

ORIGINAL ARTICLE

Open Access



Using digital forensics in higher education to detect academic misconduct

Clare Johnson^{*} , Ross Davies  and Mike Reddy

^{*}Correspondence:
clare.johnson@southwales.
ac.uk
University of South
Wales, Newport Campus,
Newport NP20 2BP, UK

Abstract

Academic misconduct in all its various forms is a challenge for degree-granting institutions. Whilst text-based plagiarism can be detected using tools such as Turnitin[™], Plagscan[™] and Urkund[™] (amongst others), contract cheating and collusion can be more difficult to detect, and even harder to prove, often falling to no more than a 'balance of probabilities' rather than fact. To further complicate the matter, some students will make deliberate attempts to obfuscate cheating behaviours by submitting work in Portable Document Format, in image form, or by inserting hidden glyphs or using alternative character sets which text matching software does not always accurately detect (Rogerson, *Int J Educ Integr* 13, 2017; Heather, *Assess Eval High Educ* 35:647–660, 2010).

Educators do not tend to think of academic misconduct in terms of criminality per se, but the tools and techniques used by digital forensics experts in law enforcement can teach us much about how to investigate allegations of academic misconduct. The National Institute of Standards and Technology's Glossary describes digital forensics as 'the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony.' (NIST, *Digital Forensics*, 2021). These techniques are used in criminal investigations as a means to identify the perpetrator of, or accomplices to, a crime and their associated actions. They are sometimes used in cases relating to intellectual property to establish the legitimate ownership of a variety of objects, both written and graphical, as well as in fraud and forgery (Jeong and Lee, *Digit Investig* 23:3–10, 2017; Fu et. al, *Digit Investig* 8:44–55, 2011). Whilst there have been some research articles and case studies that demonstrate the use of digital forensics techniques to detect academic misconduct as proof of concept, there is no evidence of their actual deployment in an academic setting.

This paper will examine some of the tools and techniques that are used in law enforcement and the digital forensics field with a view to determining whether they could be repurposed for use in an academic setting. These include methods widely used to determine if a file has been tampered with that could be repurposed to identify if an image is plagiarised; file extraction techniques for examining meta data, used in criminal cases to determine authorship of documents, and tools such as FTK[™] and Autopsy[™] which are used to forensically examine single files as well as entire hard



drives. The paper will also present a prototype of a bespoke software tool that attempts to repurpose some of these techniques into an automated process for detecting plagiarism and / or contract cheating in Word documents.

Finally, this article will discuss whether these tools have a place in an academic setting and whether their use in determining if a student's work is truly their own is ethical.

Keywords: Digital forensics, Academic integrity, Misconduct, Higher education, Detection

Introduction

Academic misconduct is a challenge that any organisation assessing student work faces. Awarding credit for work that has not been completed solely by the student can bring the reputation of the institution into question and devalues the qualification (Kimber 2018). Plagiarism is defined in the European Network for Academic Integrity's Glossary as "Presenting work/ideas taken from other sources without proper acknowledgment" (ENAI 2021) and it can take a variety of forms including copy and paste plagiarism, collusion and contract cheating.

Whilst the best solutions to academic misconduct would be to predict, discourage or even prevent cheating behaviours, the reality is that this is a highly complex challenge, so assessors currently rely primarily on detection. It is a topic that has been studied in some detail, and a variety of detection tools already exist such as Plagscan (<https://www.plagscan.com>), Urkund (<https://www.orkund.com>), Turnitin (<https://www.turnitin.com>) and recently, Word 365's Editor feature (Microsoft n.d.), for example. In the main these tools use text matching to detect plagiarism, by searching journal repositories and / or the Internet for sources that match content in the student submission, and as such they can have significant limitations as identified by existing research (Bertram Gallant et al. 2019; Rogerson 2017; Weber-Wulff 2019). These challenges include matching content where the text is a standard definition or explanation, difficulties in identifying and attributing patchwriting because of its fragmented nature, and problems with analysing text where the student has made deliberate attempts to obfuscate their actions by submitting text as graphics or with hidden characters, or through linguistic or stylistic alternations (Bertram Gallant et al. 2019; Foltýnek et al. 2019; Rogerson 2017). More recently, Turnitin has introduced authorship tools which looks at basic metadata such as date and time created, who the document was created by, time spent editing and software version, as well as comparing work to previous student submissions and other students in a group using linguistic analysis, and as Dawson, Sutherland-Smith and Ricksen (2020) found in their research. The availability of authorship reports can have a positive impact on detection rates. But the challenges in detecting plagiarism and particularly contract cheating still persist, and what none of these tools do at the time of writing is apply more sophisticated digital forensics techniques to student submissions, which begs the question as to whether we can learn anything from criminal investigations that could be used within academia.

This paper will discuss existing tools and techniques along with several brief examples of how they are currently used, followed by experimentation on several test files to demonstrate how they might be used in an academic setting, along with an explanation of the limitations of these existing tools. The authors will then go on to present a

proof-of-concept for the development of a bespoke tool that repurposes these methods for academic integrity purposes. Finally, the authors will reflect on the findings of these experiments and the implications of using such techniques in an academic setting.

Background review

The application of digital forensics techniques in establishing the facts of a crime is not new. First termed 'computer forensics', these techniques began during the mid 1980's, growing in popularity throughout the late 80's and early 90's, with the first ever Computer Analysis and Response Team being created in the USA in 1984 (Whitcomb 2002), followed a year later by a Computer Crime Squad in London's Metropolitan Police. With the massive growth in cyber crime in recent years, digital forensics techniques and tools have developed at pace as we race to secure our information in the online space, including in the protection of intellectual property rights, of which student work could be considered an example.

The National Institute of Standards and Technology Glossary (NIST 2021) describes digital forensics as 'the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony'. These techniques are used in criminal investigations as a means to identify the perpetrator of, or accomplices to, a crime and their associated actions. They are sometimes used in cases relating to intellectual property to establish the legitimate ownership of a variety of objects, both written and graphical (Fu et al. 2011), as well as in fraud and forgery (Jeong and Lee 2017).

Using digital forensics in academic misconduct settings has been mooted previously by Klopper (2009), who suggests that the weakness of anti-plagiarism programs is that they function on non-semantic grounds and that they only use the surface web to access documents. Klopper discusses the disciplines of Forensic Auditing and Computer Forensics and their shortcomings, and suggests that a new interdiscipline combining Cyber Forensics and Forensic Linguistics, namely 'Cyber Forensic Linguistics', would help harness the tools that could counteract plagiarism. This focuses on linguistics and forensic analysis using computing techniques, linked to the surface and dark web. However, as with many previous suggestions of 'forensics' this approach focuses primarily on the text or language within the document, not on the document as an object in its own right.

Examples of digital forensics in law enforcement

In both cyber crime and physical crime, digital forensics are playing an increasingly important part in evidence gathering. Freeman and Llorente (2021) discuss various forms of digital evidence and their application in law, including video and audio evidence, data in the cloud and on the Internet, files on a hard drive, emails and text messages. There are examples of wearable devices being analysed to ascertain the movements of individuals involved in murder cases, for example the murders of Connie Dabate in 2015, where a Fitbit was used to disprove the husband's story (Almogbil et al. 2020) and Caroline Crouch in 2021, where heart rate data was used to disprove the husband's story (BBC 2021). In business, evidence of data exfiltration has been provided through network forensics analysis, proving that employees have sent data outside of the organisation, as in the case of Zhang and Apple

(US Department of Justice, 2018) where log files were used to prove theft of Trade Secrets. The presentation of such digital evidence in court follows strict regulations for admissibility to help avoid any false conclusions being drawn.

Digital forensics tools and techniques

Before establishing whether digital forensics tools and techniques have a role in detecting academic misconduct, it is useful first to summarise some of the tools available and what information they can tell us.

Reverse Engineering in digital forensics is a technique commonly used to understand how malware works, by reversing or unpacking files and programmes back to their component parts. This is often a manual process requiring an excellent understanding of programming and compiling code. Digital forensics software does a similar thing on files and devices by taking entire storage drives and separating out all the various parts (users, graphics, text, email, chat and so on). Typically carried out on digital forensics software such as Access Data's FTK™ (Forensic ToolKit), Magnet Forensics™, Encase™ and Autopsy™ these software solutions facilitate the building of a user profile by establishing a timeline of activity across many different components including web browsing history, some chat logs, email interrogation, image searching and much more. Similar techniques can be used on single files, although they yield less comprehensive results. During evidence gathering, investigators are permitted only to analyse areas of a device that relate to the case in question, thus protecting user profiles to some degree. It is possible that these software tools could help in the detection of some cases of academic misconduct.

Alongside these software solutions, there are some standard techniques used by law enforcement and digital forensics which could also prove useful in detecting academic misconduct. For example, 'hashing' is a one-way cryptographic function which takes any input (e.g. a password, image or file) and produces a unique message digest – effectively a fingerprint of the file, which cannot be reversed (in that it is not possible to reconstruct the original file from just the hash value) and which is unique to the file that was input. Therefore, if two images share the same hash value, those images must be identical. Hash values are used to swiftly examine the images on entire computer hard drives searching for known illegal images, such as child pornography, and it is a technique which is likely to become increasingly important in identifying cases of fake news and deepfakes. Fig. 1 is an example of a hash value created from a random file on the author's computer:

Another technique used in law enforcement is that of Reverse Image Lookup (RIL). RIL is a form of Content Based Information Retrieval that uses special search image methodologies based on an image's attributes such as colour, shape and texture to search the Internet for images that match (Chutel and Sakhare 2014). Digital Forensic investigators use RIL to carry out investigations such as determining the location of crimes that have been videoed or photographed and put on social media, to help locate missing persons and in cases of identity theft. Various online tools exist for this purpose including Tin Eye, Google Images, Yandex and Bing Image Match.



ea706481bc2b66cb50eb3469b81385df

Fig. 1 Example of a hash value

These are just a few examples of digital forensics techniques that are used by law enforcement, but examining the data using these tools requires significant expertise, meticulous attention to detail, and knowing what to look for and how to find it. Applying these techniques in an academic setting would require a radical rethink of how the tools can be used. For example, none of the digital forensics software tools (FTK, Autopsy etc) readily extract the underlying metadata (e.g. XML) from a file and yet this data can provide a rich source of information in relation to document construction, which can be very useful in an academic setting.

The law's reach into academia

Academic integrity enforcement is not typically associated with the law and criminal proceedings, yet there are an increasing number of specific cases where this is beginning to happen. Whilst most institutions will have sort of academic integrity or misconduct policy these tend to be focused on institutional breaches and would not usually involve the law, other than in cases relating to intellectual property theft of research related works.

Quality assurance agencies in several countries have made essay mills (the organisations providing essay writing services to students for a fee) illegal. Australia, New Zealand, some states in the USA, and the Republic of Ireland all have legislation that criminalises some aspect of these services, and the UK announced in September 2021 it will shortly follow suit, meaning that it will become a criminal offence to provide, arrange or advertise cheating services for financial gain (UK Government 2021). This clear intention to use legal force to prevent contract cheating, or outsourcing of assessments, is an example of how legal processes are seeping into educational settings.

Furthermore, the UK Quality Assurance Agency (2021) has done a great deal of work in supporting academic institutions to prevent, detect and manage academic misconduct. In 2021 they provided advice for Higher Education Institutions on how to prevent the emerging threat of essay mills hacking into university websites to redirect students to their essay writing services. One suggestion they make is to block connections to university networks using the IP addresses of known essay mills (effectively using the online address of an essay mill to block access to students by filtering out any Internet traffic coming from these addresses). However, this relies on security methods such as IP scanning and IP blocking, which are only successful if the IP address of the Essay Mill is known and does not change regularly.

Types of academic misconduct

It's useful at this point to briefly consider types of academic misconduct and how students attempt to obfuscate their actions. Copy and paste plagiarism (where content is taken from a source without proper referencing), contract cheating (where a third party provides the work for the student, often, but not always, in return for payment) and collusion are the main forms of academic misconduct that are considered in this paper. In terms of copy and paste plagiarism and collusion, students may change minor elements of the text, perhaps substituting single words throughout a document with an alternative, or making small deletions or additions, as this will thwart text matching software. Other techniques which students have been known to use to 'beat' text matching

software include adding white characters between words, using alternative character sets and replacing text with images of text. When using images to support the narrative, students may crop out unwanted parts of the image and sometimes these cropped out areas may provide clues to the original source of the image, such as from a social media 'chat' or post, or from a website. In terms of contract cheating, minor changes to the work received from the contracted author are sometimes carried out, such as adding the student's name, or changing odd words to reflect nuances of the institution where the student is based and so on.

Can digital forensics tools and techniques be used to detect and evidence academic misconduct?

Examples of tools and techniques used in a digital forensics setting have been discussed, but can these methods be repurposed to aid in the detection of academic misconduct? Techniques such as file hashing could potentially be used to confirm collusion, or to match an image in a student submission to an online image, but this application would seem to be of limited benefit. Reverse Image Lookup could similarly have some uses if, for example, an image in a student submission has not been referenced, in order to locate the original source. However, this too seems limited, perhaps being more relevant as a way of pursuing cases of intellectual property theft. Techniques for extracting forensic data can be useful and are already used in some institutions. The learning management system, for example, can provide information on access to the platform, engagement with resources, issues encountered during examinations and more via logs and reports. E-Proctoring is also used increasingly for examinations carried out at a learner's place of choice, where analytical tools can be used to track the learner's activities in an attempt to reduce the possibility of cheating. However, of all the digital forensics tools mentioned thus far, reverse engineering of student submissions would appear to be the most useful.

Reverse engineering in academic integrity

Microsoft file formats, along with a number of other software packages, use XML as their underlying language. XML refers to Extensible Markup Language and is used because it helps with file sharing, tracking changes and keeping file version histories which allow a user to revert to a previous version of the document if required. XML forms the backbone of many documents, but it is rarely examined for any other purpose.

Whilst authorship tools are beginning to extract some of this XML metadata from student submissions they currently collect only the most basic details. Essentially these techniques dip into reverse engineering, but only in a very limited way. Didriksen (2014) carried out a forensic analysis of Open Office XML (OOXML), the underlying language of a Microsoft Word document, to establish what information can be extracted by unpacking its component parts. Didriksen notes that documents created with word processors may form part of a forensic investigation and that the XML of these files contain data that may support an investigation in a number of ways, including determining the original source of the document and detecting plagiarism. Didriksen's work examines the underlying XML in some detail, providing a very useful starting point for this type of forensic investigation of Word documents.

Johnson and Davies (2020a) take this a step further by extracting the XML from a student submission known to have been written by an essay writing service. By extracting the XML they were able to examine how the document had been created and edited using Revision Identifiers or 'rsid' tags. rsidR tags are used to mark changes carried out within the numerous editing sessions for a document, and editing carried out in a single session will share the same rsidR value, which are randomly assigned throughout the life of the document. Documents with very few edit (rsidR) tags suggest that very little editing has been carried out, which could be indicative of contracted work that has been saved into a new document ready for submission. Examining where the edits have been carried out can also be useful indications of contract cheating, for example, if the only information in a document that has been changed is the student name, or references to a specific course or institution related aspect. To demonstrate what XML markup looks like, a very simple document was created with the text 'The cat sat on the mat'. The document was saved, and then the word 'cat' was changed to 'dog' and the document resaved. The XML for the paragraph containing the text appears as shown in Fig. 2:

In this example, the mark up shows where the word 'cat' was changed to 'dog' in a separate editing session (or rsidR session) to the rest of the text (highlighted in bold in the example). Here, the word 'dog' has an rsidR value of 006D0D43, whilst the rest of the sentence has the rsidR value 001E7189. This shows that the word 'dog' was added to the document at a separate time to the rest of the sentence.

This XML can also help to identify the URLs of images if they have been copied from the Internet, as well as highlight where fonts and other features have been changed, something that has been further explored in Johnson and Davies (2020b) by looking at things such as underlying font styles, the relative frequency of formatting tags in plagiarised works, redundant formatting tags (that possibly suggest something has been deleted or reformatted to match the default document styles), frequency of words to rsidR edits and more, in an attempt to build a series of 'flags' for assessors. In addition,

```
<w:p w14:paraId="109D6D06" w14:textId="1623CF67" w:rsidR="001E7189" w:rsidR
Default="00D20A60">
  <w:r>
    <w:t xml:space="preserve">The </w:t>
  </w:r>
  <w:r w:rsidR="006D0D43">
    <w:t>dog</w:t>
  </w:r>
  <w:r>
    <w:t xml:space="preserve"> sat on the mat.</w:t>
  </w:r>
</w:p>
```

Fig. 2 Example xml extracted from the document.xml file

the media files that are available when the document has been converted to its component parts show images in full, even if the document itself shows the cropped version, which can provide useful information if taken from screen shots (where information that helps to identify the original source may appear in the cropped-out area). Jeong and Lee (2017) also note that two documents sharing a rsid value in the settings.xml file indicates that both files have originated from the same source and suggest that these findings could be useful in fraud and forgery cases, though this would also be highly beneficial in providing evidence for allegations of collusion.

Research methodology

Several simple experiments were carried out using existing digital forensics software in order to see how useful these tools might be in detecting academic misconduct. This consisted of creating three files for analysis, using techniques known to be used by some students to obfuscate cheating behaviours, which were then transferred to a USB storage device for analysis. The documents included:

- A test document called 'Text document.docx', containing only simple text for baseline testing;
- A document called 'Cropped Images.docx' which contains a cropped image to see how easily the software could alert the examiner to a cropped image within the text;
- A document called 'Random white space.docx' that contains text copied directly from the Internet, which attempts to fool text matching software by adding white x's between words (thus making the words unrecognisable).

'Text document.docx' acted as the control, and was used to verify that there were no unusual or anomalous characteristics within the file when examined by checking that the file contents and metadata were as expected, thus establishing that the software was not faulty.

The USB containing the above three files was imaged using Access Data's FTK Imager v4.2.1.4. An 'image' is an exact copy of the data on the drive that can be analysed in detail without risk of tampering with the contents and is a technique used by digital forensics examiners to maintain the integrity of the evidence. The image file was opened in FTK v7.1.0.290 as evidence, ensuring that MS Office was included as an option in the set-up screen (Fig. 3). FTK is a proprietary digital forensics software kit, used by police departments across the world. These tests were also carried out on Autopsy 4.15.0, which is an open source (free) digital forensics examination tool. Results tallied with those of FTK.

Once opened in FTK, it was possible to see all the files on the USB storage device (Fig. 4).

Results

The 'Cropped Images' file was examined to see if the results were able to identify that the image within the file had been cropped. In the Overview tab, the Natural view of the file showed the cropped image as it appears in the finished document (Fig. 5), but by switching into the Graphics tab it was possible to see the whole image (Fig. 6). However, identifying that the image within the Word document had been cropped was entirely manual,

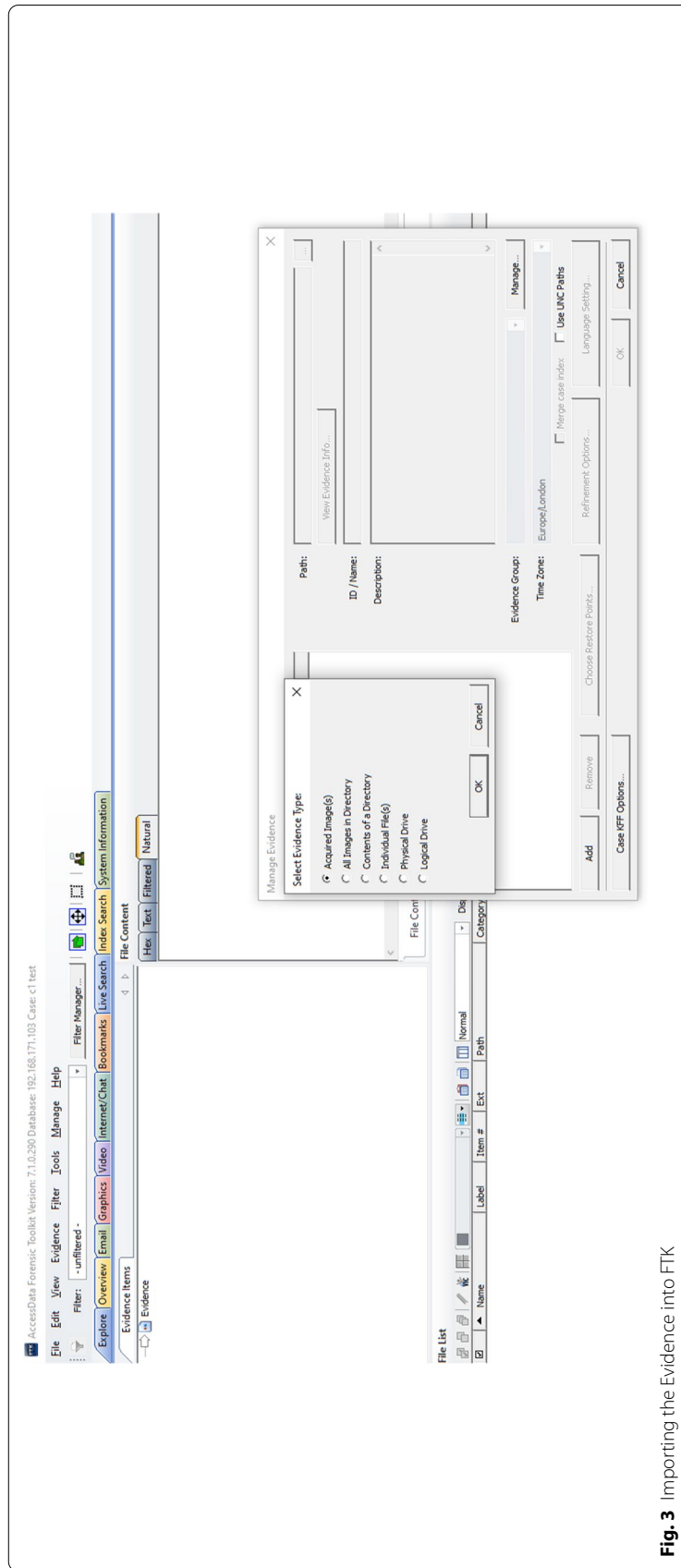


Fig. 3 Importing the Evidence into FTK

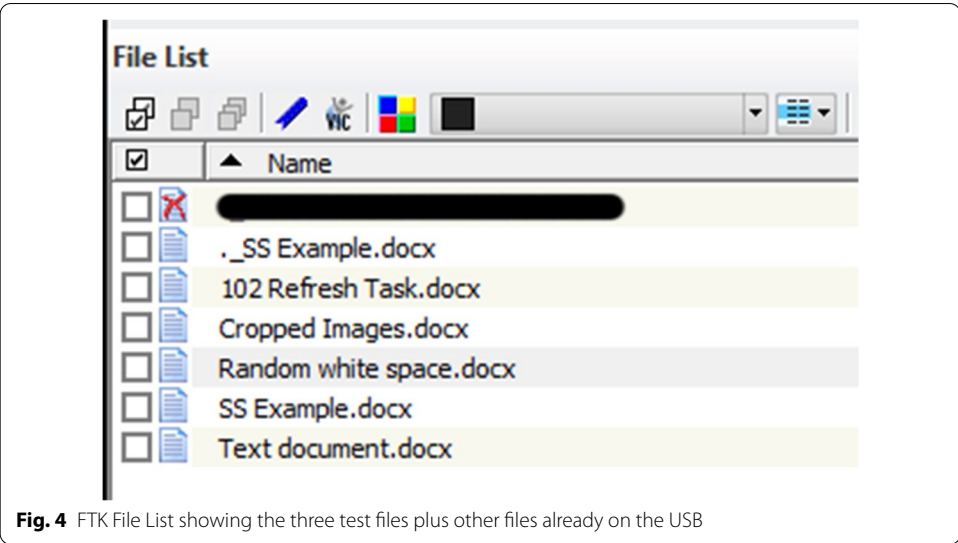


Fig. 4 FTK File List showing the three test files plus other files already on the USB

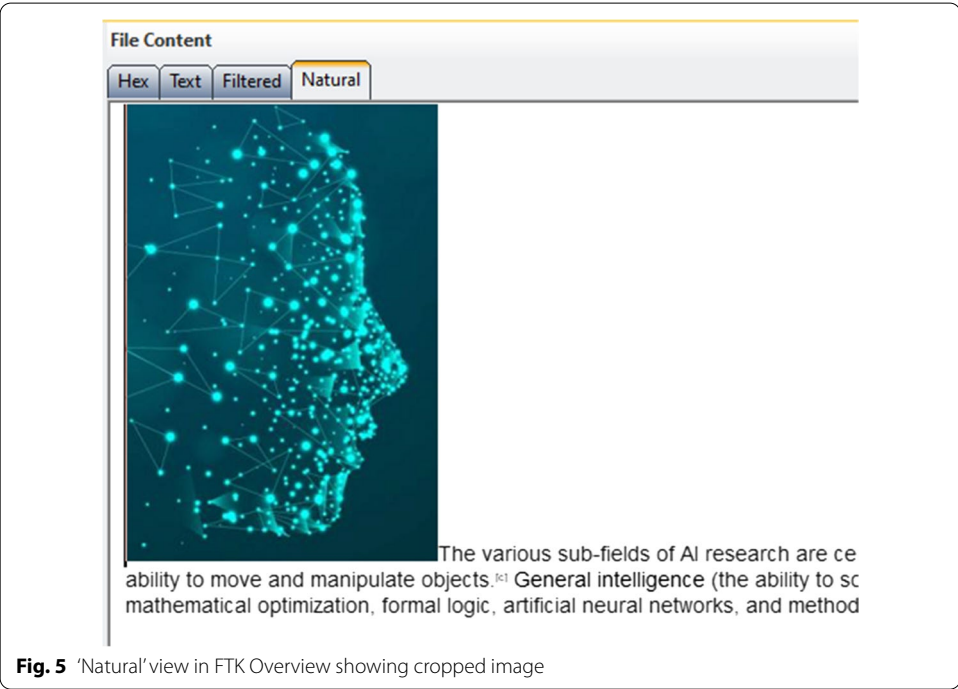


Fig. 5 'Natural' view in FTK Overview showing cropped image

requiring the investigator to be on the lookout for cropped images and as such was not intuitive. Any investigator not experienced in examining files for this could easily miss it.

Similarly, when the 'Cropped Images' file is reviewed in Autopsy, the full, uncropped image is seen (as in the Graphics tab in FTK). Additionally, the window displays information about the image such as its hash value, make and model of camera the image was taken on if it is a photograph (and the information is available).

In Fig. 7 we can see the metadata of the 'Cropped Images' file showing information such as the Author, Creator (obfuscated for anonymity purposes), word count, revision count, last modified date etc. This is all useful information in a forensic

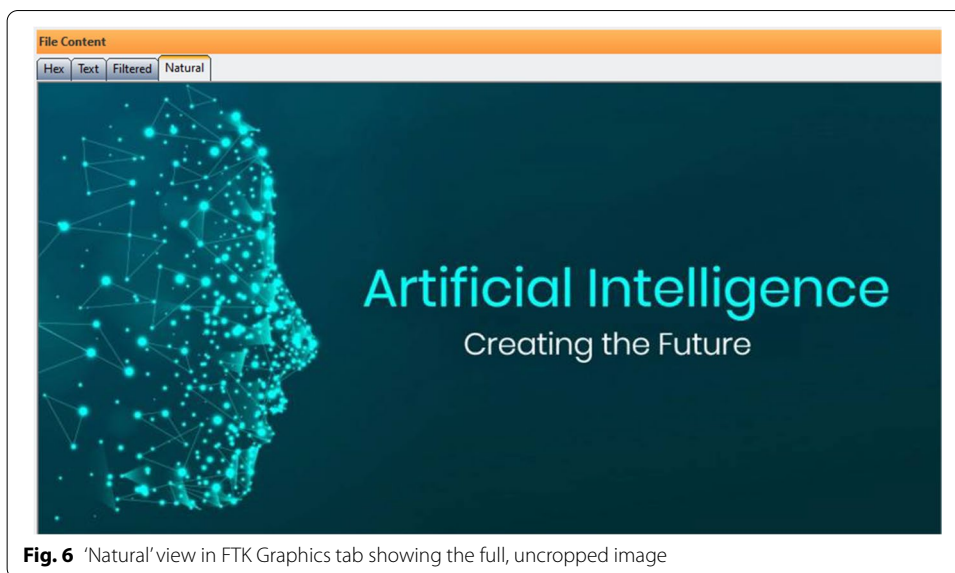


Fig. 6 'Natural' view in FTK Graphics tab showing the full, uncropped image

```
-----METADATA-----  
  
Application-Name: Microsoft Office Word  
Application-Version: 16.0000  
Author: ██████████  
Character Count: 701  
Character-Count-With-Spaces: 822  
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document  
Creation-Date: 2021-10-18T13:48:00Z  
Last-Author: ██████████  
Last-Modified: 2021-10-18T14:00:00Z  
Last-Save-Date: 2021-10-18T14:00:00Z  
Line-Count: 5  
Page-Count: 1  
Paragraph-Count: 1  
Revision-Number: 3  
Template: Normal.dotm  
Total-Time: 4  
Word-Count: 122  
X-Parsed-By: org.apache.tika.parser.DefaultParser  
cp:revision: 3  
creator: ██████████  
custom:ClassificationContentMarkingHeaderFontProps: #000000,10,Calibri  
custom:ClassificationContentMarkingHeaderShapeIds: 1,2,3  
custom:ClassificationContentMarkingHeaderText: PUBLIC / CYHOEDDUS  
custom:ContentTypeId: 0x01010035D31F019552FA469876B0CCCC8F8204
```

Fig. 7 Metadata from Cropped Image when examined in FTK

examination that would also be valuable in an academic misconduct case: for example, a long document with a very low editing time or revision count would be unusual, as would a creation date ahead of the assignment release date, and an author that doesn't match the student's detail would be worth checking. Some of this data is already being extracted by text matching software such as Turnitin.

The 'Random white space' file contains text with white x's inserted between words in order to confuse plagiarism software, as it will not match the original source. To

the reader the text looks normal, but when all the text is selected and made black in colour it is clear to see the x's between the words. For example, this is how a sentence may appear in print or online:

The cat sat on the mat

But when the whole sentence is selected and the font reset to black it would appear like this:

Thecatxsatxonxthexmat

When the 'Random white space' file is reviewed in both software packages, they do reveal the hidden white font as shown in Fig. 8. However, this is only apparent on manual inspection of the file and the examiner is not specifically alerted that white text is present. Indeed, unless you were looking for it, it would be difficult to spot.

In summary, whilst the software does identify the anomalies in these files it is not intuitive and would require a very good understanding of what to look for in order to spot the flags of academic misconduct.

Developing a bespoke digital forensics tool for academic integrity

The authors of this paper are developing a software tool to automate some of these digital forensics techniques to help in the detection of academic misconduct. Firstly, the file is extracted back to its XML component parts and the underlying data is analysed to pull out information that could be useful in determining whether the file bears the hallmarks of authentic, original work, or whether it has flags for misconduct, displaying this information in a user friendly format within a web browser. Extracting this information into an easy to read format makes it considerably simpler for the assessor to make a decision on whether the submission needs further investigation. Once extracted, standard metadata such as author, creator, number of revisions and so on are extracted and displayed in a table format, something now also done by Turnitin and other text matching software. However, extending beyond this, the tool summarises further information, such as whether the file contains cropped images, providing a thumbnail of the uncropped image for comparison purposes, whether there is white coloured font within the text, the number of font changes (which can be indicative of the need for formatting and reformatting), and image URLs (i.e. where they were originally obtained). It also lists the number of revision identifiers or rsid values, which can indicate how many edits the author has carried out. A visual representation of the edits is displayed on a web browser – multiple edits across a document shows a normal pattern of editing, whereas blocks of text with very little editing would be very difficult to create without copying and pasting the information from elsewhere (the Internet for example, or from an outsourced or contracted document).

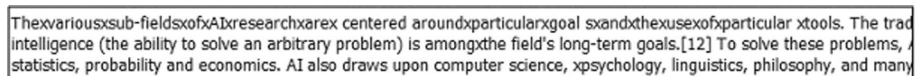


Fig. 8 Both FTK and Autopsy show the hidden white x's as unformatted type in the visual output

A small number of edits in a long document can indicate that the contents have been copied from elsewhere with very few changes, whilst authentic work is usually littered with edits as the author builds and modifies the work over a period of time.

In addition, values such as the total editing time are extracted and flagged if outside of a baseline value – for example if the total editing time is very small (perhaps just a few minutes) this indicates that the student has spent very little time in this particular document. This could be because they copied and pasted all their final work into a single document just before submitting, but it could also be because they have not carried out much editing within the work (which would be unusual). A date created time that precedes the assignment release is also flagged and the author / creator highlighted for comparison with the submitting author's information.

The files created for the experiments in FTK and Autopsy were analysed using the authors' digital forensics tool, starting with 'Cropped Images'. The tool initially displays a PDF of the finished document, which is useful for reference during the analysis. Currently, the PDF must be created manually, but it is hoped that this element can be automated in the future. Fig. 9 shows how 'Cropped Images' appears in the web browser.

In the Results section, a table lists the number of text runs (blocks of text) and edit runs (rsidR values) as shown in Fig. 10. In this case, there are a large number of each of these, despite there being only a relatively small amount of text. This is, in fact, because the text is copied from a Wikipedia page, which contained a considerable number of external hyperlinks that had to be edited out of the text once copied into Word. These values alone are flags for the assessor that the document appears to contain more runs of text than the words on the page would seem to suggest. The authors' research suggests that in a document of this size (containing a little over 100 words in total) it is unusual to see this number of text and edit runs unless extensive reformatting has been required.

Furthermore, the visual representation of the text is also highly useful. This takes the rsidR value and converts it to a colour coded map that overlays the text. Many colours suggests many different editing sessions over time, whereas very few colours indicate little or no time spent between edits. In the case of 'Cropped Images', Fig. 11 shows that whilst edits have been carried out, they have all been done in one editing session – i.e. very little time has elapsed between opening the document and editing the words.

Other elements extracted by the authors' tool into an easy to read table include total time spent editing, who created the document, when it was created along with other features and highlights where these may be worthy of further investigation.

Finally, Fig. 12 shows how the cropped image is alerted to the assessor:

Next, 'Random white space' was analysed using the tool. The visual representation of the text is particularly useful in this case, as it is very clear to see the two different editing sessions, one for the main text (shown here in blue), and a regular shaped block (shown in red) where the white coloured x's have been inserted to attempt to fool text matching software (Fig. 13):

In the Results table, there is a specific row that alerts the assessor to white text within the document, as shown in Fig. 14. In the 'Random white text' file we are told



Fig. 9 The 'Cropped Images' file displayed as a PDF in the authors' forensic tool

Item	Results
Total number of paragraph elements:	3
Total number of runs (w:r):	44
Total number of text nodes (w:t):	39

Fig. 10 Results output from the authors’ digital forensics tool



Fig. 11 Colour coding shows only one editing session

There are 1 images in this archive. Of these, 1 images have been cropped.

The original of a cropped image may contain information that is useful in detection plagiarism / collusion cases

This is the original image file (image1) without any cropping. Please compare this to the image found in the submission, checking for additional information that may be useful for establishing ownership of the image



Fig. 12 Notification by the tool that a cropped image exists within the document

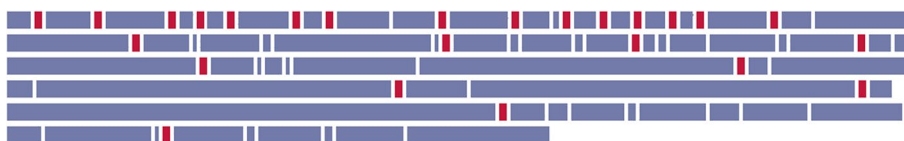
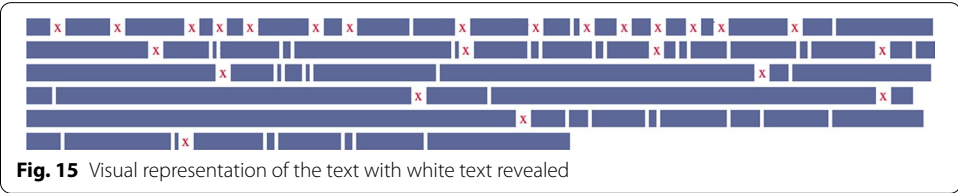


Fig. 13 Visual representation of the ‘Random white text file’

that there are 29 instances of white text, thus flagging to the assessor that the document is worth investigating further:

There is also the option to highlight in the visual representation of the text where this white text appears, and when this is selected by the assessor, the results appear as in Fig. 15, which clearly extracts the hidden x’s:

Experiments on actual student submissions that have been through an academic misconduct panel and been found as having a case to answer have been carried out using this new tool. Results to date are promising, and work is continuing to establish



benchmarks of authentic student work for comparison. Just as with text matching software, whilst this information cannot conclusively prove a case of academic misconduct, it does provide the assessor with flags to trigger further investigation and very useful evidence to support cases going to academic panel.

Discussion

There are some interesting results that come out of these experiments. The extraction of uncropped images is useful, but the existing digital forensics software does not alert the examiner to their existence. Content that may appear in the cropped areas can be useful in determining ownership of the original image (e.g. if from a website that contains surrounding text, or from a social media post or online conversation, or from another person’s desktop. Existing tools can provide timelines of activities across a number of documents, web site visits etc., but these are less useful in relation to single student submissions. The tools also provide examiners with hash values for images, which could provide irrefutable evidence that an image has been copied from elsewhere. What the existing tools do not do is provide an analysis of the xml data that the authors have presented in their tool. This ‘reverse engineering’ of documents is a very useful application of digital forensics techniques, and extracting the data into a visual ‘report’ is an important step for assessors who are unlikely to be experts in document analysis of this sort. Adding to this the possibility of including document comparison in a later development (searching for edit values that match across multiple documents) would also greatly assist in providing evidence of collusion. The proof-of-concept provided by the tool therefore presents a novel and interesting application of these techniques.

Limitations

As with all methods of detection, the results obtained from such methods are only as good as the assessor interpreting them. This is true in some extent to digital forensics tools in the main, although the role of a digital forensics examiner is solely to present the facts of the case: did ‘x’ do ‘y’ to this document or on this device; did ‘z’ access this document or device at a given time, and not to make judgements of wrong-doings. This differs to academic misconduct, where the results do need to be interpreted

much more carefully: 'x' may well have edited a document at a particular time, but as yet there are no frameworks for forensically examining a student submission that enable an examiner to present the facts in a truly objective way.

Conclusion

Digital forensics is a field which is developing very rapidly, and whilst there are clear guidelines for presenting digital evidence in courts of law, there is very little in the way of digital forensic methodologies and guidelines for the examination of files. Repurposing these tools for an alternative use is always going to be challenge as they are not being used for their originally intended purpose. For example, in a legal case exploring intellectual property rights theft, entire computer disks will be seized by law enforcers and searched for evidence. If done correctly this evidence will be admissible in court, and could lead to the prosecution (or acquittal) of the accused. In academic misconduct cases, we rarely have access to anything more than the file submitted for assessment, and we are not alerted to the fact that misconduct has occurred by the original author of the work, so building a profile of the student's actions is much more challenging. If we *did* choose to take this approach when an allegation of misconduct has arisen, we could potentially find ourselves in the position of criminalising students, something that the UK Quality Assurance Agency were keen to avoid, noting in their preparatory reports discussing legislative action against essay mills, the significant impact on time and cost to both staff and students, as seen in the MyMasters essay cheating scandal, where around 1000 students from 16 Australian Universities were found to have purchased essays from the online essay writing service (Visentin 2015).

When considering the amount of data such investigations will generate, institutions may also find themselves owners of significantly more detail than a single assignment would provide. When a file is extracted into its component parts, the result is significantly more data than the original file contains. If this data is then compared across multiple students and potentially multiple institutions, Higher Education Institutions may need to review their data retention policies, data protection and governance and whether such data gathering is ethical. It also means there is a greater risk to the student if the institution suffers a data breach.

In addition, putting an assessor in the position of detective who is trying to solve a crime is questionable, as they are neither trained to do this, nor is it appropriate to put the onus of responsibility to prove guilt upon them. In Lynch, Salamonson, Glew et al (2021), the ambivalence to 'detect and report breaches in integrity' was noted as potentially undermining the effectiveness of policy, despite participants in their study doubting that all cases of academic misconduct were being detected. Indeed, their research comments on the challenges for staff forced to take on 'surveillance roles'. In terms of utilising any sort of digital forensics software it is worth restating that these are tools used for criminal investigations and examiners are highly specialised in what to search for, and it is unlikely that an academic assessor will be proficient in their use, nor should they be. Reviewing past submissions across multiple students and courses could also be considered heavy handed and potentially unethical in terms of students' personal privacy rights.

On the other hand, methods for establishing evidence with minimal effort from the assessor would be highly beneficial. As Dawson et al. (2020) note, ‘specialist software can provide reports that assist in evidence gathering for contract cheating allegations’, thus supporting assessors in investigating hunches of misconduct by both reducing the time it takes to analyse student work, as well as providing objective evidence that misconduct has occurred. Consideration could be given to adding these digital forensics tools to the Institution’s learning management system, allowing students to review their results prior to submission, as can be done with other text-matching tools as a learning opportunity that could lead to prevention of misconduct. It should be recognised that there will inevitably be a continuation of cat-and-mouse tactics as methods of detecting misconduct will be matched with increasing efforts by students and essay mills to overcome these methods.

Every institution, of course, wants to ensure that academic integrity is upheld throughout every students’ studies, and that qualifications earned are based on the student’s own work and not that of someone else. If we can repurpose some of the digital forensics methods discussed above into an easy to use tool that could integrate into existing text-matching software, thus providing additional markers or flags for assessors to alert them to unusually presented student work, then perhaps there is a place for exploring these methods further, and whilst all academic misconduct detection methods will require manual review, any tool which reduces the impact on the assessor could potentially be highly beneficial.

Authors’ contributions

All authors have contributed to this article in some way. All have read and approved the final manuscript.

Funding

No funding was received for this research.

Availability of data and materials

There are no accompanying data sets for this article.

Declarations

Ethics approval and consent to participate

The authors confirm that accepted principles of ethical and professional conduct have been followed, and that all research has been carried out with appropriate ethical approval from the authors’ institution.

Competing interests

There are no competing interests.

Received: 4 November 2021 Accepted: 15 March 2022

Published online: 24 May 2022

References

- Almogbil A, Alghofaili A, Deane C, Leschke T, Almogbil A, Alghofaili A (2020) Digital Forensic Analysis of Fitbit Wearable Technology: An Investigator’s Guide. In: 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp 44–49. <https://doi.org/10.1109/CSCloud-EdgeCom49738.2020.00017>
- BBC (2021) Greece killing: Husband confesses to Caroline Crouch death. BBC News Available at: https://www.bbc.co.uk/news/world-europe-57523469?svrsn=5f31c081_2, Accessed 30 Oct 2021
- Bertram Gallant T, Picciotto M, Bozinovic G, Tour E (2019) Plagiarism or not? investigation of Turnitin®-detected similarity hits in biology laboratory reports. *Biochem Mol Biol Educ* 47:370–379 Available at: <https://iubmb.onlinelibrary.wiley.com/doi/full/10.1002/bmb.21236?af=R>, Accessed 28 Oct 2021
- Chutel P, Sakhare A (2014) Reverse image search engine using compact composite descriptor. *Int J Adv Res Comput Sci Manage Studies* 2(1):564–570 Available at: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1047.302&rep=rep1&type=pdf>
- Dawson P, Sutherland-Smith W, Ricksen M (2020) ‘Can software improve marker accuracy at detecting contract cheating? A pilot study of the Turnitin authorship investigate alpha’, *Assessment and evaluation in higher education*, pp. 1–10, doi: <https://doi.org/10.1080/02602938.2019.1662884>, Accessed 25 Feb 2022

- Didriksen E (2014) Forensic Analysis of OOXML Documents. Master's Thesis, Gjøvik University College Available at: <https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/198656/EDidriksen.pdf?sequence=1>, Accessed 07 June 2021
- European Network for Academic Integrity, (2021), 'Glossary', Available at: <https://www.academicintegrity.eu/wp/glossary/>, Accessed 28 Sept 2021
- Foltýnek T, Meuschke N, Gipp B (2019) Academic plagiarism detection: a systematic literature review. *ACM Comput Surv* 52(6):112 (January 2020), 42 pages. Available at: <https://dl.acm.org/doi/abs/10.1145/3345317>, Accessed Jan 2020
- Freeman L, Llorente RV (2021) Finding the Signal in the Noise. *J Int Crim Justice* 19(1):163 Available from [LexisNexis.com](https://www.lexisnexis.com), Accessed 28 Oct 2021
- Fu Z, Sun X, Liu Y, Li B (2011) Forensic investigation of OOXML format documents. *Digit Investig* 8(1):44–55 <https://doi.org/10.1016/j.diin.2011.04.001>, Accessed 19 Oct 2021
- Jeong D, Lee S (2017) Study on the tracking revision history of MS word files for forensic investigation. *Digit Investig* 23:3–10 <https://doi.org/10.1016/j.diin.2017.08.003>, Available at: <https://www.sciencedirect.com/science/article/abs/pii/S1742287617301354>, Accessed 29 Sept 2021
- Johnson, C. & Davies, R., (2020a), 'Using digital forensic techniques to identify contract cheating: a case study', *J Acad Ethics*, 18, 2, 105-113. <https://doi.org/https://doi.org/10.1007/s10805-019-09358-w>
- Johnson C, Davies R (2020b) Plagiarism from a digital forensics perspective. In: Khan ZR, Hill C, Foltýnek T (eds) *Integrity in education for future happiness*. Mendel University in Brno, Brno, p 78 Available at: <https://academicintegrity.eu/conference/proceedings/2020/johnson.pdf>
- Kimber I (2018) Broadening the Scope of QA: The Role of Quality Assurance in Ensuring Academic Integrity. In: 13th European Quality Assurance Forum, Vienna, EQAF Available at: <https://eua.eu/component/attachments/attachments.html?task=attachment&id=1757>, Accessed 01 July 2021
- Klopper R (2009) The Case for Cyber Forensic Linguistics. *Alternation* 16(1):261–294 available at <http://alternation.ukzn.ac.za/Files/docs/16.1/15%20Klopper%20F.pdf>
- Lynch J, Salamonsky Y, Glew P et al (2021) I'm not an investigator and I'm not a police officer - a faculty's view on academic integrity in an undergraduate nursing degree. *Int J Educ Integrity* 17:19 Available at: <https://doi.org/10.1007/s40979-021-00086-6>
- Microsoft, n.d., 'Check your document for similarity to online sources', Microsoft Support, Available at: <https://support.microsoft.com/en-us/office/check-your-document-for-similarity-to-online-sources-6d942360-b5ca-445f-a84d-6e8c66fc40d2>, Accessed 28 Oct 2021
- NIST (2021) Digital Forensics. Computer Security Research Centre available at: https://csrc.nist.gov/glossary/term/digital_forensics, Accessed 28 Sept 2021
- Quality Assurance Agency (2021) QAA and Jisc join forces to advise HEIs how to counter cyber security threat. *QAA News* Available at: <https://www.qaa.ac.uk/news-events/news/qaa-and-jisc-join-forces-to-advise-heis-how-to-counter-cyber-security-threat>, Accessed 27 Oct 2021
- Rogerson AM (2017) Detecting contract cheating in essay and report submissions: process, patterns, clues and conversations. *Int J Educ Integr* 13(1) Available at: <https://edintegrity.biomedcentral.com/articles/10.1007/s40979-017-0021-6>, Accessed 21 May 2021
- UK Government (2021) Essay mills to be banned under plans to reform post-16 education. Department for Education Available at <https://www.gov.uk/government/news/essay-mills-to-be-banned-under-plans-to-reform-post-16-education>, Accessed 25 Feb 2022
- United States Department of Justice (2018) Former Apple Employee Indicted On Theft Of Trade Secrets, Department of Justice. US Attorney's Office, Northern District of California Available at <https://www.justice.gov/usao-ndca/pr/former-apple-employee-indicted-theft-trade-secrets>, Accessed 26 Oct 2021
- Visentin L (2015) Sydney University to Crack Down on Cheating Following MyMaster Investigation. *Sydney Morning Herald* online Available at <http://www.smh.com.au/nsw/sydney-university-to-crack-down-on-cheating-following-mymaster-investigation-20150413-1mju3q.html>, Accessed 23 Feb 2022
- Weber-Wulff D (2019) Plagiarism detectors are a crutch, and a problem. *Nature* 567:435 Available at: <https://www.nature.com/articles/d41586-019-00893-5>, Accessed 28 Oct 2021
- Whitcomb, C., M., (2002), 'An historical perspective of digital evidence: a forensic Scientist's view', *Int J Digit Evid*, 1(1), Available at: <https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf>, Accessed 17 Feb 2022

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Ready to submit your research? Choose BMC and benefit from:

- fast, convenient online submission
- thorough peer review by experienced researchers in your field
- rapid publication on acceptance
- support for research data, including large and complex data types
- gold Open Access which fosters wider collaboration and increased citations
- maximum visibility for your research: over 100M website views per year

At BMC, research is always in progress.

Learn more biomedcentral.com/submissions

