Chapter 13
Forensic Readiness for Enhanced eDiscovery

Dauda Sule
https://orcid.org/0000-0002-8795-4717
Air Force Institute of Technology, Nigeria

ABSTRACT

To discover, uncover, and stamp out digital crime while ensuring information security and assurance, there is a need to investigate the crime once it has occurred. This will help trace the criminals and also secure an organization against future attacks. Forensic readiness entails organizations being at alert as per digital evidence collection and storage – that is collecting and storing such evidence constantly in a forensically sound manner, not just when the need for such evidence arises. In the event litigation arises or is anticipated, digital evidence may need to be reviewed by the opposing parties prior to court proceedings to assess quality of the evidence; this is eDiscovery. Digital evidence for eDiscovery needs to be forensically sound and provided in an efficient timely manner – forensic readiness helps to ensure this. This chapter is an update on the chapter on "Forensic Readiness and eDiscovery" in the previous edition and still seeks to establish how forensic readiness is relevant to the eDiscovery process, taking into consideration current developments in the field.

INTRODUCTION

Most of our lives have virtually become completely intertwined with digital devices and information systems: virtually everything we do today is done through or in conjunction with a digital device or platform. This is the digital age, issues pertaining to information security and assurance abound; and with increased technological advancements, criminals are also improving on their skills and causing more and more havoc. Additionally there is also the use of digital systems for political and military purposes in such a way as to manipulate the way things happen in a jurisdiction the way the perpetrator wants; like the issue of the 2016 US Presidential elections allegedly being tampered with by a foreign country by way of influencing public opinion using information systems (CNN Library, 2019). Digital forensic investigations are used to ensure information assurance and security by discovering how an

DOI: 10.4018/978-1-7998-5728-0.ch013

incident connected to an electronic device occurred and possibly tracing and apprehending those behind it. Knowledge of how such an incident occurred can also help an organization strengthen its defenses since it reveals where there are lapses in an organization's information security infrastructure. Forensic readiness requires an organization to be constantly on alert as regards gathering, storing and analyzing digital data in a forensically sound manner – such data has the potential of serving as digital evidence in the event of an incident or litigation, without waiting for such an incident or litigation to occur. The digital evidence will come in handy in the event the need for it arises and will be readily available to be used by an organization to trace how an incident could have taken place; defend itself or indict a party. Forensic readiness can further serve to show regulatory compliance and best practices on the part of an organization. Forensic readiness can guarantee faster and more efficient investigations with minimal disruption to normal business operations, and it also enhances cost-effectiveness in terms of evidence gathering. Electronic evidence is constantly gathered and stored until a need for it arises as a result of an incident, regulatory or legal requirement whereby it would serve as evidence in incident response or be used as backup for disaster recovery and continuity – it is just like saving for a rainy day. Therefore in the event of an incident that requires investigation or a legal/regulatory requirement for the production of digital evidence, the evidence only has to be presented being that it was already collected and stored in a forensically sound manner. This helps make evidence presentation and investigation much faster and allows for business continuity with minimal disruption to normal operations, which would have arisen if investigators had to gather the evidence after-the-fact. It also helps ensure reduce the risk of the evidence being eroded or lost due to normal operations of an organization before the evidence source is isolated (if that is possible) or an attacker covering his/her tracks when an attack is carried out since evidence is collected before, during and after such an act – collecting evidence after the breach could afford an attacker time to wipe out his tracks before evidence gathering and investigations begin.

eDiscovery on the other hand comes up in the event of litigation or its anticipation, where opposing parties are required to review the others' digital evidence to assess its quality prior to full court proceedings. eDiscovery may also be viewed as the sum total of the processes involved in a digital investigation including evidence gathering and analysis. eDiscovery works by the reduction of data volume that requires review from a large repository into a manageable and easily reviewable form by extracting only that which is relevant to the case at hand. This is apparent in the electronic discovery reference model (EDRM) which has a yellow triangle with the tip to the right, implying funneling of large amounts data beginning from the right resulting in the minimal quantity the process ends up with.

eDiscovery can be a very delicate issue, its rules and guidelines have to be safeguarded by the litigating parties. The digital evidence has to be forensically sound, timely, relevant, and in the format required by the requesting party or the court; failure to meet up with the rules and guidelines can result in severe consequences for any party that falls short. The case of *AMD vs. Intel (2005)* is a classic one, Intel failed to provide digital evidence as requested by AMD in good time, which resulted in heavy costs to Intel at the end of the day.

Whether digital evidence is required for review prior to court proceedings or regulatory requirements or for digital investigations, the evidence has to be collected and presented in a timely and efficient manner which is legally acceptable (forensically sound). In order to achieve this, it would be best to collect and store such evidence constantly, not only when the need for it arises – that is forensic readiness. Forensic readiness ensures constant collection of digital evidence in a forensically sound manner making the eDiscovery process much easier and efficient. Forensic readiness goes a long way in ensuring that an organization is adequately prepared for eDiscovery.