Finding digital forensic evidence in document counterfeiting

Enos Mabuto and Prof Hein Venter

Counterfeit documents created in graphic design programs often enable serious crimes, such as terrorism, fraud, money laundering and theft. Therefore, it is very important that law enforcement entities are able to identify counterfeit documents by acquiring an accurate understanding of how these documents are created. A study in the Department of Computer Science investigated ways in which these documents can be traced in order to be used as evidence.

Many graphic design applications can be used to create counterfeit documents, such as identity documents (IDs), driver's licences and passports. Adobe Systems Incorporated is regarded as the largest software manufacturer of graphic design software (Kell, 2011). The Adobe suite consists of applications such as Adobe Photoshop, Adobe InDesign and Adobe Illustrator. Adobe Photoshop is a professional industry standard application for digital image editing and creation. Adobe InDesign is a professional layout and design application that delivers production workflows, complex graphics and typography. Adobe Illustrator is an application used for vector artwork in planning projects.

These three graphic design applications were used to create approximately 300 dummy counterfeit documents. These documents were created by editing the following four personal identifying insertions: barcodes, fingerprints, signatures and photographs of human faces.

Because the counterfeit documents are generated electronically, digital evidence can be collected to trace the source of fraud. Digital evidence is defined as any hardware, software or data that can be used to prove the occurrence of a breach of security (Barret et al., 2005).

Computer evidence further consists of digital files and their contents left behind after an incident. Traces that are left behind from the use of an application or from an operating system can be referred to as digital forensic artefacts. There are three methods of gathering digital evidence: system-generated, user-generated and timeline-associated digital evidence.

System-generated digital evidence

System-generated digital forensic evidence refers to evidence that is automatically produced by the application without any specific user intervention. These digital forensic artefacts show that a document has been scanned, edited, saved and printed.

Generally, when one attempts to create a fraudulent document, it is necessary to first acquire an original document so that one can use it to create a new and fraudulent identity. When a criminal does this, the first action is to scan the original document to make it available for digital editing on a computer.

The study focused on the digital artefacts that are created from executing the scan commands in the graphic design application. These scan commands need to be executed in the same graphic design application that subsequently edited the scanned document.

In the course of the study, 20 documents for each application were scanned. When a document has been scanned, the application automatically records the digital artefact (the forensic evidence that scanning has taken place) into one of its log files. After scanning has taken place, the criminal may inevitably follow it up by editing the acquired document in order to falsify some of its content.

Document editing is one of the most important stages in the creation of a counterfeit document, because it allows the criminal to insert objects of interest into the scanned document. These may include the image of a human face, a barcode or a fingerprint.

Editing actions include typing, colouring or drawing. The study focused on the kind of editing that results in the insertion of an image or object, because these can later be used by an investigator to determine whether the document that was created was counterfeit or not. During the analysis of the inserted objects, the researchers tried to establish what could be inferred from a computer system that would indicate to a digital forensic examiner what had been inserted and the location from which it was inserted.

Once a document has been edited, the user usually needs to save it in order to print it, or to edit it further.

An Adobe Photoshop log file records the digital artefacts that indicate entries saved. Adobe Photoshop records the location where the files were originally saved, as well as the original file size. Entries with the actual names of the saved documents are located at about six tenths of the log file. This entry consists of the full file name. It includes the location and the file extension in which the document was saved.

The log file InDesign SavedData contains information about the name and type of the file that was saved, as well as the location where the file was saved. This information is recorded at various locations in the log. The digital artefacts for saved entries are recorded consecutively in the log file, with the latest saved document appearing first.

Printing is one of the last stages of counterfeit document creation. A user might need to create a hard copy of the edited document so that it can be used in a physical environment. Unlike what happens in scanning actions, printing actions can be performed in all the graphic design applications under consideration.

In order to locate the place from which printer(s) were used to print a document, one makes use of one of a number of registry entries to establish a printer connection. After establishing the installed printers, the actual physical existence of the printers can be verified. This can be a great help to an investigator in cases where actual printers have been removed. Physical printers are necessary in an investigation, because they are needed to match the digital evidence to the actual printer so that the case against the criminal can be supported in court proceedings.

User-generated digital evidence

In order to conduct a comprehensive investigation into any crime that has been committed with the use of a graphic design application, the digital forensic examiner must first acquire a thorough understanding of the nature of the files that are generated from the particular graphic design applications that are being used by the criminal.

When examining counterfeit documents, the digital forensic examiner initially examines all changes that have been made to files in a systematic way. The investigator will thus make a careful study of all the fingerprints, barcodes and human faces that are embedded in the graphic design application file types. The three graphic design applications that have been described and utilised in this study are associated with more than 39 file types. In this study, however, the researcher has only focused on file types that are specific to the three graphic design applications, and has excluded other well-known file types.

Before an investigator examines a file intensively, he or she needs to first establish its identity or file extension. Content identification is the process that an investigator uses for determining or verifying particular types of specific files. Counterfeiting criminals have the capacity to alter the file extension of a particular file to confuse potential investigators and conceal the trail that might lead to their conviction. It is therefore essential to confirm the integrity of files by conducting a file signature analysis. In this particular case, a digital forensic examiner must be able to recognise a file type. The real file identity can be found in the content of the file, and is usually known as the file signature. This kind of signature is uniform for all files with an identical file extension. It is normal practice to identify a file signature by examining its first bytes (Carvey, 2009).

Content examination refers to the retrieval of any embedded metadata that may be present in any given file. Content examination necessitates the identification of the metadata of files, which are graphic design application file types. Metadata means "data about data". Metadata is an indispensable component of any forensic digital investigation, because it contains evidential information about what might be extracted from a particular file. Such information may include the name of the tool that was used for criminal purposes or the name of the perpetrator who used the application.

Timeline-associated digital evidence

The timeline of activities refers to the kind of digital evidence that is based on the interpretation of the time stamps that are automatically generated in graphic design applications. Time stamps are a vital and indispensable part of any forensic digital investigation because they provide incontrovertible digital evidence of when alleged criminal activities occurred.

In any digital forensic investigation, it is necessary to establish a timeline so that the chain of criminal actions can be linked and explained in such a way that they are comprehensible to anyone connected with the case who is not familiar with the technicalities of a digital forensic investigation. This kind of explanation is indispensable for obtaining a successful outcome in a criminal case. For example, the suspect will sometimes deny that a particular application was installed and used for creating counterfeit documents. Under such circumstances, it becomes necessary to prove that a particular application was installed and that it was actually

used for criminal purposes. The time stamps that are associated with the installation and the application's subsequent uses are interpreted.

The timeline indicates the sequence of a series of events between the installation and the execution of an application. At this point, the digital forensic examiner will know when the application was installed and when it was last run. The investigator will then be able to make use of the actual files, the time stamps, and the modifying dates obtained from user-generated digital evidence to establish whether these files were created between the time of installation and the last date of execution of the application.

Timelines of this kind can be used to determine whether the actions taken during the editing of the document occurred between the installation of the application and its last use. All of this is vital information to support a case in court against someone who is suspected of counterfeit activities. It is, of course, possible to construct a timeline for other applications if one takes their unique circumstances and settings into account.

Investigating counterfeiting

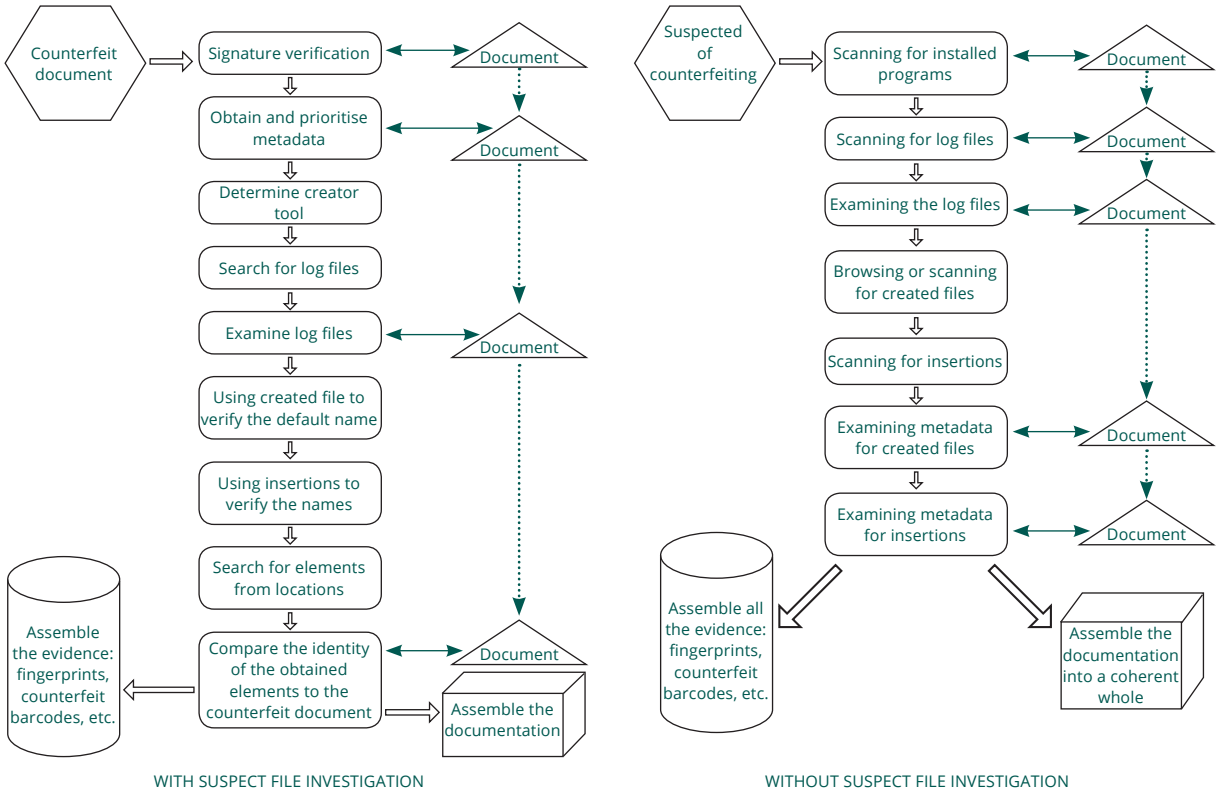
Investigating counterfeiting is a two-pronged process, which is both application- and platform-independent. This means that, with the necessary adjustments, it can be applied to any graphic design application or operating system.

This two-pronged approach is based on two hypotheses. The first, referred to as "without suspect file" (also known as the blue route), is based on a computer system that might have been used for counterfeiting purposes, even though there is no suspicious digital evidence. The system might be questioned because hard-copy counterfeited documents were found in the vicinity of the system. The investigator's task is to establish whether or not the system was actually used for counterfeiting. The second is concerned with investigating a file for which there is *prima facie* evidence of counterfeiting. This is referred to as "with suspect file" (also known as the green route). This approach is based on the existence of a digital file that is assumed to be implicated in the creation of a counterfeit document.

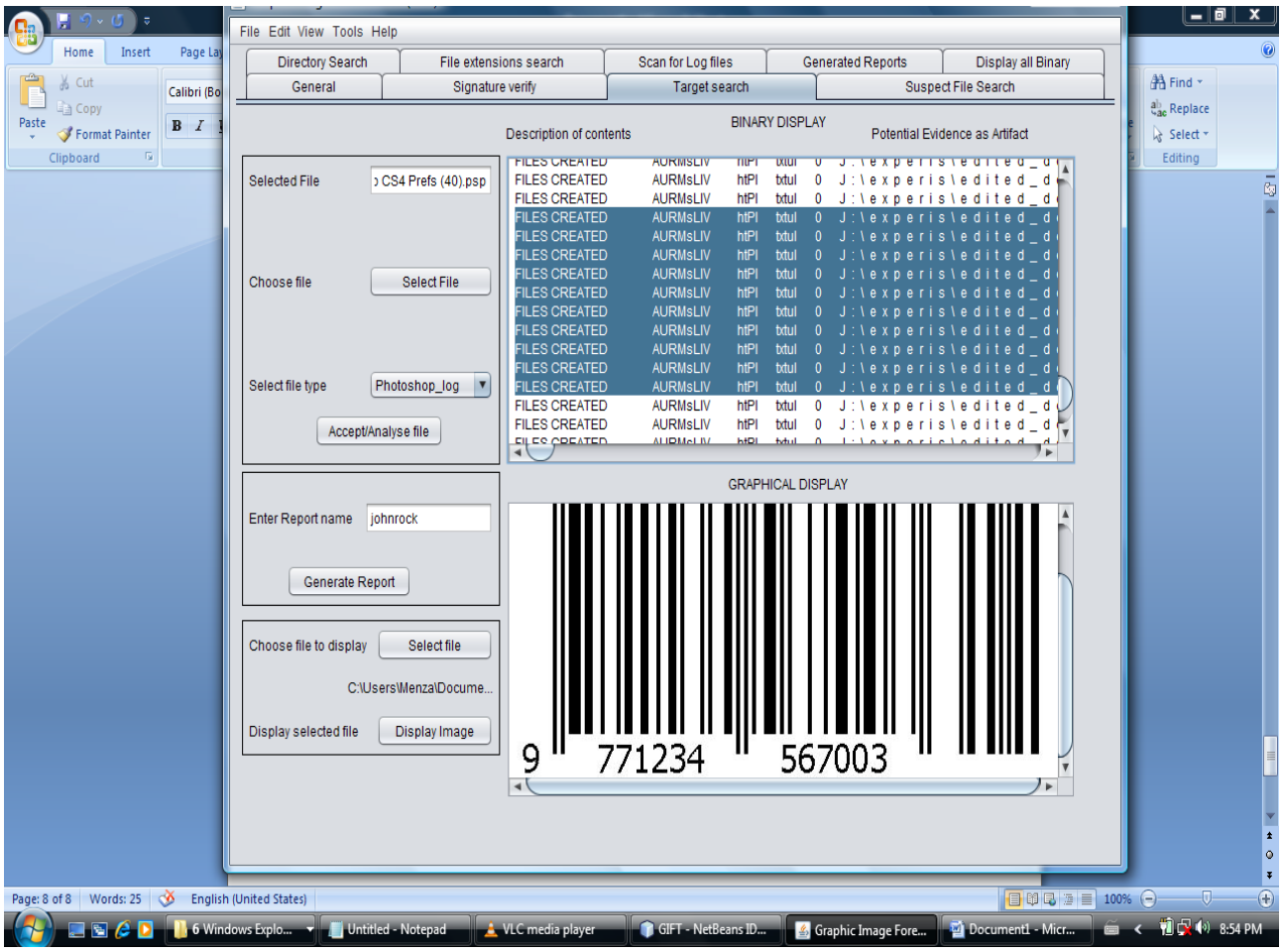
The investigator who uses the green route assumes that an acquired digital document is counterfeit. An investigator can identify a document saved in a graphic design file type and open it using any pre-installed application. This may result in an assumption that it is a counterfeit document. One may arrive at the same assumption by examining the naming of a document. For example, a document that is named Jacob_Meyer_passport is likely to arouse suspicion. When there are reasonable grounds for suspicion, an investigator will accumulate sufficient digital evidence to support the suspicion that the document is counterfeit.

In the counterfeit investigation, the investigator undertakes a number of logical steps to obtain digital evidence that can be used to establish whether the document is counterfeit.

Once a suspect document has been obtained, the first step is to verify its file type (file format). By verifying a file's signature, an investigation is initialised on the identity of that file. It is then necessary to document the file signature from analysis.



→ *Figure 1: Two-pronged counterfeiting investigation process.*



→ *Figure 2: Graphic representation of the tool.*

Graphic Image Forensic Tool

A tool was developed to assist investigators to accumulate digital evidence that indicates how counterfeiting activities were carried out. Graphic Image Forensic Tool (GIFT) was developed in Java programming language on a Net-beans platform. GIFT enables an investigator to examine and perform digital forensic tasks on the basis of the graphic design applications that were selected for this research. This tool can determine whether a suspect file is counterfeit by extracting essential forensic evidence. GIFT can identify the author's name, the time stamps, the copying of the original document and the names of the printed documents. It can also recognise the identities of the inserted objects by displaying the actual barcode and the image of the human face that were inserted during editing, as indicated in Figure 2. As it works on the principle of extracting essential forensic evidence from documents, GIFT may prove to be an indispensable tool for catching perpetrators, particularly as it can successfully reveal actions by criminals to conceal their actions, such as the renaming of files, file deletion and disc wiping.

Prof Hein Venter *is associated with the Department of Computer Science in the School of Information Technology at the University of Pretoria.*

References

Barett, G, Broom, D & Solomon, M. 2005. *Computer forensics*. London: Sybex.

Carvey, H. 2009. *Windows forensic analysis DVD toolkit* 2nd Ed. Elsevier.

Kell, J. 2011. Adobe 2Q net up 54% on broad sales gains, higher margins. *Dow Jones Newswires*. [Online]. Available at http://online.wsj.com. Accessed: 21 June 2013.

Enos Mabuto *is a digital forensic researcher with an MSc Computer Science degree from the University of Pretoria.*