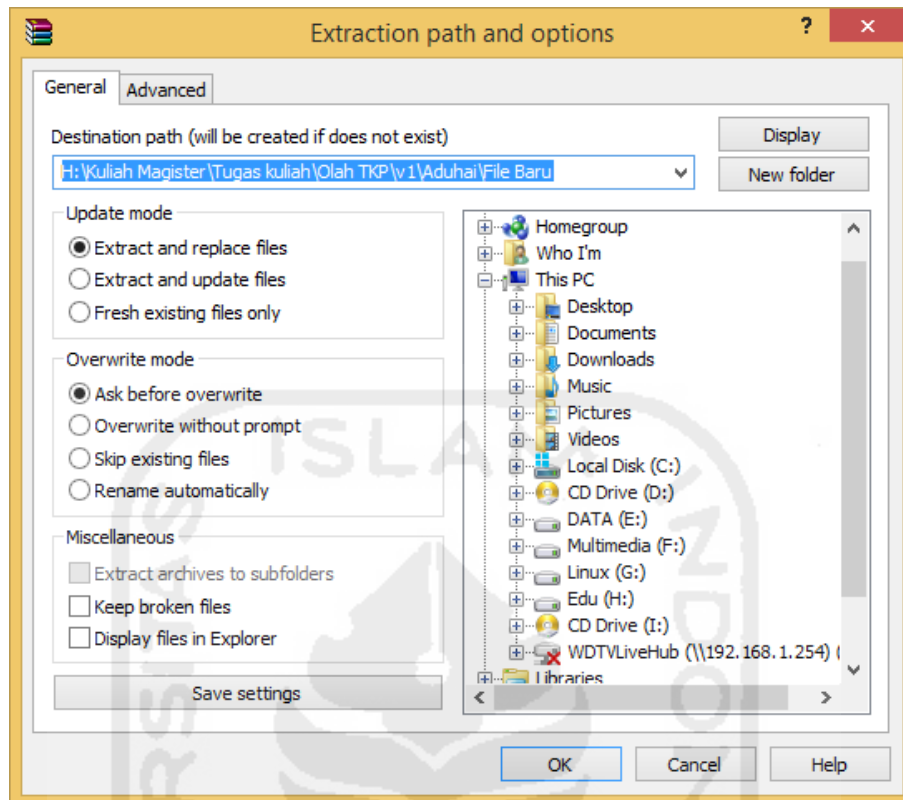
Gambar 4. 25 File Akuisi “Rahasia Kelompok 7.E01”

- Langkah kedua melakukan *export file* bukti digital ke salah satu folder di Laptop/PC



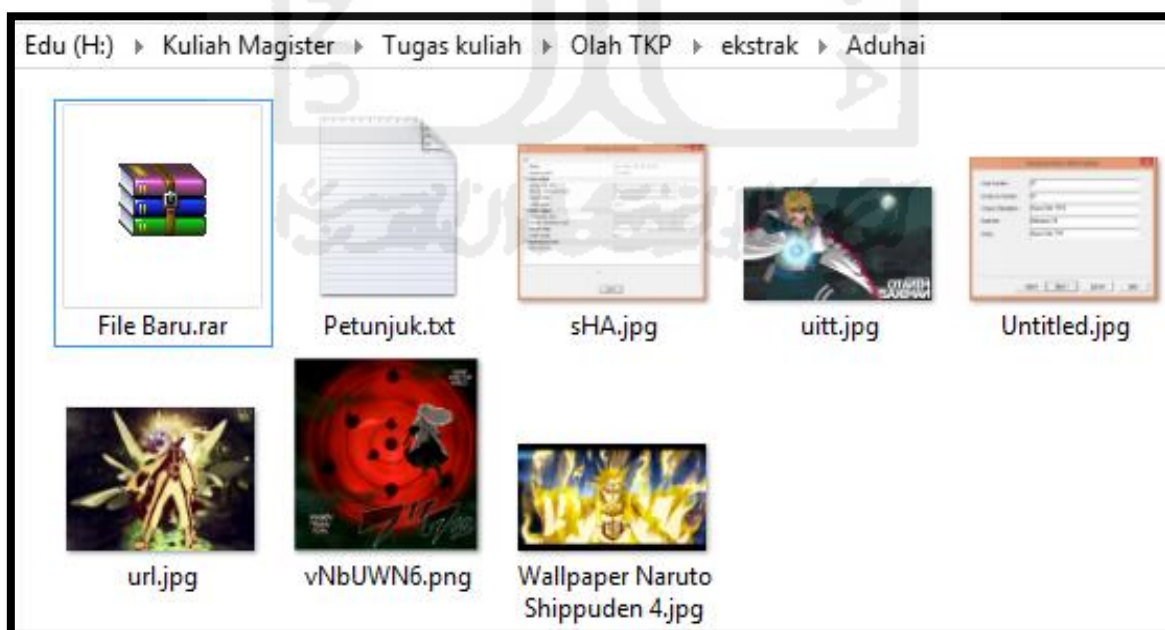
Gambar 4. 26 Export File Bukti Digital

3. Proses ekstraksi file Aduhai seperti pada gambar 4. 27



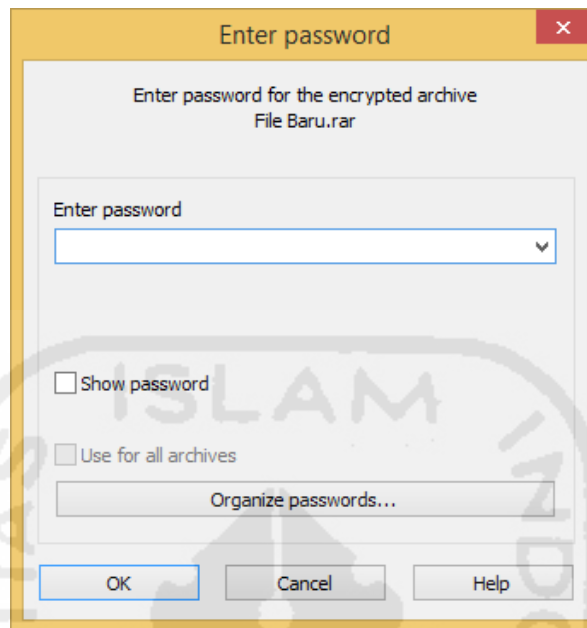
Gambar 4. 27 Proses Ekstraksi File Aduhai

4. Tampilan hasil ekstraksi folder Aduhai



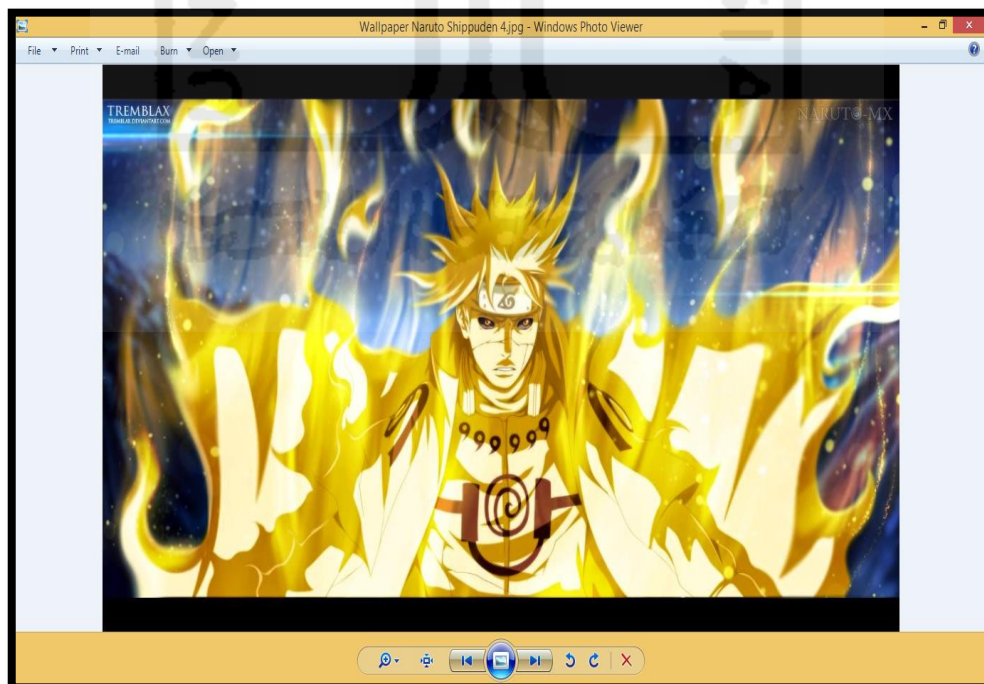
Gambar 4. 28 Hasil Ekstraksi Folder Aduhai

5. Langkah selanjutnya melakukan ekstraksi pada file “Baru.rar” yang ternyata menggunakan *password*



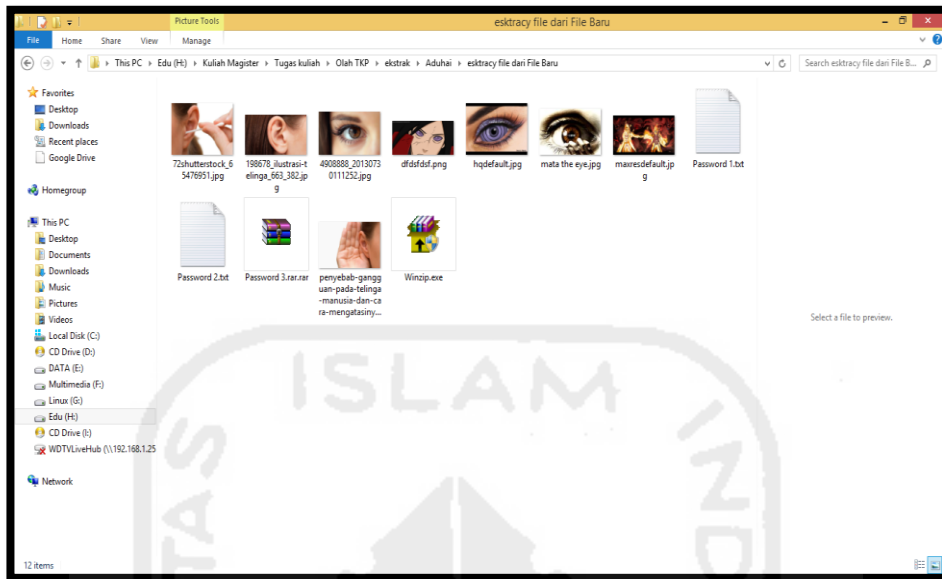
Gambar 4. 29 Enter Password File Baru.rar

6. Langkah berikutnya melakukan pencairan kata kunci atau password “File Baru.rar dengan mencoba kata atau angka yang ada di beberapa file gambar di folder aduhai dan akhirnya menemukan kata *password* Baru.rar “9” seperti terlihat pada gambar 4. 30 dibawah ini:



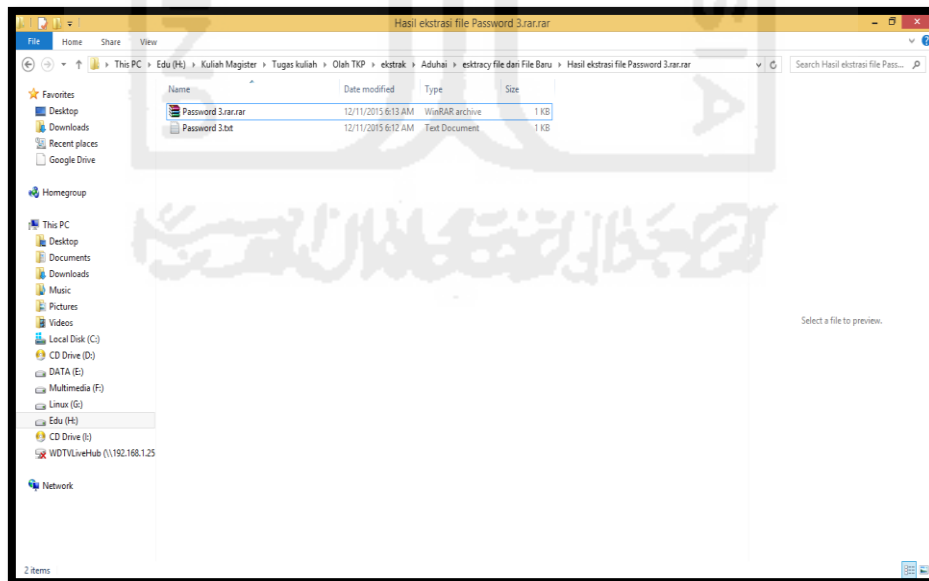
Gambar 4. 30 Kata Password Baru.rar “9”

7. Setelah ditemukan password “File Baru.rar” langkah selanjutnya melakukan ekstraksi dan hasil ekstraksi pada file Baru yang terlihat pada gambar 4. 31 dibawah ini:



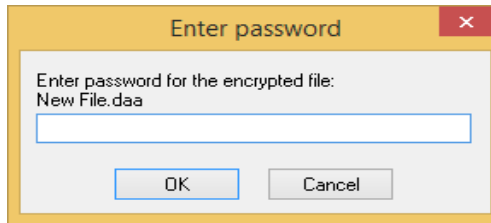
Gambar 4. 31 Hasil Ekstraksi File Baru

8. Langkah selanjutnya melakukan pencairan bukti-bukti kasus yang di perintahkan pada saat penugasan investigasi dengan ekstraksi lagi file Baru.rar dengan nama “Password 3.rar.rar” dengan kata kunci dari file Baru.rar tersebut adalah Password 3.rar.rar



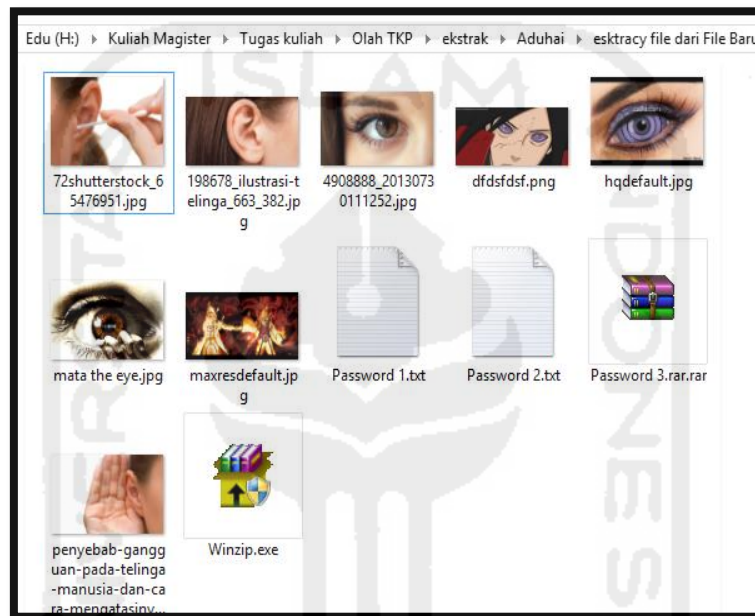
Gambar 4. 32 Ekstraksi Lagi File Baru.rar

9. Ternyata setelah di eksteraksi file tersebut hanya sebaga file pengecoh examiner dari pelaku kejahatan melainkan bukan bukti yang di cari



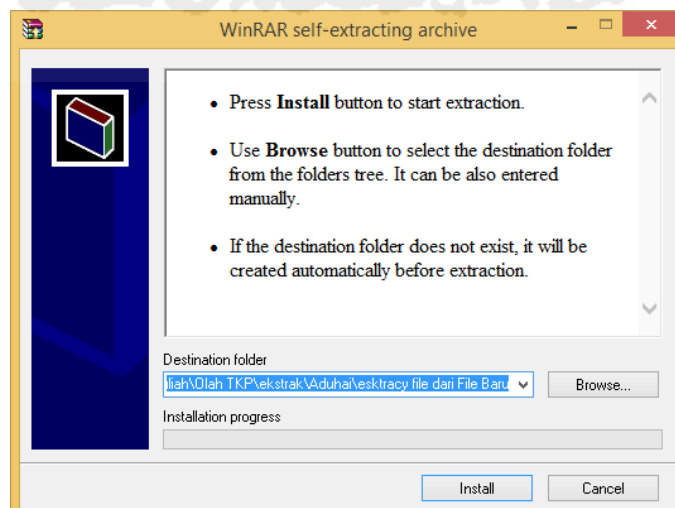
Gambar 4. 33 File Pengecoh Enter Password

10. Langkah selanjutnya mengecek sebuah file berextensi .exe dengan nama file Winzip.exe yang kemungkinan menyembunyikan bukti-bukti yang selama ini di cari



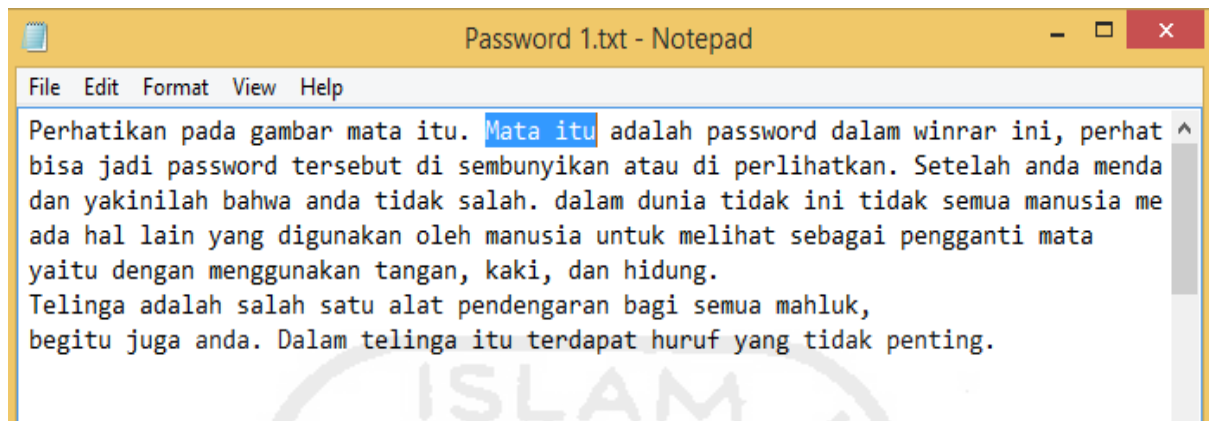
Gambar 4. 34 File Winzip.exe

11. Proses berikutnya instalasi file yang di duga menyimpan bukti-bukti dari kejahatan tersebut dengan file Winzip.exe



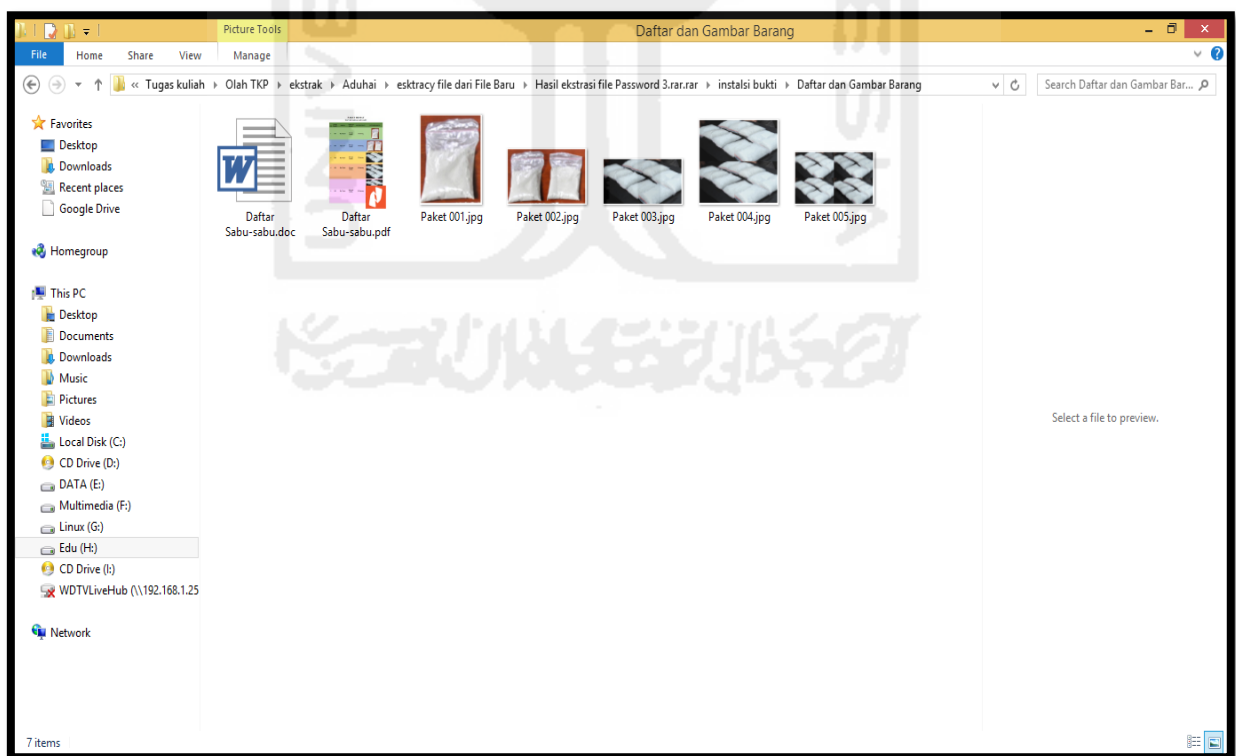
Gambar 4. 35 Instalasi File Winzip.exe

12. Dalam langkah instalasi file Winzip.exe harus memasukan kata kunci. Kata kunci atau password instalasi dari file Winzip.exe adalah “Mata itu”



Gambar 4. 36 Password Instalasi File Winzip.exe

13. Setelah proses installasi ekstraksi file Winzip.exe, maka ditemukan semua bukti-bukti digital yang diperintahkan pada penugasan investigasi yaitu file dokumen harga sabu dan gambar sabu-sabu, seperti pada gambar 4. 37 dibawah ini:



Gambar 4. 37 Daftar dan Gambar Barang

Kesimpulan

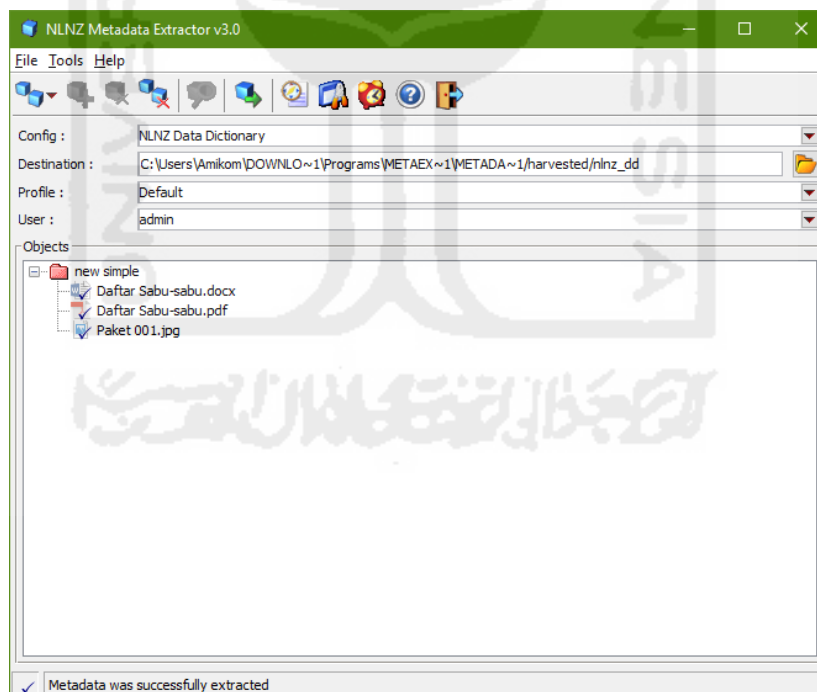
Setelah melakukan proses yang panjang, akhirnya diambil sebuah kesimpulan bahwa: **DI TEMUKAN** keterlibatan “X” dalam peredaran dan penjualan narkoba ke beberapa tempat dan jumlah daftar harga sabu beserta foto sabu-sabu di dalam *Thumbdrive* Toshiba yang di akuisisi dan di analisa oleh Tim Investigator.

Melihat Metadata Temuan Bukti-bukti Analisa File “Rahasia Kelompok 7.E01”

Untuk penguatan barang bukti dari hasil analisa file “Rahasia Kelompok 7.E01” diatas, cara lain yang bisa dilakukan adalah pendekatan metadata terhadap temuan bukti-bukti dari analisa file “Rahasia Kelompok 7.E01” dengan tools standar metadata extractor dan metadata forensik yang telah dibangun dari hasil penelitian ini. Adapun temuan bukti-bukti tersebut yang akan di analisa metadatanya adalah sebagai berikut:

1. Melihat Metadata dengan tools Metadata Extractor

Langkah pertama membuka Metadata Extractor – browse file yang akan dilihat metadatanya (bisa langsung banyak file), berikut metadata extractor ketika dijalankan:



Gambar 4. 38 Metadata Extractor Ketika Berjalan

Hasil yang didapat dalam bentuk XML dan di buka dengan menggunakan Internet Explorer. Berikut gambar *screenshot* pada masing-masing temuan bukti file dibawah ini:

a. Temuan Bukti File Dokumen “Daftar Sabu-sabu.docx” berikut tampilan metadatanya:

```
- <MasterCreationDate locale="SGT">
  <Date format="yyyyMMdd">20170330</Date>
  <Time format="HHmmssSSS">011143784</Time>
</MasterCreationDate>
<ObjectComposition>simple</ObjectComposition>
- <StructuralType>
  <Name/>
  <Extension/>
</StructuralType>
<HardwareEnvironment>amd64</HardwareEnvironment>
<SoftwareEnvironment>OS: Windows 8.1 6.3, JVM:Oracle Corporation 1.8.0_20</SoftwareEnvironment>
<InstallationRequirements/>
<AccessInhibitors/>
<AccessFacilitators/>
<Quirks/>
<MetadataRecordCreator>admin</MetadataRecordCreator>
- <MetadataCreationDate locale="SGT">
  <Date format="yyyyMMdd">20170330</Date>
  <Time format="HHmmssSSS">011143785</Time>
</MetadataCreationDate>
<Comments/>
- <Files>
  - <File xmlns:nz_govt_natlib_xsl_XSLTFunctions="nz.govt.natlib.xsl.XSLTFunctions">
    <FileIdentifier/>
    <Path>D:\ProsesImaging\Daftar Sabu-sabu.docx</Path>
    - <Filename>
      <Name>Daftar Sabu-sabu.docx</Name>
      <Extension>docx</Extension>
    </Filename>
    <Size>169756</Size>
    <FileDateTime>
      <Date format="yyyyMMdd">20140417</Date>
      <Time format="HHmmssSSS">131110628</Time>
    </FileDateTime>
    <MimeType>application/open-office-1.x</MimeType>
    - <FileFormat>
      <Format>Open Office, </Format>
      <Version/>
    </FileFormat>
    - <Text>
      <CharacterSet>ISO-8859-1</CharacterSet>
      <MarkupLanguage/>
    </Text>
  </File>
</Files>
```

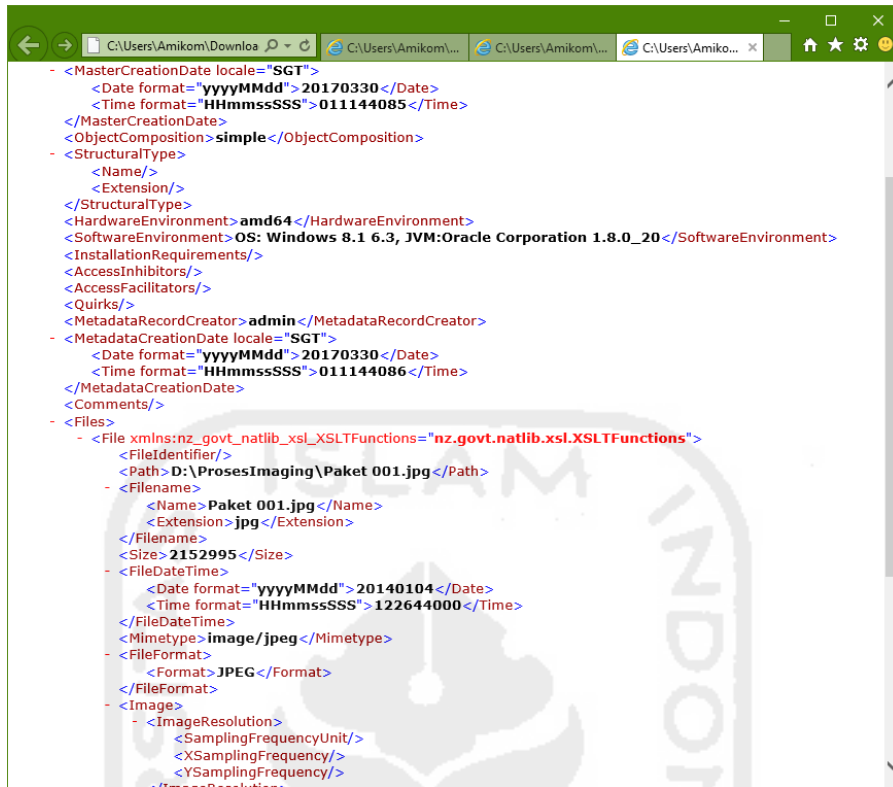
Gambar 4. 39 Hasil Metadata Extractor Daftar Sabu-sabu.docx

b. Temuan Bukti File Dokumen “Daftar Sabu-sabu.pdf” berikut tampilan metadatanya:

```
- <MasterCreationDate locale="SGT">
  <Date format="yyyyMMdd">20170330</Date>
  <Time format="HHmmssSSS">011143967</Time>
</MasterCreationDate>
<ObjectComposition>simple</ObjectComposition>
- <StructuralType>
  <Name/>
  <Extension/>
</StructuralType>
<HardwareEnvironment>amd64</HardwareEnvironment>
<SoftwareEnvironment>OS: Windows 8.1 6.3, JVM:Oracle Corporation 1.8.0_20</SoftwareEnvironment>
<InstallationRequirements/>
<AccessInhibitors/>
<AccessFacilitators/>
<Quirks/>
<MetadataRecordCreator>admin</MetadataRecordCreator>
- <MetadataCreationDate locale="SGT">
  <Date format="yyyyMMdd">20170330</Date>
  <Time format="HHmmssSSS">011143968</Time>
</MetadataCreationDate>
<Comments/>
- <Files>
  - <File xmlns:nz_govt_natlib_xsl_XSLTFunctions="nz.govt.natlib.xsl.XSLTFunctions">
    <FileIdentifier/>
    <Path>D:\ProsesImaging\Daftar Sabu-sabu.pdf</Path>
    - <Filename>
      <Name>Daftar Sabu-sabu.pdf</Name>
      <Extension>pdf</Extension>
    </Filename>
    <Size>292362</Size>
    <FileDateTime>
      <Date format="yyyyMMdd">20141022</Date>
      <Time format="HHmmssSSS">175215377</Time>
    </FileDateTime>
    <MimeType>application/pdf</MimeType>
    - <FileFormat>
      <Format>Adobe PDF</Format>
      <Version>1.5</Version>
    </FileFormat>
    - <Text>
      <CharacterSet>ISO-8859-1</CharacterSet>
      <MarkupLanguage>unknown</MarkupLanguage>
    </Text>
  </File>
</Files>
```

Gambar 4. 40 Hasil Metadata Extractor Daftar Sabu-sabu.pdf

c. Temuan Bukti File Gambar “Paket 001.jpg” berikut tampilan metadatanya:



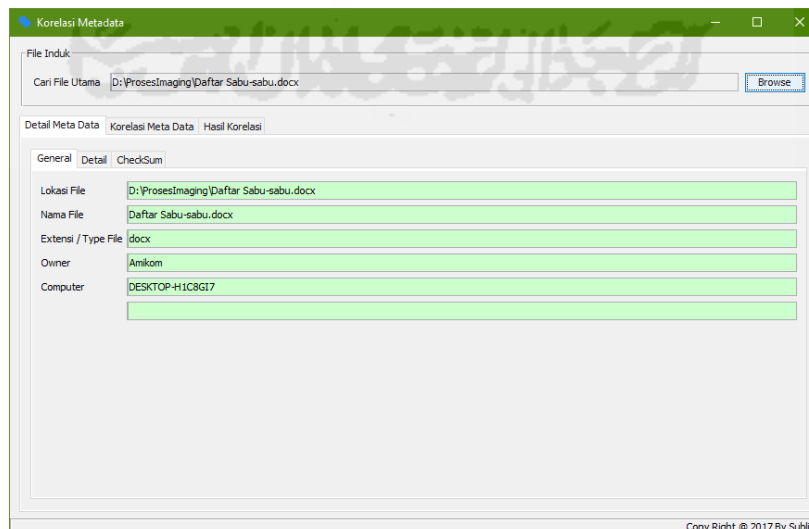
```
<MasterCreationDate locale="SGT">
  <Date format="yyyyMMdd">20170330</Date>
  <Time format="HHmmssSSS">011144085</Time>
</MasterCreationDate>
<ObjectComposition>simple</ObjectComposition>
<StructuralType>
  <Name/>
  <Extension/>
</StructuralType>
<HardwareEnvironment>amd64</HardwareEnvironment>
<SoftwareEnvironment>OS: Windows 8.1 6.3, JVM:Oracle Corporation 1.8.0_20</SoftwareEnvironment>
<InstallationRequirements/>
<AccessInhibitors/>
<AccessFacilitators/>
<Quirks/>
<MetadataRecordCreator>admin</MetadataRecordCreator>
<MetadataCreationDate locale="SGT">
  <Date format="yyyyMMdd">20170330</Date>
  <Time format="HHmmssSSS">011144086</Time>
</MetadataCreationDate>
<Comments/>
<Files>
  <File xmlns:nz_govt_natlib_xsl_XSLTFunctions="nz.govt.natlib.xsl.XSLTFunctions">
    <FileIdentifier/>
    <Path>D:\ProsesImaging\Paket 001.jpg</Path>
    <Filename>
      <Name>Paket 001.jpg</Name>
      <Extension>.jpg</Extension>
    </Filename>
    <Size>2152995</Size>
    <FileDateTime>
      <Date format="yyyyMMdd">20140104</Date>
      <Time format="HHmmssSSS">122644000</Time>
    </FileDateTime>
    <MimeType>image/jpeg</MimeType>
    <FileFormat>
      <Format>JPEG</Format>
    </FileFormat>
    <Image>
      <ImageResolution>
        <SamplingFrequencyUnit/>
        <XSamplingFrequency/>
        <YSamplingFrequency/>
      </ImageResolution>
    </Image>
  </File>
</Files>
```

Gambar 4. 41 Hasil Metadata Extractor Paket 001.jpg

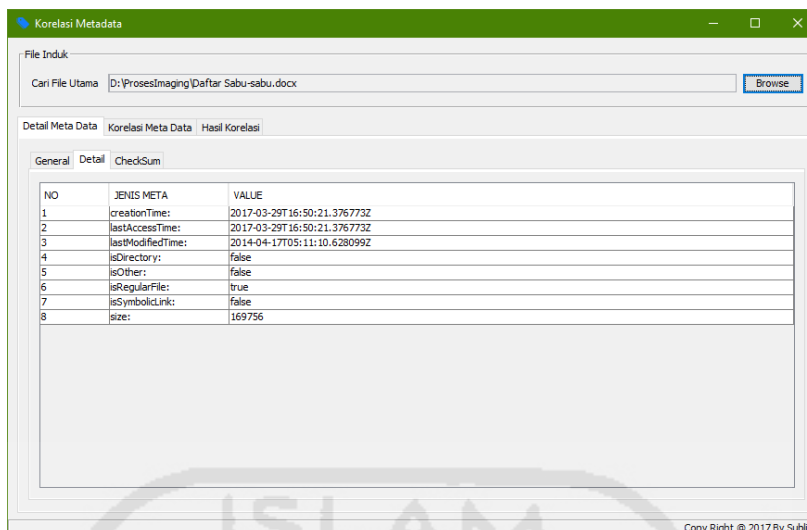
2. Melihat Metadata dengan tools Metadata Forensik

Langkah pertama yang dilakukan adalah membuka tools metadata forensik - *Browse* tempat penyimpanan file dokumen yang akan dilihat metadatanya - Proses beberapa saat nanti muncul Menu Detail Metadata - Hasil outputnya pada masing-masing file dibawah ini:

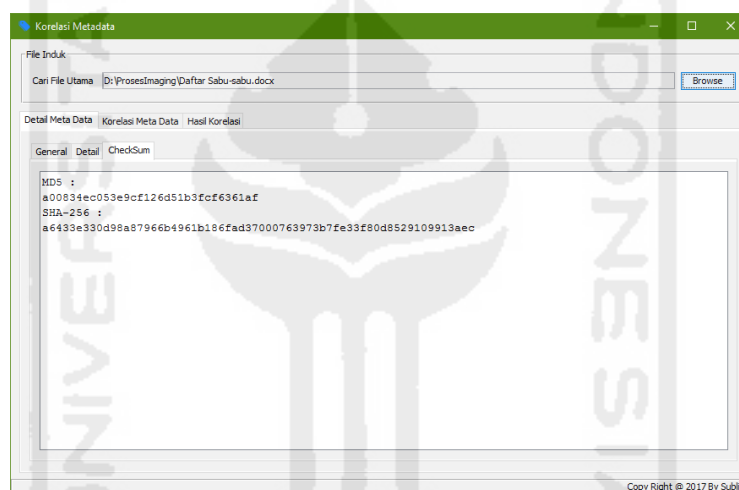
a. Temuan Bukti File Dokumen “Daftar Sabu-sabu.docx” berikut tampilan metadatanya:



Gambar 4. 42 Hasil Metadata Forensik General Daftar Sabu-sabu.docx

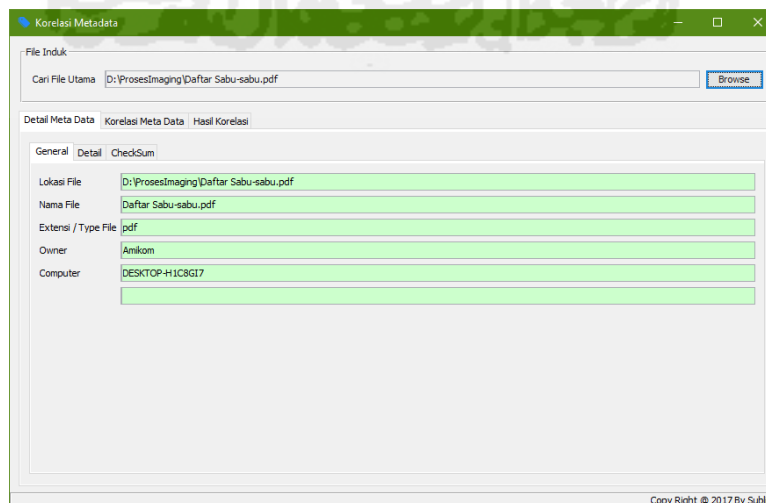


Gambar 4. 43 Hasil Metadata Forensik Detail Daftar Sabu-sabu.docx

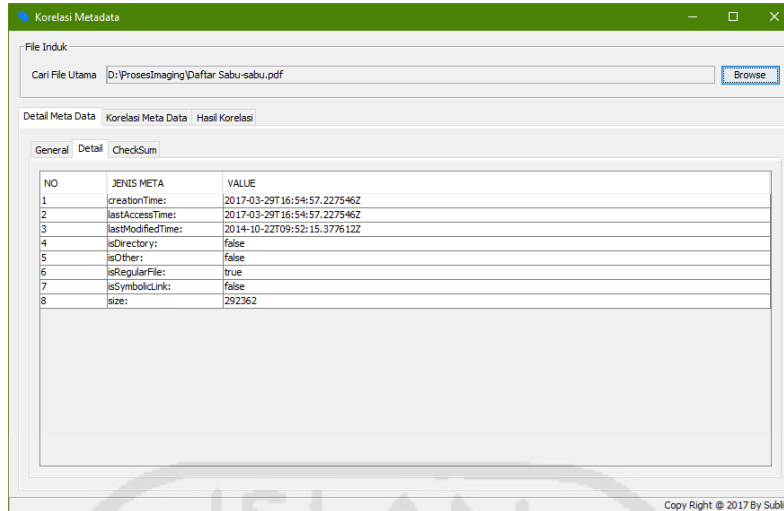


Gambar 4. 44 Hasil Metadata Forensik Checksum Daftar Sabu-sabu.docx

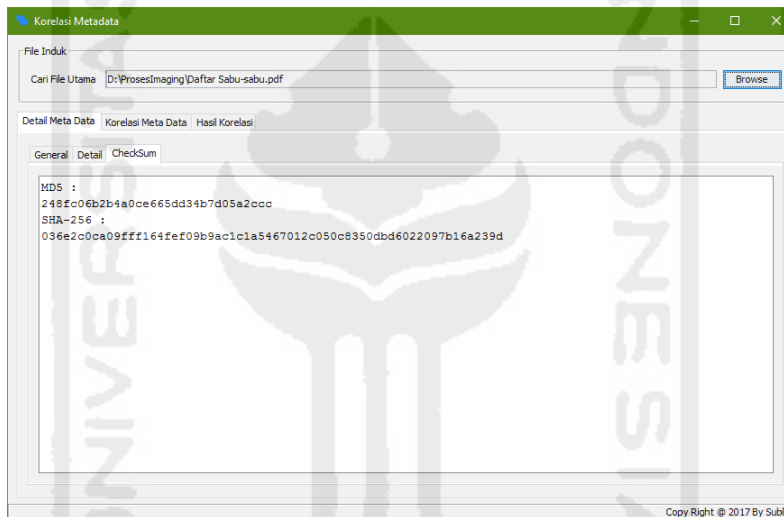
b. Temuan Bukti File Dokumen “**Daftar Sabu-sabu.pdf**” berikut tampilan metadatanya:



Gambar 4. 45 Hasil Metadata Forensik General Daftar Sabu-sabu.pdf

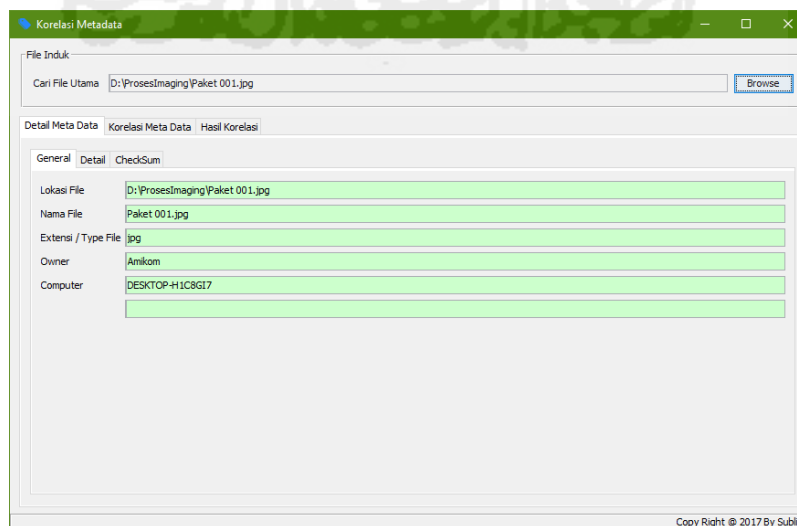


Gambar 4. 46 Hasil Metadata Forensik Detail Daftar Sabu-sabu.pdf

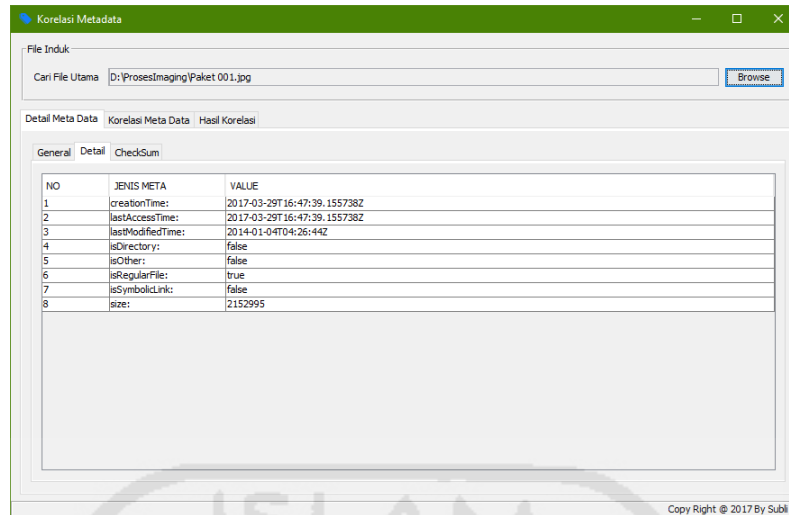


Gambar 4. 47 Hasil Metadata Forensik Checksum Daftar Sabu-sabu.pdf

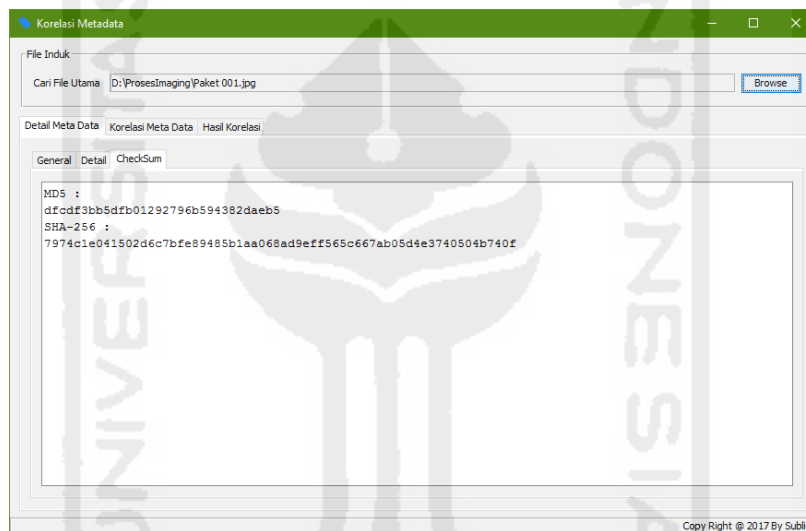
c. Temuan Bukti File Gambar “**Paket 001.jpg**” berikut tampilannya:



Gambar 4. 48 Hasil Metadata Forensik General Paket 001.jpg



Gambar 4. 49 Hasil Metadata Forensik Detail Paket 001.jpg



Gambar 4. 50 Hasil Metadata Forensik Checksum Paket 001.jpg

Perbandingan Penggunaan Kedua Tools Analisa Metadata File

Pada pembacaan metadata diatas oleh kedua tools Metadata eExtractor dan Metadata Forensik, dapat ditarik kesimpulan perbedaan pembacaan hasil metadatanya. Berikut dapat dilihat pada tabel 4. 33 perbandingan hasil pemeriksaan metadata file gambar Paket 001.jpg dari kedua tools tersebut:

Tabel 4. 33 Hasil Analisa Metadata Kedua Tools

Jenis Metadata	Metadata Extractor	Metadata Forensik
Folder Path	D:\ProsesImaging\Paket 001.jpg	D:\ProsesImaging\Paket 001.jpg
Name File	Paket 001.jpg	Paket 001.jpg
Type File	jpg	jpg

Lanjutan **Tabel 4. 33** Hasil Analisa Metadata Kedua Tools

Jenis Metadata	Metadata Extractor	Metadata Forensik
Owner	-	Amikom
Computer	-	DESKTOP-H1C8GI7
Creation Time	2017030, 011144086	2017-03-29T16:47:39.155738Z
Last Access Time	-	2017-03-29T16:47:39.155738Z
Last Modified Time	20140104, 122644000	2014-01-04T04:26:44Z
Is Directory	-	false
Is Other	-	false
Is Regular File	-	true
Is Symbolic Link	-	false
Size	2152995	2152995
Checksum MD5	-	dfcdf3bb5dfb01292796b594382 daeb5
Checksum SHA-256	-	7974c1e041502d6c7bfe89485b1 aa068ad9eff565c667ab05d4e374 0504b740f
System Type	amd64	-
Jenis OS	Windows 10	-
JVM	Oracle Corporation 1.8.0_20	-

Pada pendekatan metadata dengan kedua tools tersebut, bisa dipastikan file dokumen tersebut adalah file Paket 001.jpg dengan ukuran file 2152995 byte. Terdapat kelebihan dari masing-masing kedua tools tersebut, misalnya metadata extractor dapat membaca metadata system type, jenis OS dan JVM, sedangkan metadata forensik dapat membaca metadata nilai checksum MD5 dan SHA-256.