# Miscarriages of Justice and Errors of Impunity: Ramifications of Poor Digital Evidence Management

**Article** · December 2016

CITATIONS
0

READS
9

**2 authors**, including:

Shakirat Aderonke Salihu
University of Ilorin
**7** PUBLICATIONS **9** CITATIONS

SEE PROFILE

Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 7 No. 4, December, 2016 - www.cisdijournal.net

# Miscarriages of Justice and Errors of Impunity: Ramifications for Poor Digital Evidence Management

**Balogun, A.M.**
Department of Information & Communication Technology,
Vaal University of Technology
Vanderbijlpark, South Africa
dayhorz@yandex.com

**Salihu, S.A.**
Department of Computer Science
University of Ilorin
Ilorin, Nigeria

## ABSTRACT

Evidence is always the most important factor for proving or refuting, and ultimately resolving a criminal or civil plaint inside or outside the court. Evidence, therefore need not only be genuine, but also demonstrate their worthiness and assure all involved parties about the investigation finesse. A number of guidelines for handling digital evidences have been established by bodies of experts. A deviation from any of such procedures, which may give rise to an existence of a cause to deem an evidence as shabby, will ruin a case. The consequent dismissal of an otherwise true evidence always affect the outcome of the ruling, which are often undesirable. This paper has set out to examine evidence dynamics and the roles of digital evidence mishandling in miscarriages of justice and errors of impunity. Various evidence management procedures are analysed to reveal their fortes and limitations. The review of legal precedents is undertaken and viewpoints are given to demonstrate the consequential impacts of evidence mishandling. The potential effects of such induced miscarriages of justice are projected. Recommendations are made to minimizing miscarriages of justice, which are becoming conspicuously rampant.

**Keywords-** Digital Evidence; Evidence Handling; Chain of Custody; Expert Witness; Miscarriage of Justice; Error of Impunity.

**CISDI Journal Reference Format**
Balogun, A.M. & Salihu, S.A. (2016): Miscarriages of Justice and Errors of Impunity: Ramifications for Poor Digital Evidence Management. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 7 No 4. Pp 9-16.
Available online at www.cisdijournal.net

## 1. INTRODUCTION

Electronic evidences are digitally-processed information, and as such are usually time-conscious, vague, latent and volatile. These make digital evidence very delicate and more difficult to possess or analyse, without tampering and altering the evidential information contained therein (Sheetz, 2007). The tendency of an evidence to be changed, obscured or obliterated by some human or non-human influence, regardless of intent, between the time of collection and presentation is dominant. This constitutes the investigative and legal challenge of evidence dynamics (Chisum & Turvey, 2000; Solon & Harper, 2004).

As the ultimate objective of a forensic investigation is to find and establish facts that will assist the authority to conduct a fair trial, it is consequently paramount to ensure the evidence will be a very reliable one (Anastasi, 2003). Other than being reliable, a digital evidence needs to be complete in the sense that it must adequately describe the whole incident. It must be authentic by being wholly an element of the said incident. Most importantly, it must be believable and understandable, as well as being admissible to the deciding authority (Hopkins, 2006). However, a legal precedence of a United States' court in 2002 ruled that the threat posed on digital devices by evidence dynamics is not sufficient to distrust a digital evidence (Johnson, 2006). The fact that the defendant party will attempt to exploit any uncertainty in the evidence production also requires that the reliability and admissibility of the evidence being tendered should be proved. The necessity for the onus placed on an evidence has brought various number of approved approaches to the way evidences are managed (Casey, 2009). These approaches are embedded into case management protocols employed by the investigation team. Case management protocol contains a pre-planned draft of the entire steps, processes and procedures to be carried out during the investigation of a digital crime case, which are then strictly adhered or applied to specialised cases (Marshall, 2008). It serves to guide the steps of the examiners, as well as to demonstrate the reliability of the evidence to the parties and authority involved.

Miscarriage of justice is generally understood to describe a situation where the most appropriate ruling has not been passed. However, miscarriage of justice - *mutatis mutandis* - is described as "a failure of a court or judicial system to attain the desired end of justice" (Walker & McCartney, 2008). They went on to describe it as "one that results in the conviction of an innocent person". Jenkins (2012) was able to describe miscarriage of justice, both as a researcher and a first-hand victim, as the wrongful conviction of persons for offences not committed by them. A much more recurrent issue is the error of impunity, which depicts a situation where an offender either gets minutely punished or escapes being punished at all. It is imperative to know that both situations, having been, will continue to be undesirable effects of the inadmissibility of evidence resulting from the poor manner with which they were handled during investigation (Casey, 2009).

This paper has painstakingly examined the relationship between evidence mishandling and miscarriage of justice and error of impunity. This will help to find out the extent to which the former is a causative agent of the latter, and how avoidable evidence dynamics problems are. In the course of doing this, various evidence handling procedures, recommended by authoritative forensic bodies, are discussed with respect to possible admissibility threats at each stage. The successes and drawbacks of such procedures are highlighted. A number of real life precedents are discussed for practical demonstration of the "evidence mishandling-miscarriage of justice" relationship. Eventually, the effects of the resultant miscarriage of justice on the community at large are discussed. While possible solutions to check the incidence are recommended.

The rest of this paper is organized as follows: The need for undertaking this work is explained in the next subsection. Section 2 provides brief overview of evidence dynamics. The popular evidence management methodologies are described in section 3. Section 4 features the relatable legal precedents. Lastly, section 5 presents the conclusions and future recommendations.

**1.1 Rationale**

The value of man's liberty is such inestimable, that the exercising of state powers to restrict it must be absolutely justified. The restriction of a person's freedom for unjustified reasons is considered gravely unfair and unwanted. However, the total exclusion of mistakes from rulings is practicably impossible in a legal system that relies 'heavily' on expert witnesses and forensic evidences during investigations and trials (Walker & McCartney, 2008). The relative obliviousness and /or indifference of the public to such incidents and mistakes is also unhelpful to deciding people's liberty.

Although new legislations have forced the information of the public about potential risks, there has been little or no way the public could help (Ponemon Institute, 2009). Expert witnesses introduce evidences to assist the trying of incidents in the fairest ways possible. Fortunately, the legal systems acknowledge a number of principles that guide them in admitting reliable digital evidences. Nonetheless, the true evidences that have failed to meet the principles are useless and aid exercising the inappropriate ruling. Forensic investigators may not be an issue, especially the experienced ones, as far as ensuring the reliability of digital evidences is concerned (Mandia et al, 2003).

The big concern arises in situations where the concerned organization tasks its corporate security personnels or outsources forensic investigators to gather evidences for their case. It is usual for some normal operational activities to have had some altering interactions with potential evidences, thereby hardening the possibility of getting the right ruling over the incident (American Bar Association, 2008). That has justified the need for the non-existent 'forensic readiness' in targetable organizations (Mouhtaropoulos et al, 2011).

In addition to that, employees lack the awareness of the importance of maintaining the integrity of items of evidential value. In cases where such requirements are ingrained into the organization's policies, the employees usually have no idea what they are about (Hewling, 2012). This paper is thereby aimed at organizations for the enlightenment of both their general and information technology employees about the importance, as well as procedures to ensure that potential evidences are not rendered inadmissible. Thereby helping to reduce the undesirable occurrences of miscarriage of justice and error of impunity.

## 2. EVIDENCE DYNAMICS

As mentioned earlier in the introduction section of this paper, evidence dynamics refer to all activities that exert alterable influence on the evidentiary data items being considered. Such activities may be carried out voluntarily or involuntarily, and knowingly or unknowingly of their alterable abilities . The wide range within which a digital evidence can exist makes the possible influences on them the more comprehensive in scope. All physical evidences – traditional and electronic – are subject to dynamic influences, but the unrepeatability and irreproducibility of electronic evidences make them more complex to possess (Volonino et al, 2007). Digital evidences usually span all devices capable of either or both storing and processing data. Peripheral devices are definitely not left out as evidences, since they can have weights on establishing whether or not a process that requires them was performed. Although evidences can be influenced any time from when the incident occurred, Chisum & Turvey (2008) used the occurrence timing to classify possible dynamic influences into two. Each class on the either side of the incident becoming known to the relevant authority, which would usually go on to manage the incident case.

### 2.1 Pre-Discovery Dynamic Influences

These are the influential activities that are performed right between the moment the incident occurs and the moment the investigation team takes over. A significant number of dynamic influences in this category are either voluntarily and unknowingly launched or involuntarily and unknowingly launched. Interestingly, this category also accommodates the voluntarily and knowingly launched activities known as anti-forensics (Sheetz, 2007; Forte & Power, 2007). An activity is voluntarily performed when the process is explicitly called by the user, while it is involuntary when the process was not explicitly called by the user. An activity is knowingly performed when the user has the idea of how the action will affect data structures, while an unknowingly performed activity is carried out by a user who doesn't know what effects his action will have on data structures (Casey, 2004).

Pre-discovery dynamic influences are the most indiscernible influences due to the fact that investigators assume the intactness of the incident's scene. They tend to discard the chances that the evidences might have been tampered with before their arrival at the scene. When this happens, any subsequent conclusions drawn from the examination of such evidences are thus wrong. Should an authoritative decision be made based of such inaccurate evidence and conclusion, a miscarriage of justice or error of impunity will most likely be committed.

Activities of the offenders, victims, witnesses, other persons, and natural elements may institute a dynamic influence on the digital evidence. The offender may employ anti-forensic techniques to distort the nature of evidence left behind. The victim may have performed some actions before the incident that may co-incidentally give the evidence a different outlook. The victim may also have distorted the evidence in a bid to avoid the embarrassment that may be attached to the publicity of the incident. This is especially common with commercial outfits that dread losing their customers. Witnesses and other neutral persons may also contribute dynamic influences to the evidence in some ways unknown to them, usually by interacting with the evidential device. An inexperienced system administrator may employ deleting the system and port access logs as a short fix for a suspicious hacking attempt. A first responder may influence evidence by pressing the keyboard to bring a computer out of its sleep state. The exposure of an evidence-contained device to natural elements, such as water and fire will have serious damaging effects on the evidence.

Dynamic influences at the pre-discovery stage cause the most evidence-handling issues. This is due to the fact that their control is beyond the investigation team, who often miss them, and the victims and first responders are usually not prepared nor trained to preserve the integrity of evidences (Mouhtaropoulos et al, 2011).

### 2.2 Post-Discovery Dynamic Influences

Influential activities in this category are those ones that are performed between the moment the investigation team takes over and the moment the evidence production is presented to the ruling authority. In essence, post-discovery dynamic influences are inflicted by a member of the investigation team either knowingly or unknowingly. The chances of such dynamic influences occurring depends on the expertise and experience levels of the investigation personnel (Stephenson, 2002). This classification of dynamic influences have readily established procedures to avert them. They are anticipated by the investigators and as such, can be properly managed to not affect the integrity of the evidence. Evidence dynamics at this stage attract the most attention since either party of an incident hearing and the deciding authority tend to be focussed on the evidence's lifecycle during investigation alone, or at least, more that outside investigation (Mouhtaropoulos et al, 2011).

An instance of this dynamic influence is an accidental write operation on the target hard disk, when the wrong directory has been specified by the evidence collection personnel. Improper storage of the evidence may expose it to unauthorised and unauthenticated access, thereby casting doubts on its reliability. Confusing identification and labelling can give rise to uncertainties. Post-discovery dynamic influences often span the seize and search, collection, identification, examination, analysis, documentation, reporting and presentation phases of investigation.

## 3. EVIDENCE MANAGEMENT PROCEDURES

Casey, in 2002, described a digital forensic case management as the planning of the totality of steps, processes and procedures to be carried out during the investigation of a computer misuse incident. The ubiquitous nature of evidences makes investigators anticipate them at the incident scene. In such anticipation, the plans to handle the evidences are also included in the case management procedures. Evidence management procedures address the challenges of poor handling of digital evidences (Mandia et al, 2003).

The case management plan encompasses the preservation, acquisition, examination, analysis, documentation, reporting and presentation of the digital evidences involved (Casey, 2002). E-discovery cases, especially those involving corporate organizations, usually involve several terabytes of data across multiple digital devices. Coupled with the tight deadlines imposed by courts and the high costs that are incurable with delays and mistakes, efficiency and organization is given the premium concern.

An effective case management guarantees that, through well designed protocols that help to increase examiner's efficiency and manage expectations of all parties involved in the case (Pollitt & Shenoi, 2010; Volonino et al, 2007). The protocols are drafted to describe the intentions of the investigation team (attorneys, organizations and expert witness) about handling the evidential items. Issues that protocols usually address include "what media should be searched for specific file types, what tools can be used during collection, whether deleted data should be recovered by default, and what keywords and date ranges should be used to filter the data" (Casey, 2010).

All of the procedures employed by the investigation team centres around the admissibility of the evidence, which is as important a goal as the existence of the evidence itself. The Association of Chief Police Officers in the United Kingdom (ACPO) employed its aggregation of expertise and experience to produce and continually revise an all-in case management guide – *Good Practice Guide for Computer-Based Electronic Evidence*. It contains guideline procedures from the possession of authority to search for evidence to the presentation of evidence, as a witness, to the ruling authority. The ACPO's guide contains virtually all an investigation team needs to ensure the reliability and admissibility of case evidences. (Sheetz, 2006).

Mandia et al (2003) stated that it is the norm for evidence-handling procedures to be attacked by the defence during case hearings, in the bid to discredit the prosecution's evidence and win the case. A failure to prove that the evidence has been handled in the best possible ways can have a devastating effect on the prosecution's case, they further stated. Chisum & Turvey (2008) buttressed this and also attached consequential reputation damage for the investigation team and an undesirable outcome on the ruling to inadequate evidence-handling or inability to prove efficient evidence-handling.

The reliability of an evidence can be proved majorly through an explicit and dedicated custody chain. The demonstration of the efficiency of tools and techniques used to process the evidence can be done through Daubert's principles. The integrity of the evidence is majorly proved through the comparison of the original evidence at collection and at production stages (ACPO, 2008). The following sections will relate legal precedents, discuss the deficient evidence-handling procedures involved and examine possible handling procedures that could have averted the resultant miscarriage of justice.

## 4. CASE REVIEWS

As evident in the 1978 United *States v. Kilgus* as well as the 2008 *Victor Stanley Inc. v. Creative Pipe Inc.* proceedings, scientific evidence including digital evidence is admissible only if the principle/methodology upon which it is based is "sufficiently established to have gained general acceptance in the field to which it belongs". It is also a legal consensus that attorneys treat anything new and lacking in previous case law with suspicion. Hence, it is more effective to have a precedence to corroborate the evidence production principle, even when it is a peer-reviewed and generally accepted principle. A number of digital evidence management precedents are thus, analysed for existential miscarriages of justice in the following sections. Their potential contributions to similar cases in the future and now are also discussed.

### 4.1 Qualcomm Inc. v. Broadcom Corp

Broadcom had just released a chip which featured the H.264 video compression standard, when Qualcomm accused and sued them for flouting their '104 and '767 patents in 2005. Qualcomm continuously refuted Broadcom's subsequent assertion that they were not aware of any disclosure of such patents, especially to the Joint Video Team (JVT) that sets video standards. As a result, Broadcom sort clarification by issuing a series of discovery requests ultimately that all documents that suggests any disclosure of the said and related patent, as well as any form of their engagement in the proceedings of the ISO, JVT, ITU-T and/or IEC. Qualcomm responded to the discovery request and subsequent deposition request from Broadcom by asserting that non-privileged and responsive documents relevant to the request that results from a reasonable search would be provided. On the trial day, Qualcomm's attorneys provided a signed *expert declaration* that no documents suggested Qualcomm's engagement in any of JVT' s proceedings. However, a cross examination of Qualcomm's witness revealed that she received 21 emails from JVT. Qualcomm's patents were thus rendered invalid, and Broadcom was adjudged to not have flouted any patent by the jury (Qualcomm Inc. v. Broadcom Corp, 2007).

The engagement of Qualcomm with JVT remained unproven during the course of the trial, even though it might have made a case for the patent rights' claim. It was obvious that the result of their e-discovery process was false and misleading, whether intentionally or not. It was then reported that the Qualcomm attorneys found an email welcoming the cross-examined witness to an *avc_ce mailing list*, which instigated and revealed 21 emails from an *avc_ce* keyword search on her computer. These emails were then deleted on an account of the witness that the emails were irrelevant and none of her colleagues had been involved in any standard-setting proceeding (Qualcomm Inc. v. Broadcom Corp., 2007). This could be seen as a naïve decision, and is an evidence-transforming action that can only be characterised with an untrained first responder. The e-discovery process was supposed to attempt to recover emails that might have been deleted in other to produce an accurate evidence instead. This would require expertise and experience beyond that of most attorneys even though they take on e-discovery tasks within their cases when they have no understanding of required technical aspects like evidence location, evidence format and metadata analysis, among others (United States v. O'Keefe, 2008).
More revelations were made after the trial, when Qualcomm's new attorneys performed basic keyword search on the emails of five witnesses using obvious terms related to the case. The keyword searches returned 200,000 pages of relevant information in 46,000 documents (Qualcomm Inc. v. Broadcom Corp., 2007). This omission was even more astonishing considering the amount and the simplicity and relevancy of the search terms. Further corroborating the assertion that the e-discovery task should be performed by a qualified expert witness, and should follow reasonable and justifiable search methodologies (Victor Stanley Inc. v. Creative Pipe Inc., 2008).

Luoma & Luoma (2009) suggested that a meet-and-confer between the two parties prior to the trial over the details of what was required of the e-discovery would have given a different direction to the case, and guarded the Qualcomm attorneys against their ethical misconduct. They argued that the case might have gone otherwise for Broadcom had the falsified evidence been admitted, thus indicating that all concerned parties must be proactive in the e-discovery process to prevent inaccurate and incomplete evidence production.

An important principle in e-discovery and digital forensics encourages practitioners to know the limitations of their knowledge, and escalate or consult with more qualified and experienced practitioners when found in an uncertain situation (Hewling, 2012). This principle was unknown and disregarded by the Qualcomm attorneys, and expectedly resulted in the whole e-discovery process going wrong. The mismanagement of the electronic discovery process, resulting from the attorneys' incompetence, assumption and disregard for e-discovery principles has caused Qualcomm the suit, even if it actually possessed the patent rights and was not involved in any standards team's proceedings. Similarly, the admittance of the resultant evidence from the mismanaged e-discovery process could have unfairly tipped the case out of Broadcom's favour. The court's sanction against the Qualcomm attorneys for failing to produce the accurate e-discovery results either due to collusion with their client, ignorant acceptance of unsubstantiated client assurance of sufficient search, or disregardful discharge of e-discovery expert witness task that requires specialized training and qualification would ensure thorough conduction of consultative, proactive and accurate e-discovery in future cases.

**4.2 Laura Zubulake v. UBS Warburg LLC**

UBS Warburg LLC et al. had just fired a senior salesperson – Laura Zubulake – when she accused and sued them for gender bias and wrongful appointment termination in 2003. She had been passed over for a promotion and then filed a gender discrimination charge with the EEOC when harassed by the promoted colleague, leading to her dismissal. Zubulake's attorneys requested that UBS produce all documents that indicate correspondence by the firm's employees concerning Zubulake. The defendants produced documents which had about 100 pages of email, but they were further requested to produce correspondence from all sources since Zubulake's attorneys already had possession of about 450 pages of email. UBS then claimed that other documents are archived on backup media and as such are not accessible. They requested that the court shift the cost of production to Zubulake as the request would amount to an undue expense. The court then shifted a quarter of the $166,000 estimated to restore and search the backup tapes for correspondence to Zubulake, pending the reviewal of the eventual evidence produced. However, it was discovered that some backup tapes were actually missing and some relevant emails had not been saved though the firm already had a retention policy in place. The cost shifted to Zubulake initially was then deemed unwarranted, followed by the judge providing the jury with an adverse inference instruction. More e-discovery was requested by the court at this stage which resulted to indications of deliberate email deletions by UBS managers and personnels, as well as the suppression of relevant emails that were on UBS's active servers from production. Zubulake eventually received payments in excess of $29.3 million for damages (Kroll Ontrack; Zubulake v. UBS Warburg, 2004).

The fact that the existence of gender bias against Zubulake remained unproven even after the trial, makes it unfortunate if there was actually no form of gender discrimination discussed or discharged (Maynes & Downing, 2009). However, that did not matter as the e-discovery results had consistently shown wilful tampering with the evidence on one hand. On another hand, the e-discovery process had been poorly impacted by UBS's inadequate retention policy and disregard for proper preservation when the deemed it unnecessary to place all relevant documents on litigation hold in anticipation since Zubulake's EEOC filing . In another vein, the defendant counsel failed to manage the entire e-discovery process properly (Douglas & Ballintine, 2006). It was their duty to take charge and bring in experts in a domain where they are obviously unskilled. Conveying with the firm's IT officers in an attempt to identify what was relevant and specify how and what should be produced would have prevented the shoddy e-discovery that persuaded the jury to rule against UBS and attract sanctions themselves.

Hence, a proper electronic discover-ready system should be put in place to ensure retention and preservation of electronically stored information relevant to anticipated litigations. Employees should be sensitized about the dangers of tampering with organization's systems and IT personnel should be trained to respond properly to employees' system actions. This is particularly highlighted with a confirmed hacking attempt on Aston Investments due to the presence of a keylogger spyware with IP addresses traced to OJSC, only for OJSC to eventually win the suit because Aston's IT had tampered with the evidence in the bid to deter any other hack attempt (Deaeslr, 2008). Another similar case advocating for competent e-discovery/forensic practitioners is highlighted by Benedict's plead twist and reduced sentence, after the investigator had tampered with evidence when he copied files from the abettor's device and installed forensic software on the suspect's device (McCullagh, 2002).
The Zubulake case played a major role in the 2006 revision of the Federal Rules of Civil Procedure, which sets out definite expectations for parties involved in any e-discovery process (Luoma & Luoma, 2009).

**4.3 American Express Inc. v. Vee Vinhnee**

A bankruptcy order had been brought against Vinhnee by American Express for amassing $21,000 in outstanding bills over a expired tenure. AMEX sought to produce an electronic evidence to support their claim, and tendered a record of the billing from their backup tapes. The court requested a demonstration of the authenticity of the record, as stated in the Federal Rule of Evidence. AMEX was requested to either demonstrate that the record from their backup tape was created at or near the time the activity occurred, that the record was created and has been properly maintained since creation, or that the method or procedure employed by the system in preparing the record in not in any way flawed. However, the evidence was tossed out of the proceedings because AMEX presented an unqualified expert witness, and was unable to prove their assertion that their systems were designed to ensure accuracy and identify errors during retention and retrieval of information (United States Bankruptcy Court, 2005; Gardner, 2009). It remained unproved that whether Vinhnee actually owed AMEX or not. In which case AMEX would have been hard done by, should Vinhnee had actually owed the reported amount. Thus, constituting a miscarriage of justice resulting from poor e-evidence management by the AMEX party.

The expert witness that presented the evidence did not convincingly prove the accuracy of AMEX's systems or procedures in ensuring a reliable record. He failed to answer questions regarding the policies and procedures for program and database usage or the controls to the access, changes, implementation of the database while ensuring continuous integrity (Gardner, 2009). He simply could not demonstrate a valid chain of custody for the evidence presented. The expert witness was also deemed to not be adequately qualified enough, having just claimed to be familiar with the hardware, software and computer record-keeping systems in the payment card industry, with no related training, experience or job title indicating his competence in the domain.

The attempt by AMEX to put forward an in-house IT employee to produce and present their evidence – a task he was not trained or experienced in – led to the mismanagement of the e-discovery, and thus a justice miscarriage that caused AMEX more than the $21,000 set out to recover. This need to always hire a qualified e-discovery/forensic practitioner is also highlighted in Cochranes's acquittal from theft, after the bank's expert witness was found to be unable to demonstrate that their mainframe computer had accurately identified and logged Cochrane's withdrawal at a cashpoint (R v. Cochrane, 1993).

## 5. CONCLUSION

Miscarriage of justice and error of impunity have been ever-present banes that stakeholders in the larger organizational and legal environments have become well acquainted with. However, the average citizens still remain oblivious until someone they know or themselves get entangled. The last two decades has seen the employment of digital evidence as a valuable necessity, with mistakes and lessons shaping their use in newer cases. Studies have shown that these unfortunate incidences have negative impacts on the society, including the freedom granted to guilty criminals that somehow compromises the people's trust in the justice system, increases their fear for insecurity, and brings disillusionment about life. One of the many significant contributing factors to this incidence is the poor management of the electronic evidence discovery process. This paper has given proper insights into the dynamics of electronic evidence that could invalidate the results of a discovery/investigation process, which could in turn impact the facts available to rule on a case. Case management procedures for e-discovery practitioners and attorneys that ensure an efficient admissible evidence production have been highlighted. A few legal cases with elements of miscarriage of justice or error of impunity were also analysed to identify what went wrong and what could have been done to prevent the errors. The importance of employing only qualified e-discovery practitioners, training employees about incident response, and adopting proven case management and evidence handling procedures in ensuring pristine electronic evidence production has also been demonstrated in the course of this work in a bid to reduce miscarriage of justice and error of impunity in future cases.

**REFERENCES**


1. Anastasi, J. (2003). The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property. Hoboken, New Jersey: John Wiley & Sons Inc.
2. Berg, E. (2000). Legal Ramifications of Digital Imaging in Law Enforcement. City of Tacoma Police Department, Tacoma, Washington.
3. Chisum, J. & Turvey, B. (2000). Evidence Dynamics: Locard's Exchange Principle & Crime Reconstruction, *Journal of Behavioral Profiling*, Vol. 1, No. 1.
4. Chisum, J. & Turvey, B. (2008). An Introduction to Crime Reconstruction. In Turvey B. (2008). Criminal Profiling: An Introduction to Behavioral Evidence Analysis. Chap 6. Pp. 155. 3rd Ed., Boston: Elsevier Academic Press.
5. Deaeslr, (2008). Aston Investments v OJSC Russian Aluminum. http://www.deaeslr.org/2008.html [Online].
6. Douglas, B. & Ballintine, D. (2006). Electronic Discovery: Lessons from Zubulake. Larkin Hoffman Daly & Lindgren Ltd. http://www.larkinhoffman.com/files/OTHER/bjd_ppp_elecdis.pdf [Online].
7. Forte, D. & Power, R. (2007). A tour through the realm of anti-forensics, Computer Fraud & Security, Vol. 2007, Issue 6, June 2007, pp. 18-20.
8. Gardner, O. (2009). The Lack of Evidentiary Foundations Fosters Fraud. www.creditslips.org/creditslips/2009/08/the-lack-of-evidentiary-foundations-fosters-fraud.html [Online].
9. Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, Digital investigation, Vol. 3, Supplement 1, pp. 44-49, The Proceedings of the 6th Annual Digital Forensic Research Workshop (DFRWS '06).
10. Hewling, M. & Sant, P. (2012). Digital Forensics: An Integrated approach, Proceedings from 6th Cybercrime Forensics Education and Training, Canterbury Christchurch University, Canterbury, UK.
11. Hopkins, B. (2006). Evidence: Key Fact. 2nd Edition. London: Hodder Education.
12. Jenkins, S. (2012). Methodological challenges of conducting insider reflexive research with the miscarriages of justice community. International Journal of Social Research Methodology DOI: 10.1080/13645579.2012.709777.
13. Kroll Ontrack, Zubulake v. UBS Warburg. https://www.krollontrack.co.uk/zubulake/ [Online].
14. Mandia, K., Prosise, C., and Pepe, M. (2003) Incident response and computer forensics(2nd ed.) McGraw Hill, California.
15. McCullagh, D. (2002). Electronic evidence anchors porn case. https://www.gpo.gov/fdsys/pkg/USCOURTS-akd-1_14-cr-00001/pdf/USCOURTS-akd-1_14-cr-00001-0.pdf [Online].
16. Mouhtaropoulos, A., Grobler, M., and Chang-Tsun L. (2011) Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives. European Intelligence and Security Informatics Conference,Athens.
17. Pollitt, M. and Shenoi, S. (2010). Advances in Digital Forensics. Springer. ISBN13: 9781441940124.
18. Ponemon Institute LLC, (2009). 2009 Annual Study: UK Enterprise Encryption Trends.
19. Qualcomm Inc v Broadcom Corp, Order at 41 (S. D. California 6, August 2007).
20. R v Cochrane, [1993] Criminal Law Report 48, CA.
21. Solon, M. and Harper, P. (2004). Preparing evidence for court. Digital Investigation Vol1 Iss 4, Pp. 279-283.
22. Stephenson, P. (2002). Collecting Evidence of a Computer Crime. Computer Fraud & Security, Vol 2002 Iss 11, Pp. 17-19.
23. United States Bankruptcy Court, (2005). Am. Express Travel Related Servs. Co. v. Vinhnee (In re Vinhnee). caeb.uscourts.gov/documents/Judges/Opinions/Published/vinhnee-04-1284.pdf?dt=13424612 [Online].
24. United States v O'Keefe, 537 F. Supp. 2D at 22 (D.D.C February 18, 2008).
25. Victor Stanley, Inc v. Creative Pipe, Inc., 250 FRD 251 (D.Md 2008).
26. Volonino, L., Anzaldua, R., and Godwin, J. (2007). Computer Forensics: Principles and Practices. Upper Saddle River, New Jersey: Pearson Education Inc.
27. Walker, C. and McCartney, C. (2008). Criminal Justice and Miscarriages of Justice in England and Wales. Chapter 10 in C. Ronald Huff & Martin Killias (2008) Wrongful Conviction: International Perspectives on Miscarriages of Justice. Philadelphia. Temple University Press.
28. Zubulake v. UBS Warburg, WL 1620866 (S.D.N.Y. July 20, 2004).