Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 49 (2015) 74 – 81

Procedia Computer Science

ICAC3'15

Faster File Imaging Framework for Digital Forensics

Neha Kishore[a]*, Bhanu Kapoor[b]

[a]*Department of Computer Science and Engineering, Chitkara University, Himachal Pradesh, India*
[b]*Consultant/Owner, Mimasic, Dallas, TX USA*

Abstract

The use of digital forensics tools has become common in typical crime investigations involving computing and communication devices. As with any evidence in criminal investigations, the preservation of digital evidence is of critical importance for the success of the investigation. Cryptographic Hash Functions (CHFs) are used by digital forensic tools to ensure the preservation of digital evidence during the acquisition and analysis of evidence. These tools make the use of the CHFs during the acquisition process to ensure that the created image of the evidence is accurate. The CHFs that are currently in use are serial in nature and can be time consuming when working with the large data sets. We propose a new parallel CHF transformation to speed up the image creation process by a factor of 6.5 over existing methods. We discuss the use of the parallel algorithm in the image creation process and compare the results with the existing sequential methods.

Peer-review under responsibility of organizing committee of the 4th International Conference on Advances in Computing, Communication and Control (ICAC3'15)

*Keywords:*Digital Forensics; Cryptographic Hash Functions; Cybercrime; Disk Imaging; SHA-1; Parallel Algorithms; OpenMP;

1. Introduction

With the prevalent use of information technology in our day-to-day lives, most of the information today is typically stored on computing systems of various forms. Unfortunately, the popularity and growth of information technology has also resulted in tremendous increase in cybercrimes of many different types including denial of

* Corresponding author. Tel.:+91-959-240-5665; fax: +91-01795-661013.
*E-mail address:*neha.kishore@chitkarauniversity.edu.in

Peer-review under responsibility of organizing committee of the 4th International Conference on Advances in Computing, Communication and Control (ICAC3'15)
doi:10.1016/j.procs.2015.04.229

service attacks, intellectual property thefts, child pornography, identity theft, frauds, extortions, cyber stalking, spamming, and hacking. When you have crimes, they are bound to end up in the court of law and evidences need to be presented. Cybercrimes have digital evidences, also known as e-evidences.

As a result of these advances, digital forensics has become essential in the field of forensic science for solving crimes that use some type of computer as an instrument or as target.There have been changes in the criminal laws to take the advances in technology into account. After the passage of Computer and Fraud Abuse Act of 1984, computer hacking became a crime and further led to the advances in research and development in the field of digital forensics[1]. Since then, Federal Bureau of Investigation (FBI) and other law enforcement agencies are developing programs to examine evidence present in digital form. Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science[2] as a discipline including the need for a standardized approach to examinations.

There are many commercial and open source digital forensics tools[3]that are available today and are used by computer forensic examiners and analysts to perform their investigations. The digital data or the digital evidence needs to be acquired and analysed from the source in this process. As a result, the process of disk imaging is an important task in the field of digital forensics. Every digital investigation of a crime begins with disk imaging and CHFs[4] are used to ensure the accuracy of the imaging process. A hash signature is created for the data that uniquely represents the original data. In forensics, the hash signature is normally used during acquisition of the evidence, during verification of the forensic image, and again at the end of the examination to ensure the integrity of the data and forensic processing. The amount of data often exceeds a terabyte and can be many terabytes. Relationally, the time consumption in calculating hash code also increases as the size of code.

This issue can be solved with the parallelization of the hashing process. The advances in the processors and manufacturing technology as predicted by the Moore's Law[5] has led to increasing performance of modern hardware and is continuing with the availability of multiple cores executing in parallel. The availability of multiple cores and massively parallel GPUs enables parallelization[6] of various computing algorithms. However, the basic hashing algorithms are inherently sequential in nature and cannot take advantage of the parallel processors that we have available today. We will discuss a modified hashing transformation that is suitable for parallel processing and is applicable to a wide range of applications such as digital forensic tools. This paper discusses a parallel algorithm based upon the proposed transformation for faster image generation, its use, and importance in digital forensics.

The rest of the paper is organized as follows: Section 2 covers digital forensics. Our parallel image generation framework named IRTH is discussed in Section 3. We follow it with a comparative performance analysis of SHA-1 and RSHA-1(algorithm of IRTH) in Section 4. The last section presents the conclusions from the work as well as some directions for future work.

2. Digital Forensics

The evolution of Digital Forensics (DF)[2, 7, 8]emerged as a retort to the increase in crimes which are somehow related to the digital information involved either in planning or committing a crime. The analysis of computer systems, networks, mobile, social networking sites etc. can provide various digital evidences against the crimes like cyber harassment, pornography, planning of a murder or a robbery, theft of data and information from the computer system, hacking, website defacement etc.

The task of Computer Forensic Specialists (CFs) is to investigate the digital crime and generate a report reflecting the summary of the contents of crime sources by scrutinizing number of digital sources that are available and which are thought to be involved in the crime. In order to make the report acceptable to the court the CFs has to ensure integrity, authenticity, re-productivity, non-interference and minimization of the digital evidence for which they have to follow certain methodology.

In Digital forensics CHFs are important because they provide a means of identifying and classifying electronic evidences. Hash functions play a critical role in evidence authentication, and it is important a judge or jury can trust the hash values that uniquely identify electronic evidence.