# Finding Digital Forensic Evidence in Graphic Design Applications

E.K. Mabuto and H.S Venter

Department of Computer Science, University of Pretoria, Pretoria, South Africa
e-mail: emabutos@cs.up.ac.za, hsventer@cs.up.ac.za

## Abstract

Graphic design applications are often used for the editing and design of digital art. The same applications can be used for creating counterfeit documents like identity documents (IDs), driver's licenses or passports among others. However the use of any graphic design application leaves behind traces of digital information which can be used during a digital forensic investigation. Current digital forensic tools examine a system to find digital evidence but they do not examine a system specifically for the creating of counterfeit documents. This paper reviews the digital forensics analysis process involved in the creation of counterfeit documents by determining and corroborating the events that previously occurred. The analysis is achieved by associating the digital forensic information gathered to the possible actions taken, precisely, the scanning, editing, saving and printing of counterfeit documents. The digital forensic information is gathered by analyzing the files generated by the particular graphic design application used for document creating. Another analysis is conducted on user generated files, the actual files that can be used as potential evidence to establish file structural contents and the relationship with the associated actions. This involves analyzing the user generated files associated with these applications and determining their signatures and related metadata. Contextually, the authors illustrate an evaluation disclosing the digital forensic evidence gathered from graphic design applications.

## Keywords

Digital evidence, Digital forensics, Digital forensic artifacts, Graphic design applications

## 1 Introduction

A great number of professions and industries such as advertising, newspaper printing, architecture, fashion and design, project management and manufacturing, depend upon being able to create complex graphic designs in the course of their work. It is for this reason that graphic design applications have numerous image-enhancing tools such as paint brushing, vector drawing, digital pen and pencil drawing and many others. Such graphic design applications use computer-aided design to create unique art for company logos, magazine advertisements and many other purposes. There are numerous individuals who rely upon being able to use graphic design applications to create visual presentations that utilize pictorial images to communicate and express ideas.

In another related development, the use of forged documents has become ubiquitous all over the world. Ilham Rawoot observes, in an article in the "Mail and Guardian" that terrorists make particular use of forged South African passports because of the ease with which these can be faked (Mail and Guardian Website, (2011)). But counterfeit documents are in circulation all over the world. The same graphic design applications that are used by professionals in their work can also be used for illegitimate purposes such as creating counterfeit documents. The problem is that, with the editing and design capabilities of these graphic design applications, they can be used to create extremely convincing counterfeit documents such as IDs, passports and drivers licenses. Criminal activities such as these necessitate the need for digital forensic investigations.

The use of graphic design applications leaves behind traces that can be revealed during a digital forensic investigation. A digital forensic investigation generally consists of the following phases: the acquisition, examination, analysis and reporting (U.S National Institute of Justice, 2001). Wherever an individual is suspected of creating counterfeit documents, the regular process of acquisition is followed. Generally the phases of acquisition and reporting are similar in different cases; therefore focus is on the examination and analysis phases. The focus is also on determining what the examiner needs to know prior to examining digital evidence. This paper identifies and discusses the digital traces that are left behind after a counterfeiter has used graphic design applications. This is achieved by associating the actions taken during document creation to the traces left behind. In addition, a file analysis of files generated by a user from within the application is conducted. To address the problem, the authors focus on the following two steps. First, identify the digital forensic information that shows whether a document was scanned, edited, saved and printed. Digital forensic information can be found in graphic design applications where the source of the evidence is mainly system-generated. The second step entails identifying the contents of user- generated files by looking at the file signatures and related metadata. In so doing, over above these two steps, an association with the potential criminal may be achieved. However, it is not the focus of this paper to link the crime to an actual person.

The remainder of the paper is structured as follows. In the second section, some background about digital forensics is presented, and this is followed by a brief survey of graphic design applications. The third section, which is the contributing section, is divided into two parts. The first part highlights the potential evidence that the authors refer to as "digital forensic artifacts". The source of potential evidence referred to above equates to the results from actions taken. More precisely the actions involved could be document scanning, editing, saving and printing. Most of this would originate from the system registry and application log files. The second part is an examination of user-generated files. The source of potential evidence referred to in this part involves results from content identification and content examination of files utilized by graphic design applications. The authors also name the tools that can be used in aiding the analysis where applicable. The fourth section contains an evaluation of the kind of evidence that may be extracted from the graphic design applications. The fifth section concludes the paper.

# 2 Background

In the following section the authors provide some brief background literature on digital forensics including an explanation of digital evidence. The authors also define what is meant by digital forensic artifacts. The second section of the background consists of a very brief literature survey on graphic design applications.

## 2.1 Digital Forensics

At the Digital Forensics Research Workshop (DFRWS) in 2001, digital forensics was defined as the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

The goal of a digital forensic investigation on a system is to find out what happened and who was responsible for a particular incident or crime. Digital forensic investigations focus on finding digital evidence after a computer or network security incident has occurred or locating data from systems that may form part of some litigation, even if it has been deleted. In this context, evidence is the most critical in any case. Therefore any items that can be considered to be of evidential value should be identified and collected (Jones and Valli, 2008).

### 2.1.1 Digital Evidence

Computer evidence or digital evidence is defined as any hardware, software or any data that can be used to prove one or more of the “who, what, when, where, why and how” questions of a security incident (Solomon et al., 2005). Computer evidence furthermore consists of digital files and their contents left behind after an incident. Casey defined digital evidence as any data that can be used to establish that a crime was committed or can prove a link between a crime and its victim or an offender (Casey, 2000). Digital evidence consists entirely of sequences of binary values called bits (Cohan, 2010). Traces that are left behind from the use of an application or from an operating system can be referred to as digital forensic artifacts.

### 2.1.2 Digital Forensic Artifacts

An examiner reveals the truth of an event by discovering and exposing the remnants of the event that have been left on the system. These remnants are known as artifacts, which can be referred to as digital evidence (Altheide and Carvey, 2011)However, due to the loaded legal connotations binding the term “evidence” the term “artifacts” is used more often. Evidence is referred to as something to be used during a legal proceeding. Artifacts are traces left behind due to activities and events, which may or may not be innocuous. The scattered evidence inside a system can indicate what has happened for a particular digital forensic investigation. Application artifacts left by installed applications can be an excellent source of potential evidence when performing an analysis. Also an artifact does not become evidence unless its ability to prove a fact has been established (Zelkowitz , 2009). Therefore it is necessary to reconstruct events that occurred by gathering all the possible digital information from a system.

In an investigation, how and where evidence is located differs depending on the crime being investigated, the platform (operating systems) and the application used to commit the crime.

### 2.2 Graphic design applications

Although many graphic design applications are currently available to users, Adobe Systems Incorporated is regarded as the largest software maker in the graphic design software category (Wall-street Journal Website, 2011). For the purposes of this research, the authors therefore undertook a case study by investigating Adobe graphic design applications. Adobe Photoshop, Adobe In-Design and Adobe Illustrator are Adobe applications that are used for graphic design purposes. Any one of these applications can be used for the editing of a document. It is therefore necessary to conduct an exclusive examination of the potential digital forensic evidence produced by these applications. Since most graphic design users prefer to use the latest editions, the authors used the latest version of Adobe (Version, CS5) in the experiments. It should be noted, however, that additional experiments with the two previous versions (CS4 and CS3) produced similar results. Any slight differences that are attributed to different versions will be mentioned wherever necessary throughout the paper.

## 3 Digital forensic evidence in graphic design applications

The authors created dummy counterfeit documents by using Adobe graphic design applications, and carried out various experiments in order to search for pertinent evidence left behind from the use of these graphic design applications. The contribution is divided in two parts. The first part highlights digital forensic artifacts found in graphic design applications where the source of the potential evidence is mainly system-generated with results mostly from registry entries and application log files. The second part of the experiments, which involves examination of user-generated files, highlights results from file content identification and examination.

Software reviews from 2011 revealed that the Windows operating system is still the most popular operating system (Gartner Research, 2011). The authors therefore conducted the analysis for forensic artifacts on a Windows 7 platform. For future work, focus can also be placed on other popular operating systems like Linux and Mac OS.

To respond to the problem stated earlier, that graphic design applications can be used for creating counterfeit documents, firstly four possible actions taken during the creation of a document were used as a hypothesis to gather digital forensic information related to graphic design applications. These actions are document scanning, document editing, document saving and document printing. The analysis is formulated to find the digital forensic information that indicates that these actions were actually taken. By following the actions taken an investigator is able to conduct an investigation in a uniform manner that helps to acquire the actual images like a human face used to create the document and the created counterfeit document. For example, if the document was scanned, then probably it was then edited. If not scanned then probably it was edited by acquiring a copy of the original from another source. If not edited then probably it was printed only after being edited from another source. If none of the four actions were taken then there is no need to ascertain whether or not the application was used in the creation of the document.

Furthermore to respond to the same problem, a user-generated file analysis section follows, with two sub-sections dealing with content identification and content examination.

Experimental results gleaned from finding the four actions are elaborated in the each of the subsections to follow.

### 3.1 System-generated digital forensic artifacts

"System-generated digital forensic artifacts" refer to those artifacts created by the application without user intervention, while "user-generated digital forensic artifacts refer" to artifacts created by the user intentionally. The latter are discussed later in the paper.

For the experiments conducted, the following section describes the techniques used on Adobe graphic design applications. Four sub-sections follow in this section, namely artifacts related to document scanning, editing, saving and printing. It should be noted, however, that not all applications have the same capabilities to perform all these actions. Therefore, not all actions are described for each graphic design application. However, initiation of one of the actions can lead to possible identification of potential evidence relating to the creation of counterfeit documents. The authors explain the artifacts gathered from each action precisely for each graphic design application. Adobe Illustrator does not record any information regarding the four actions in any of its log files. Therefore, for Adobe Illustrator essential information will be acquired from the exclusive examination of user-generated files still to follow in section 3.2.

#### 3.1.1 Artifacts relating to document scanning

Generally, if one is to attempt to create a fraudulent document, one has to acquire an original document so as to imitate or copy it. Scanning is an option which results in a copy of the original document being available on pc for digital editing. Many different models of scanners are available, using various software packages for executing scan commands. Therefore, for this research, focus is on commands generated from within the graphic design application used for editing the scanned document, rather than determining if a document is a scanned document.

Out of the three graphic design applications under consideration, only Adobe Photoshop has the capability of scanning a document using the "import WIA support" document menu option. "Import WIA support" is a function that Adobe Photoshop uses to connect to available printers or scanners. The document scanned is loaded into a destination folder as prompted. The application then creates a folder, saves the scanned image, and opens the scanned image in the application.

After a document is scanned the application records the entry into one of its log files under the name of *Adobe Photoshop CSX Prefs.psp* located in *C:\Users\<username>\ AppData\ Roaming \Adobe\Adobe Photoshop CSX\Adobe Photoshop CSX Settings*. The *X* in *CSX* represents the particular Adobe version in use. This may be either version 3, 4, or 5. After analyzing the log file's binary data an entry with the location of the scanned file is located usually about mid section of the file size. For example, if the file is 165kb the scanned file information will be located at hex byte offset 0x17004. After analyzing the content at this hex location, the folder locations of all the scanned documents can be found there.

The regular process followed by a potential criminal is to edit the acquired document in order to falsify some of its content.

### 3.1.2 Artifacts relating to document editing

Document editing is one of the critical stages of creating a counterfeit document as it allows one to place or import objects of interest, for example a human face, a bar code or a fingerprint. These objects can be inserted onto the scanned document. In relation to the inserted documents or files, experiments were executed to establish what can be found from a system that indicates to the examiner what was inserted and from which location it was inserted from. All three graphic design applications in question have the capacity to edit a document through attaching or placing an image. The terms "attaching" or "placing" an image is seen as the same action, used interchangely in various applications. In this paper, the term "attaching" is used from here on. Attaching is one of the main functions that is used in graphic design applications.

#### 3.1.2.1 Editing in Adobe Photoshop

The same log file mentioned earlier *(Adobe Photoshop CSX Prefs)* contains information with the name of the attached file and the location from which it was attached usually at a byte offset of about 0x17F40. With this information the authors managed to establish the names and location of attached documents. Furthermore, by looking at the stated location the actual image with the human face or fingerprint was found.

#### 3.1.2.2 Editing in Adobe Indesign

A file named *InDesign SavedData* without a file extension is located in the located in the folder *C:\Users\ <username>\ AppData\Local\Adobe\InDesign\Version 5.0\Cache*. It contains information indicating the name of the attached file and the location from which it was attached usually in the beginning of the file.

### 3.1.3 Artifacts relating to document saving

Once a document has been edited, usually a user (or potential criminal) might need to save it, either for printing or further editing. In this section the authors look at what is found in the system that relates to saved documents. This information is vital as it can point to an examiner where a file was saved to. If deleted or moved, search commands can be executed based on the names of the files saved. This is done by specifying the name of the file when searching thereby reducing time spent during an investigation. All three applications under consideration have the capability to save edited documents in various file types. An exclusive examination on each of the file types created from saving actions is explained in section 3.2.

#### 3.1.3.1 Saving in Adobe Photoshop

The same log file *(Adobe Photoshop CSX Prefs)* contains information about save entries. The file contains information about the name of the saved file, the location in which it was filed, and type of the file, located at mid offset of the file after the entries for attached files. The names are arranged in order of the last saved file first. This information about saved locations can be verified or compared to the registry entries. Values for the visited directories are acquired from the registry key, *HKEY_CURREN T_USER\Software\Adobe\Photoshop\ 11.0\VisitedDirs.*

#### 3.1.3.2 Saving in Adobe Indesign

The same log file *(InDesign SavedData)* that was earlier mentioned in connection with editing actions, contains information about the name of the file saved, type of the file and the location saved to. This information is located from mid offset of the file with the last saved file first. This information is located up to the end of the file depending on the number of documents saved.

Generally, saved files from any graphic design application can be verified or checked also by looking at the recent documents accessed from *C:\Users\<username>\ AppData\Roaming\Microsoft\Windows\Recent.*

### 3.1.4 Artifacts relating to document printing

Printing is one if not the last stages of potential counterfeit document creation. A user might need to create the hard copy of the edited document so that it can be used in a physical environment. Unlike scanning actions, printing actions can be commanded from all the graphic design applications under consideration via the menu command: print.

To locate which printer(s) are used to generally print a document one uses the registry. The keys from which a list of printers connections could be established from are

(1)*HKLM\soft\Adobe\Photoshop\11.0\Plugin* path.
*(2)HKEY_CURRENT_CONFIG\System\CurrentControlSet\Control\Print\Printers*
*(3)HKEY_USERS\<user id>\Software\Microsoft\Windows NT\CurrentVersion\PrinterPorts*
(4)HKEY_USERS\<userid>\Software\Microsoft\Installer\Products\
41E0A130314079C4792762937B284FF6\ SourceList

After the names of the printers have been established, an investigator can verify the physical existence of the printer. This helps an investigator usually in cases where the printers have been physically removed. Moreover, given that the option to keep printed documents was enabled in the printers' properties before printing a counterfeit document. For each print job there are two spool files generated by the operating system located in *C:\Windows\System32\spool\ PRINTERS.* The first is *XXX.shd* and *XXX.spl* where *XXX* represents the job number. Analyzing the binary data of these files indicates the name of the printed document in the beginning of the **.spl* file. Towards the end of the **.shd* file is the name of the printed file, the location from which it was printed from and the name of the printer used to print the document. The timestamp of the **.spl* and **.shd* file indicates the date and time the document was created. This information is vital in establishing which counterfeit documents were actually printed.

Once the names and locations of the files have been established, an investigator needs to examine the actual identified files. These are the files that can be used as potential evidence in legal proceedings. This process is described in the following section.

### *3.2* User-generated artifacts from file examination

In order to conduct an exclusive examination on a crime conducted within an application the digital forensic examiner has to understand the nature of the files that are generated from that particular application, in this case, graphic design applications. This is so that the examiners are able to uncover and exploit any digital forensic artifacts present in the identified files (Altheide and Carvey, 2011).

As previously stated, user-generated digital forensic artifacts refers to files created by the user intentionally. User generated file artifacts can be divided into two distinct categories, which are, content identification and content examination. Content identification is the process of determining or verifying the type of a specific file. Content examination is the retrieval of any embedded metadata that may be present in a given file.

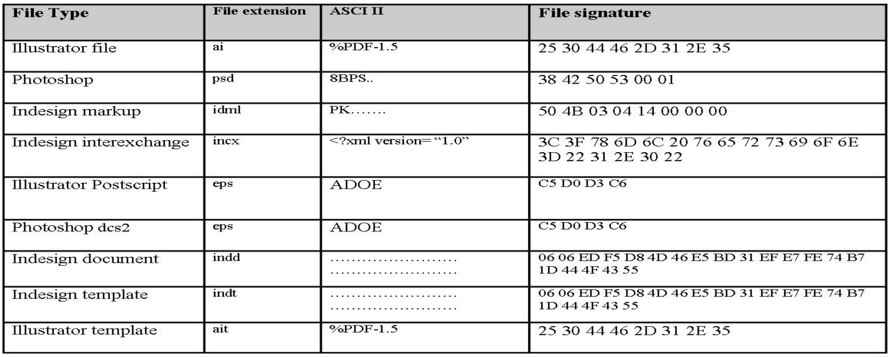
In the case of the examination of counterfeit documents the digital forensic examiner might need to identify potential changes inside files consistently, for example, the involvement of a fingerprints, barcodes or human faces embedded inside graphic design application file formats. The four graphic design applications discussed above are associated with more than thirty nine file types. However, for this research the authors focus was only on file types that are specific to the three graphic design applications, thus ignoring well-known file types like jpeg, bitmap, tag, tiff, tga etc. Gary Kesler and Martin Reddy keep a list of these common file signatures online, which is a continuing work in progress database (Kesler and Reddy, 2011)).

### 3.2.1 Content identification

As already been stated, content identification involves verifying the identity of a file extension. An offender can alter the file extension of a particular file in order to promote ambiguity. Therefore there is need to identify a files integrity by file signature analysis. An examiner needs to know what a particular file type is. A file is normally analyzed within its first bytes to determine the specific signature (Carvey, 2009). The file signature is therefore located at specific offsets usually in the beginning of a file.

It can be noted from the research conducted that known digital forensic tools like FTK can detect various file types but not for graphic design applications discussed in this paper. For example, digital forensic tools can verify file types like tga, bmp, gif, tif and png amongst others, but not the file types of graphic design applications as discussed in this paper.

The analysis to determine a graphic design file signature was also conducted using a hex editor. These values are generally hexadecimal values. Table 1 contains the list of file signatures identified and specific to the graphic design applications previously discussed. The file type in Table 1 represents the named form of the particular graphic design file. Proof of the real file identity resides within the content of the file, usually known as the file signature. The file extension is merely a suffix that represents the encoding of a file’s content, usually three or four characters separated by a dot from the file name. However, the file extension should never be trusted as it can be renamed to anything else. One should rather focus on the file signature to determine the correct file type. The ASCII column in Table 1 represents the entry in text-readable format. The file signature columns represent the entry in hexadecimal format. Both these entries appear exactly as shown in the hex editor. The digital forensic examiner can use the information in Table 1 to identify the particular files for the graphic design applications in question.



| File Type | File extension | ASCI II | File signature |
|---|---|---|---|
| Illustrator file | ai | %PDF-1.5 | 25 30 44 46 2D 31 2E 35 |
| Photoshop | psd | 8BPS.. | 38 42 50 53 00 01 |
| Indesign markup | idml | PK……. | 50 4B 03 04 14 00 00 00 |
| Indesign interexchange | incx | <?xml version= “1.0” | 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 |
| Illustrator Postscript | eps | ADOE | C5 D0 D3 C6 |
| Photoshop dcs2 | eps | ADOE | C5 D0 D3 C6 |
| Indesign document | indd | ……………………<br>…………………… | 06 06 ED F5 D8 4D 46 E5 BD 31 EF E7 FE 74 B7 1D 44 4F 43 55 |
| Indesign template | indt | ……………………<br>…………………… | 06 06 ED F5 D8 4D 46 E5 BD 31 EF E7 FE 74 B7 1D 44 4F 43 55 |
| Illustrator template | ait | %PDF-1.5 | 25 30 44 46 2D 31 2E 35 |

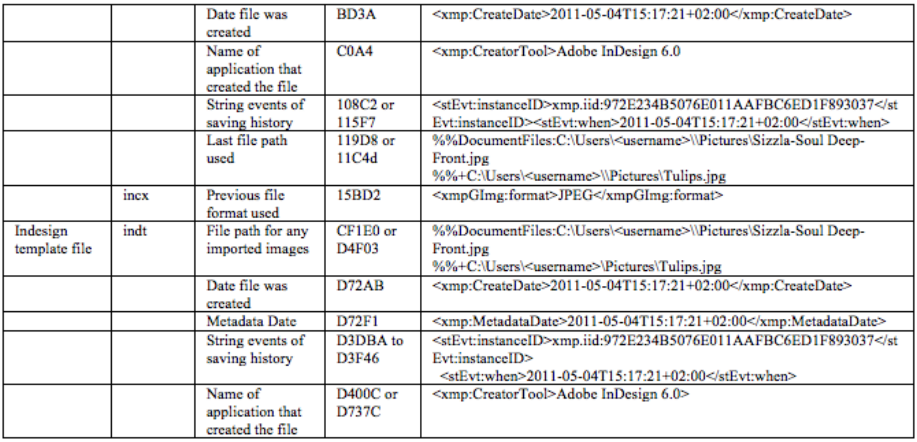
**Table 1: Graphic design file signatures**

### 3.2.2 Content Examination

Content examination involves determining the metadata of files, in this case, graphic design application file types. Metadata refers to data about data (C.Altheide, H.Carvey, 2011). On Windows systems this includes modified, accessed, creation times only to mention a few. The same hex editors, as previously stated, are used to examine the content of files associated with graphic design applications. Metadata is essential during an investigation as this reveals what useful information can be extracted from a particular file, for example this can be time stamps or name of the user who created the file.

Table 2 shows the metadata acquired from graphic design file types. The offset is the address pointer of the described metadata. In other words, if an examiner searched for a certain offset, the hex editor would skip to the particular metadata. Several experiments however revealed that the offset can vary slightly by plus or minus 780 bytes per metadata, which is usually in the same page view depending on the size of the file and quantity of metadata present in the file. Therefore the tabulated values can still be used on graphic design files of different sizes. The metadata is embedded in Extensible Metadata Platform (xmp) tags, which is Adobe's way of embedding metadata in its various file types (Adobe XMP, 2011).

| File type | File extension | Description of Metadata | Offset (Address pointer to Metadata) | Example of the Metadata (As presented in a hex editor) |
|---|---|---|---|---|
| Indesign document | indd | File location for any imported image files | D9EB | file:C:/Users/<username>\/Pictures/ dvd%20picture%20sleeves/Capture_005% 20%282%29.JPG |
| | | Name of application that created the file | E510B or E6E16 | <stEvt:softwareAgent>Adobe InDesign 6.0</stEvt:softwareAgent> |
| | | String events of saving history | F0D0C to F12FE | <stEvt:action>created</stEvt:action> <stEvt:when>2011-05-04T15:13:25+02:00</stEvt:when>stEvt:action>saved</stEvt:action><stEvt:when>2011-05-04T15:15:43+02:00</stEvt:when> |
| | | Date file was created | F5263 | CreateDate>2011-05-04T15:13:25+02:00 |
| | | Metadata Date | F52A7 | MetadataDate>2011-05-04T15:18:24+02:00</xmp:MetadataDate |
| | | Modify Date | FD2EA | <xmp:ModifyDate>2011-05-04T15:18:24+02:00</xmp:ModifyDate> |
| Illustrator Postscript file | eps | Name of application that created the file | 57 | %%Creator: Adobe Illustrator(R) 14.0 |
| | | Date file was created | 8E | %CreationDate: 9/17/2011 |
| | | Login name of user that created the file | 73 | %%For: <username>\<br>% |
| Illustrator file | ai | Metadata Date | 3A7 | <xmp:MetadataDate>2011-05-04T15:51:17+02:00</xmp:MetadataDate> |
| | | Date file was modified | 3ED | <xmp:ModifyDate>2011-05-04T15:51:17+02:00</xmp:ModifyDate> |
| | | Date file was created | 431 | <xmp:CreateDate>2011-05-04T15:51:17+02:00</xmp:CreateDate> |
| | | Name of application that created the file | 476 | <xmp:CreatorTool>Adobe Illustrator CSX</xmp:CreatorTool> |
| Photoshop file | psd | Name of application that created the file | 1A9 | <xmp:CreatorTool>Adobe Photoshop CSX Windows</xmp:CreatorTool> |
| | | Date file was created | 1F0 | <xmp:CreateDate>2011-05-04T14:39:08+02:00</xmp:CreateDate> |
| | | Date file was modified | 234 | <xmp:ModifyDate>2011-05-04T14:50:23+02:00</xmp:ModifyDate> |
| | | Metadata date | 27A | <xmp:MetadataDate>2011-05-04T14:50:23+02:00</xmp:MetadataDate> |
| | | String events of saving history | 6FF to 717 | <stEvt:instanceID>xmp.iid:DE0657134D76E011B00EFDC555D228CB</stEvt:instanceID> <stEvt:when>2011-05-04T14:50:23+02:00</stEvt:when> |
| Illustrator template | ait | Name of application that created the file | 1F3 or 452 | <xmp:CreatorTool>Adobe Illustrator CSX</xmp:CreatorTool> |
| | | Metadata Date | 383 | <xmp:MetadataDate>2011-05-04T15:51:17+02:00</xmp:MetadataDate> |
| | | Date file was modified | 3C9 or 16323 | <xmp:ModifyDate>2011-05-04T15:51:17+02:00</xmp:ModifyDate> |
| | | Date file was created | 40D | <xmp:CreateDate>2011-05-04T15:51:17+02:00</xmp:CreateDate> |
| | | String events of saving history | D02B or D5D3 | <stEvt:action>saved</stEvt:action><br><stEvt:instanceID>xmp.iid:FF7F117407206811B628E3BF27C8C41B</stEvt:instanceID> <stEvt:when>2011-05-22T16:23:53-07:00</stEvt:when> |
| | | Name of user that created the file | 17FB9 | %%For: (Pinchers) () |
| | | File path for any imported images | D727 | %%DocumentFiles:C:\Users\<username>\Pictures\Sizzla-Soul Deep-Front.jpg<br>%%+C:\Users\<username>\\Pictures\Tulips.jpg |
| | | List of previous files names used | 180A8 | /Title(illustrator .ait template) |
| Indesign interexchange file | incx | Date file was created | BFD3 | <xmp:CreatorTool>Adobe InDesign 6.0</xmp:CreatorTool> |
| | | Metadata Date | C019 | <xmp:MetadataDate>2011-05-04T15:17:21+02:00</xmp:MetadataDate> |
| | | Date file was modified | C05F | <xmp:ModifyDate>2011-05-04T15:17:21+02:00</xmp:ModifyDate> |



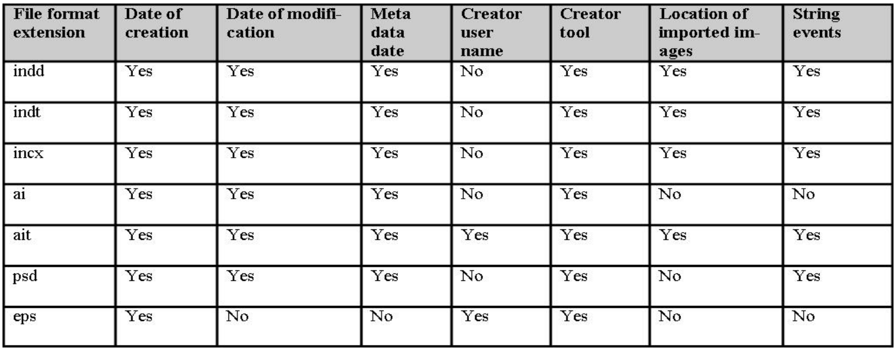
| | | | | |
|---|---|---|---|---|
| | | Date file was created | BD3A | <xmp:CreateDate>2011-05-04T15:17:21+02:00</xmp:CreateDate> |
| | | Name of application that created the file | C0A4 | <xmp:CreatorTool>Adobe InDesign 6.0 |
| | | String events of saving history | 108C2 or 115F7 | <stEvt:instanceID>xmp.iid:972E234B5076E011AAFBC6ED1F893037</stEvt:instanceID><stEvt:when>2011-05-04T15:17:21+02:00</stEvt:when> |
| | | Last file path used | 119D8 or 11C4d | %%DocumentFiles:C:\Users\<username>\\Pictures\Sizzla-Soul Deep-Front.jpg<br>%%+C:\Users\<username>\\Pictures\Tulips.jpg |
| | incx | Previous file format used | 15BD2 | <xmpGImg:format>JPEG</xmpGImg:format> |
| Indesign template file | indt | File path for any imported images | CF1E0 or D4F03 | %%DocumentFiles:C:\Users\<username>\\Pictures\Sizzla-Soul Deep-Front.jpg<br>%%+C:\Users\<username>\Pictures\Tulips.jpg |
| | | Date file was created | D72AB | <xmp:CreateDate>2011-05-04T15:17:21+02:00</xmp:CreateDate> |
| | | Metadata Date | D72F1 | <xmp:MetadataDate>2011-05-04T15:17:21+02:00</xmp:MetadataDate> |
| | | String events of saving history | D3DBA to D3F46 | <stEvt:instanceID>xmp.iid:972E234B5076E011AAFBC6ED1F893037</stEvt:instanceID><br><stEvt:when>2011-05-04T15:17:21+02:00</stEvt:when> |
| | | Name of application that created the file | D400C or D737C | <xmp:CreatorTool>Adobe InDesign 6.0> |

**Table 2: Graphic design file types related metadata**

# 4 Discussion

From the case study the authors managed to establish the location from which scanned documents were saved to. In this location several other documents were also recognized to indicate the names and original identities of documents. For the action of editing the authors established the names file types and file locations of attached documents. These were fingerprint and human face images inserted onto a copy of the original documents. Following editing, saving actions produced artifacts revealing the names of the saved files, their file types and their locations. These saving actions enabled recognition of potential evidence as they contained the actual counterfeit documents. For the printing action results from registry and log files indicated the names of the printers used and the names of the printed documents.

For user-generated file analysis all graphic design application file types analysed have timestamps as part of their metadata. However only a few of them have the user name of the creator of thefile as part of the metadata. Table 3 summarises the user-gernerated file types. "Yes" in this table indicates that the described metadata is present while "No" denotes that the file type does not contain the described metadata. The headings of the columns are brief names of descriptions of the metadata that was previously tabulated in Table 2.



| File format extension | Date of creation | Date of modification | Meta data date | Creator user name | Creator tool | Location of imported images | String events |
|---|---|---|---|---|---|---|---|
| indd | Yes | Yes | Yes | No | Yes | Yes | Yes |
| indt | Yes | Yes | Yes | No | Yes | Yes | Yes |
| incx | Yes | Yes | Yes | No | Yes | Yes | Yes |
| ai | Yes | Yes | Yes | No | Yes | No | No |
| ait | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| psd | Yes | Yes | Yes | No | Yes | No | Yes |
| eps | Yes | No | No | Yes | Yes | No | No |

**Table 3: Summary of User generated file analysis**

Given that a digital forensic investigation was initiated on a suspected counterfeit document creation crime, and the document was generated using a graphic design application. And using the identified digital forensic artifacts a digital forensic examiner is able to establish the route at which the document was created and to corroborate the gathered evidence. For example the digital forensic examiner is able to discover the human face, fingerprint, and or bar code images used to create the document. Together with the actual counterfeit document these can be presented in the court for prosecution. By presenting proof of the actions taken during document editing the process followed can provide valuable support in the court.

For content identification, the digital forensic examiner can use the recognized file signatures and the corresponding ASCII text representation to determine the file type of the graphic design applications in question. The file signatures can also be used when searching files from a formatted hard drive. Also an in-depth analysis of user-generated files can assist an examiner in knowing which particular metadata to acquire from graphic design file types and at what offset address.

Recalling that computer evidence is defined as any hardware, software or any data that can be used to prove one or more of the “who, what, when, where, why and how” of a security incident. By reviewing all the artifacts gathered the definition of digital evidence can be confirmed. This is so because all the six questions, “who, what, when, where, why and how” of the digital evidence definition are validated from the results acquired. Briefly clarifying the results: the “who” was specified by an artifact with the user name, the “what”, specified by identifying the particular files types from the application, the “when”, specified with a registry artifact indicating time of incident, the “where” specified with an artifact showing the file location, the “why” specified with a file metadata extraction revealing the file contents and the “how” with an artifact indicating which application was used for document editing. These results are essential for a digital forensic examiner to know where to look for digital forensic information, guided by knowing what information to find at a named particular location. This speeds up the process of an investigation where graphic design applications were used.

# 5 Conclusion

The approach outlined in this paper is particularly useful for solving those cases in which document editing is largely associated with a particular application. The approach only addresses case studies involving Adobe products but the same can be done for other graphic design applications. However, the approach doesn't tackle issues where the user only edits a hard copy, scans and prints without using any pre-installed application. Recalling the problem that graphic design applications can be used to create counterfeit documents, and that current digital forensic tools examine a system to find digital evidence but they do not examine a system specifically for the creating of counterfeit documents .The techniques discussed can be incorporated in bigger digital forensic tools like FTK and Encase or possibly the design of a crime specific tool similar to a Porn detection stick, ( Parabens software Website, 2011) which is a thumb drive device that will scan and detect pornographic content on a computer. Also, future work can be conducted by carrying out this exercise on other graphic design applications like CorelDraw.

# 6 References

Adobe XMP Website, (2011) http://www.adobe.com/ products/ xmp/index.html (Accessed 11 November 2011)

Altheide, C., Carvey, H. (2011), "Digital Forensics with Open Source tools". Elsevier. MA USA, pp 2.

Carvey, H. (2009), "Windows Forensic Analysis Dvd Toolkit", 2nd Ed, Elsevier, pp 296.

Casey, E. (2000), "Digital evidence and computer crime", London, Academic Press, pp10.

Cohan, E. (2010), "Towards a science of digital forensic investigation", IFIP Advances Digital Forensics VI, China, pp 17-35

Digital Forensic Research Workshop (2001), "A roadmap for Digital Forensic Research", pp 16.

Gartner Research (2011), "Which operating system will be 2011's bestseller", http://www.gartner.com/technology/research.jsp (Accessed 11 August 2011)

Jones, A., Valli, C. (2008), "Building a digital forensic laboratory", Burlington, Elsevier, pp 285.

Kesler, G. (2011), File signatures, http://www.garykessler.net/library/file_sigs.html, (Accessed 10 October 2011).

Mail and Guardian Website (2011), "Terrorists favour 'easy' fake SA passports", Mail and Guardian online, http://mg.co.za/article/2011-06-17-terrorists-favour-easy-fake-sa-passports (Accessed 17 June 2011)

Parabens software Website (2011), www.paraben-sticks.com/porn-detection-stick (Accessed 9 August 2011)

Reddy, M. (2011) Graphic design file format database, http://www.martinreddy.net/gfx/2d-hi.html (Accessed 10 October 2011)

Solomon, M.G., Barett, D., Broom, N. (2005). "Computer Forensics Jumpstart", Sybex, London, pp 51.

U.S National Institute of Justice (2001) "Electronic Crime Scene Investigation Guide: A guide for First Responders", *NIJ Special report, 2nd Ed,* pp 10-47.

Wall Street Journal (2011), Dow Jones, "Adobe 2Q Net Up 54% On Broad Sales Gains..," http://www.wsj.com, (Accessed 21 June 2011)

Zelkowitz, M.V. (2009), "Advances in computers; information security".Academic Press-Elsevier