International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 11 Issue 4, April, 2022, Impact Factor: 7.751

Digital Forensics: Digital Evidence Derived From Applications in Graphic Design – A Review

Margaret Gyaawah Duodu[1], Harry Tettey Tetteh[2], Agnes De Cardi-Nelson[3]

[1]Bachelor of Science in Forensic Science, Lovely Professional University, India
[2]Bachelor of Arts in Graphic Design, University of Education Winneba, Ghana
[2]Masters in Business administration, Lovely professional University, India
[3]Council for Scientific and Industrial Research (CSIR)-Institute of Scientific and Technological Information, Accra Ghana

ABSTRACT

Graphic design applications are used to edit and design digital art. The same applications can be used to create forgeries of identification documents (IDs), driver's licenses, and passports. However, the use of any graphic design program generates digital data traces that can be analyzed during a digital forensic investigation. Current digital forensic tools investigate a framework for digital documentation but do not directly examine a system for the creation of fraudulent documents using graphic design applications. This article discusses the Timeline, User, and System created digital forensic evidence generated by several graphic design applications such as Adobe Photoshop, Adobe In Design, and Coreldraw.

Keywords: Digital forensics, Digital evidence, Digital forensic tools, Digital documentation, Graphic design applications, Timeline.

INTRODUCTION

Digital Forensics is a term that refers to the method of preserving, identifying, extracting, and documenting electronic data that can be used as evidence in a court of law. This branch of science is focused on obtaining data from digital media such as a computer, cell phone, server, or network. It equips the forensic team with the most advanced methods and tools for resolving complex digital-related investigations. Digital Forensics assists the forensic team in analyzing, inspecting, identifying, and preserving digital evidence stored on a variety of different types of electronic devices as described by (Guru99, 2021).

Mabuto & Venter (2013) mentioned that Graphic design is used by a variety of industries, including advertising, newspaper publishing, architecture, fashion and design, project management, and manufacturing. Enhancing techniques in graphic design applications include paint brushing, vector painting, digital pen, pencil drawing, and many others. These graphic design applications are used to create one-of-a-kind artwork for business logos, magazine ads, and computer-aided design, to name a few. Most industries use graphic design applications to create visual presentations and employ pictorial expressions to help in communication and concept expression. Professionals in graphic design produce visual material to convey messages. Through using visual hierarchy and page layout techniques, designers can tailor typography and images to a user's individual needs and optimize the user experience by focusing on the logic of presenting elements in interactive designs.

When graphic design applications are used, traces are left behind that can be discovered during a digital forensic investigation. The phases of a digital forensic investigation are usually as follows: discovery, review, interpretation, and reporting. Wherever a person is accused of making forgeries, the standard acquisition procedure is followed. In general, the procurement and reporting phases are identical in different cases; hence, the evaluation and review phases are highlighted. Additionally, the focus is on deciding what the examiner requires prior to reviewing digital evidence. This article addresses the digital traces that are left behind after using graphic design applications. This is accomplished by associating record formation activities with the traces left behind. Additionally, a file analysis is performed on files created by a user from within the program. The authors concentrate on two steps to resolve the problem. To begin, define the digital forensic evidence that indicates whether a document has been scanned or edited, conserved and reproduced. Digital forensic evidence can be found in graphic design applications, where the evidence is primarily provided by the system. The second stage involves determining the contents of user-generated

files through the examination of file signatures and associated metadata. Additionally, to these two stages, a connection with the suspected suspect can be established in this way. Mabuto & Venter (2012).

DIGITAL FORENSICS

A Brief History

The word "digital forensics" was coined as a synonym for "computer forensics" at first. It has since broadened to include the investigation of any computer capable of storing digital data. While the first computer crime was identified in 1978, followed by the Florida Computer Act, it was not until the 1990s that the word "computer crime" became a recognized term. Global policies on digital forensics did not evolve until the early twenty-first century.The first computer forensic technicians were law enforcement officers who were also computer enthusiasts. In the United States, work on the FBI Computer Analysis and Response Team started in 1984. (CART). One year later, the Metropolitan Police in the United Kingdom formed a computer crime unit under the command of John Austen as part of what was then known as the Fraud Squad. At the start of the 1990s, there was a significant change. Investigators and technical support operatives in UK law enforcement agencies, as well as outside experts, recognized that digital forensics (like other fields) needed standard methods, protocols, and procedures. Apart from informal guidelines, these formalisms did not exist but were urgently required to be established. In 1994 and 1995, the Serious Fraud Office and the Inland Revenue convened a series of conferences at the Police Staff College in Bramshill that developed modern British digital forensic methodology.

As the science of digital forensics progressed, these guidelines and best practices gradually developed into standards, and the discipline was brought under the jurisdiction of the Forensic Science Regulator in the United Kingdom.(The Open University, 2021)

DIGITAL FORENSICS INVESTIGATION

A data trail that you leave behind when you use the internet, websites you access, emails you send, and data that you enter in online services is called digital footprint. The investigator can retrieve vital data for solving the criminal case by tracking the digital footprints.

Cyber forensic analysts

They are experts in decrypting data using a variety of technologies and tools. Depending on the nature of cybercrime, investigators will use a variety of techniques including emerging ones. The duties of a cyber investigator include retrieving deleted files, cracking codes, and determining the cause of a security breach. Once gathered, the information is preserved and interpreted so that it can be used in court or for police to investigate further.(Digital Forensics, 2021)

Computer evidence

Also known as digital evidence, is described as any hardware, software, or data that can be used to prove one or more of the ‘who, what, when, where, why, and how' questions pertaining to a security incident. Computer evidence also includes computer files and their contents that are left behind after an incident. Any data that can be used to determine that a crime was committed or to prove a connection between a crime and its victim or perpetrator is considered digital evidence. Digital evidence is made up entirely of binary value sequences called bits. It is necessary to note, however, that the evidence should be presented in its logical order in court or at a disciplinary hearing according to Mabuto and Venter (2013).

Digital forensic artifacts

These are traces left behind using an application or an operating system. An investigator discovers the facts about an incident by identifying and revealing the traces of the event that have been left on the device. Because of the loaded legal connotations associated with the word "evidence," the term "artifacts" is preferred to refer to these remains. When a perpetrator attempts to remove these artifacts, they will leave other artifacts behind. For example, when attempting to remove log files from a system, one can use a removal tool, which leaves additional traces suggesting that a log removal tool was used.For specific digital forensic investigation, dispersed evidence inside a framework may suggest what happened.

The more complicated the context of digital information becomes because of media factors that embed the data, the more difficult it is to uncover the truth. Formatting has an impact on how digital information is accessed, such as digital evidence in the form of records, which are divided into three categories:

- Archival Files
- Active Files
- Residual Data

Archived files are needed for the archiving purpose, which includes handling documents to be stored in the specified format, retrieving, and distributing process for other needs, such as certain digitized documents to be stored in TIFF format to preserve document quality. Active files, such as image files and text papers, are used for a variety of purposes that are closely linked to the tasks being performed. The residual files, on the other hand, are those that are generated as a result of computer processes and user activities, such as internet usage records, database logs, various temporary files, and so on. Since digital information is dispersed through multiple platforms and contexts, it necessitates more planning than simply classifying data for forensic purposes. Keep in mind that the more peripherals or devices that are built into computer systems, the more complicated and time-consuming it will be to raise digital evidence as was contributed by Leong, R. S. (2006)

THE DIGITAL FORENSICS PROCESS

The process of digital forensics can be categorized into three activities namely:

- Acquisition
- Analysis
- Presentation

(Altheide & Carvey, 2011) suggests that the selection of digital media to be analyzed is referred to as acquisition. There may be physical hard drives, optical media, memory cards from digital cameras, cell phones, embedded computer chips, or even single document files, depending on the form of inspection. In either situation, the media to be investigated should be handled with care. At the very least, the procurement process should include making a replica of the original media (the working copy) as well as keeping detailed records of any activities taken in the original media. Those objects would be subjected to the required examination. This may include file system analysis, file content examination, log analysis, statistical analysis, or any other form of study. Finally, based on the examiner's training, skill, experimentation, and experience, the examiner interprets the findings of this study. The mechanism by which the investigator presents the findings of the analysis phase with the involved party or parties is referred to as presentation. This entails creating a report detailing the examiner's activities, objects discovered, and the significance of those artifacts. The examiner can also defend these results if they are challenged during the presentation process. It should be noted that the results of the analysis process will lead to additional acquisitions, each of which will produce additional analyses, and so on. Given a large network breach or a lengthy criminal investigation, this feedback loop will last for several cycles.

GRAPHIC DESIGN APPLICATIONS

Graphic designers create visuals using their imagination as well as different tools. They make everything from blogs to video games. They work professionally in several fields such as entertainment, education, and advertisement, as well as putting special effects in movies.

Graphic design software applications are interesting and have specific features. Innovative and imaginative projects can be produced with the aid of these tools. The list of these applications is vast, and the field is continually evolving and increasing as new applications are added to the list. As there are no reference recordings or rankings for all graphic design applications, what follows is a list of random examples of graphic design applications that are currently in use.

- Adobe
- CorelDraw Graphic
- AutoCAD
- Free DWG
- Primo
- Sweet Home 3d
- Google SketchUP
- Ulead
- Edraw Max
- DAZ Studio
- ChemDraw Ultra
- Photo to Cartoon
- Easy Flyer
- PCB artist
- Sothink

All the graphic design applications listed above can perform similar tasks but in different ways. As a result, digital forensic investigators must be mindful that different applications leave different trails and residues of information behind, and that all of these must be interpreted appropriately. Even though many graphic design applications are now available to consumers, Adobe Systems Incorporated remains the best software creator in the Graphic design software group. As a result, the authors researched graphic design applications and their relationship to digital forensic evidence and digital forensic investigation. Adobe graphic design applications such as Adobe Photoshop, Adobe In-Design, and Adobe Illustrator are examples of Adobe graphic design applications. These Adobe applications are used to edit texts, images, videos and, or audios. An exclusive review of the possible digital forensic evidence provided by these applications is required. Most graphic design consumers prefer the most recent versions of these Adobe applications as cited by Mabuto and Venter (2013).

Adobe Systems Incorporated owns digital technology used for internet purchases, business applications, and social technologies, which lead forensic evidence researchers to consider using Adobe applications to retrieve forged image information and analyze them. For document editing, Adobe applications such as Adobe Illustrator, Adobe Photoshop, and Adobe InDesign can be used. Due to this, an exclusive search for possible digital forensic evidence is needed.(Elsheik, 2016).

GRAPHIC DESIGN APPLICATIONS

Photoshop - Image Editing Software
It is the industry's most versatile and widely used application. Some of the other applications of Adobe Photoshop in our everyday lives include typographic, graphical, artistic, and technical uses. Product design, website mock-up designs, business card designs, movie poster designs, different forms of digital content, branding and marketing material designs, and so on are some other typical uses of Photoshop. One can also use the software to design, draw maps, satellite views, and display the landscape, rivers, and trees in icons and small graphics. It is commonly used in gaming apps, business listing portals, and other similar applications.

Uses

- Its primary function is to edit and retouch photographs.
- It is used to build web templates.
- Using adjustment layers, brighten a picture and make the colors pop.
- Remove any unnecessary material and apply artistic effects to each sheet.

Adobe Illustrator - Image editing software
Adobe illustrator is a vector drawing application, whereby artists and graphic designers are not the only ones who will profits from it. Those who want to make a website can use Illustrator to make a mock-up, which is used to create vector images that can be used on a variety of platforms. Illustrator, as an Adobe product, integrates seamlessly with the rest of the Creative Suite.

Uses

- Illustrations, cartoons, graphs, maps, and logos are often created with it.
- The shapes are drawn using mathematical equations.

Adobe InDesign
Adobe InDesign is a desktop publishing program which allows people to make simple edits and effects to pictures. People also use the tools in InDesign to make simple vector illustrations. It can create a layout with a combination of text, photos, and color, or only text or images, without difficulty.

Uses

- The software is used to make leaflets, posters, brochures, magazines, newspapers, and books, among other things.
- When used in conjunction with Adobe Digital Publishing Suite, it can also render content suitable for tablet devices.

Corel Draw
CorelDraw is a vector graphics program with a lot of options. It gives users a variety of resources to use to generate original images or radically alter them. QR code creation, page layout, and special effects are only a few of the thing’s users can do with the software. The software to create pattern designs ranging from simple shapes and lines to more complex patterns used in vector illustration, logos, and other projects.

USER GENERATED EVIDENCE IN GRAPHIC DESIGN APPLICATIONS

When a crime occurs that relates to digital forensics, the investigator most importantly has to determine the type of files or documents that are generated from the specified graphic design application used by the perpetrator to run an in-depth or inclusive investigation.

Content Identification
This is the process that digital forensic investigators or examiners use to validate or detect the specific type of files under investigation. Therefore, when examining the file or document intensively, they must first determine the identity or file extension.

Counterfeiting investigation and counterfeit document examination

A counterfeit investigation is a bilateral process. What this means is when significant adjustments are made, they can be implemented in operating systems (OS) or various graphic design applications. This process is both application and platform autonomous. When it comes to investigating counterfeit documents like passports, drivers' licenses, social security cards, etc., the examiner checks for all the alterations or changes that have been made to the documents or files structurally. The investigators will have to painstakingly study all barcodes, fingerprints, etc., that have been inserted in the graphic design application files. Criminals who engage in counterfeiting have the requisites to change the file extension of specific files to hide the trace and trail of the files to confuse the prospective investigator or examiner. It is then necessary to confirm the file integrity by conducting a file signature analysis. (Sammons & Cross, 2017), defined a file signature as a special set of identifying bytes written to the header of a file. A file signature is usually found in the first 20 bytes of a file on a Windows system.

A Windows Bitmap image file (.bmp extension) starts with the hexadecimal characters 42 4D in the first two bytes, which correspond to the letters “BM.” The digital forensic examiner must be able to recognize and identify a file type. The file identity can be found in the contents of the file which is also known as file signature. The extraction of any embedded metadata that may be present in any given file is known as content examination. Identification of the metadata of files, which are graphic design application file types, is needed for content analysis. Metadata refers to "data about data." Metadata is an essential aspect of any Forensic digital investigation since it provides evidence about what can be recovered from a specific file. These details may include the name of the tool used for the criminal activity or the perpetrator who used it.

TIMELINE-RELATED DIGITAL EVIDENCE

In a digital forensic investigation, it is important to determine a timeline so that the series of criminal activities can be connected and explained in a way that is understandable enough for anyone unfamiliar with the formalities of a digital forensic investigation. The timeline activities refer to the kind of digital forensic evidence that is focused on the interpretations or explanations of the timestamps that are automatically generated in graphic design applications. A timestamp is a computer-recorded event's current time. A device keeps a correct current time, tuned to minute fractions of a second, using mechanisms such as the Network Time Protocol (NTP).(Tech Target contributor, 2005) describes timestamps as a valuable part of digital forensic investigation because they give indisputable digital evidence.

The timeline depicts the sequence of events that occur between the implementation and execution of an application. The potential forensic examiner will now know when the program was installed, and the last time it was used. The investigator will then use the original data, time stamps, and modifying dates collected from user-generated digital evidence to determine if these files were produced between the time of implementation and the last date of application execution. These types of timelines can be used to evaluate if the activities performed during document editing occurred between the application's implementation and its last use. All this information is critical in establishing a case against those accused of counterfeiting activities in court. Of course, a timetable for other applications is possible if one takes their specific situations and settings into account.

DIGITAL EVIDENCE GENERATED FROM GRAPHIC DESIGN APPLICATION SYSTEMS

The term "system-generated digital forensic evidence" refers to evidence that is generated automatically by an application without user intervention. These digital forensic artifacts record the scanning, editing, saving, and printing of a document.

Generally, when attempting to create a fake document, one must first obtain an authentic document used to create a new and fraudulent identity. When a suspect does this, the first thing they do is scan the original document into a digital format that can be edited on a computer. Paper editing is a critical step in the development of a forgery since

it enables the criminal to insert items of interest into the scanned document. These can include a photograph of an individual, a barcode, or a fingerprint.

CONCLUSION

Over the last decade, digital forensic science has seen many achievements. The value of digital evidence is now widely understood, and the digital forensic research community has made significant strides in ensuring that the term "digital forensic science" includes the word "science."There are numerous other aspects of computer forensics that need further examination. This sector has grown to play a critical role in exposing computer crimes. It is vital to track any human activity that affects the community's interests, more so now that people have easy access to the internet, including from their mobile phones. Additionally, digital evidence collection is needed in resolving cases involving counterfeit files or records that are widely associated with specific graphic design applications. Although this paper focused on digital evidence created by Adobe applications, the same principles apply to other graphic design applications.

REFERENCES

[1]. Altheide, C., & Carvey, H. (2011). Digital forensics with open source tools. Waltham: Elsevier Inc.
[2]. Digital Forensics. (2021). Retrieved from https://www.eccouncil.org: https://www.eccouncil.org/what-is-digital-forensics/
[3]. Elsheik, M. E. (2016). A Survey in Modern Techniques in Digital Forensic Evidence in Graphic Design Applications. International Multilingual Academic Journal, 8.
[4]. Guru99. (2021). What is Digital Forensics? History, Process, Types, Challenges . Retrieved from https://www.guru99.com/digital-forensics:https://www.guru99.com/digital-forensics.html#:~:text=Digital%20Forensics%20is%20defined%20as,phone%2C%20server%2C%20or%20network.
[5]. Ieong, R. S. (2006). FORZA–Digital forensics investigation framework that incorporate legal issues. digital investigation, 3, 29-36
[6]. Mabuto, E., & Venter, H. (2013). System-Generated Digital Forensic Evidence in Graphic Design Applications. Journal of Digital Forensics, Security and Law, 8(3), 4.
[7]. Mabuto, E. K., & Venter, H. S. (2012). Finding Digital Forensic Evidence in Graphic Design Applications. In WDFIA (pp. 12-26).
[8]. Sammons, J., & Cross, M. (2017). The basics of cyber safety. Elsevier Inc.
[9]. Tech Target contributor. (2005). Timestamp. Retrieved from https://whatis.techtarget.com/: https://whatis.techtarget.com/definition/timestamp#:~:text=A%20timestamp%20is%20the%20current,is%20recorded%20by%20a%20computer.&text=Such%20precision%20makes%20it%20possible,and%20applications%20to%20communicate%20effectively.
[10]. The Open University. (2021). Digital forensics. Retrieved from https://www.open.edu: https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.2#:~:text=Until%20the%20late%201990s%2C%20what,and%20Response%20Team%20(CART).