Abstrak

Email Forensik: Pemetaan Artefak Digital Header Email ke dalam Konsep 4W1H

Header email merupakan artefak digital yang paling mudah didapatkan dari sebuah email. Banyak informasi penting yang terdapat pada *header email* seperti informasi pengirim dan penerima email, alamat IP pengirim, waktu email dikirim oleh pengirim dan email diterima oleh penerima. Forensik email merupakan suatu tindakan pengamanan dan penelurusan terhadap email atau bukti-bukti kejahatan yang menggunakan email. Aktivitas ini meliputi pemeriksaan dan pengungkapan informasi penting yang terdapat pada email dengan memeriksa bagian *header* dari sebuah email. Beberapa *tools* forensik email yang tersedia saat ini, belum ada yang dapat memetakan informasi dari *header email* ke dalam konsep 4W1H (*What, Who, When, Where*, dan *How*). Pemanfaatan konsep 4W1H dalam dunia forensik dapat mempermudah proses investigasi dalam pemecahan suatu kasus atau masalah yang sedang terjadi. Maka dari itu, pada penelitian ini akan dirancang sebuah *tool* yang dapat membaca *header* dari sebuah email. *Tool* ini dapat memetakan informasi dari *header email* sehingga dapat menjawab pertanyaan yang sesuai dengan konsep 4W1H. *Tool* ini diharapkan dapat melengkapi *tools* yang telah ada sebelumnya dalam membantu investigator melakukan forensik email sebab *tool* ini dapat mengekstraksi dan memetakan informasi dari *header email* dengan cepat dan mudah dibaca. Selain itu terdapat fitur deteksi *email fraud* dan *email spoofing* pada tool yang dibuat. Dari hasil pengujian yang telah dilakukan, *tool* Mail Header Extractor ini dapat memetakan informasi yang terdapat pada header email ke dalam konsep 4W1H serta dapat menunjukkan indikasi apabila dalam pengujian yang dilakukan, terdapat *header email* yang termasuk dalam *email fraud* dan *email spoofing*.

Kata kunci

Header email, forensik email, konsep 4W1H

Abstract

Email Forensics: Mapping the Digital Header Email Artifacts into the 4W1H Concept

An email header is a digital artifact that is most easily obtained from an email. Many important information contained in the e-mail header such as information about the sender and recipient of the e-mail, the IP address of the sender, when the e-mail was sent by the sender and e-mail received by the recipient. Email forensics is an act of security and investigation of e-mail or evidence of crime that uses e-mail. This activity includes checking and disclosing important information contained in the e-mail by checking the header section of an e-mail. Some email forensic tools available at this time, no one can map information from the email header into the concept of 4W1H (What, Who, When, Where, and How). Utilization of the 4W1H concept in the forensic world can simplify the investigation process in solving a case or problem that is happening. Therefore, this research will design a tool that can read the headers of an email. This tool can map information from email headers so that it can answer questions that are consistent with the concept of 4W1H. This tool is expected to be able to complement existing tools to help investigators carry out email forensics because this tool can extract and map information from email headers quickly and easily. Besides, there are features of email fraud detection and email spoofing on the tools made. From the results of tests that have been carried out, the Mail Header Extractor tool can map the information contained in the email header into the 4W1H concept and can show indications if the test carried out, there are email headers included in email fraud and email spoofing.

Keywords

Email header, email forensics, 4W1H