

Analysing Forensic data by pattern recognition

Ayesha Akter

Brac University,CSE Dept

ayesha.akter2@g.bracu.ac.bd

SHIHAB SHARAR

Brac University,CSE Dept

shihab.sharar@g.bracu.ac.bd

Annajiat Alim Rasel

Brac University,Sr. Lecturer,CSE Dept

annajiat@bracu.ac.bd

September 21, 2021

Abstract

One of the most significant goals of Forensic Data Analysis is to identify criminals using suspicious pattern detection techniques from device data. Detectives often examine the evidence in search of events and information about individuals. This procedure is essentially a review task, similar to the electronic reviews outlined in the E-Discovery Reference Model for E-Discovery initiatives (EDRM). This paper presents an identity extraction, deduplication, and ranking algorithm to enable non-technical investigators prioritize evidence units in their inquiry without the assistance of a digital forensics specialist. The experiment is based on the Enron email dataset and shows how the proposed string-matching algorithms can effectively merge identities.

Keywords-suspicious pattern,detection techniques,E-Discovery Reference Model,string-matching algorithms.