Read the article "Mining E-mail Content for Author Identiﬁcation Forensics" <http://nl.ijs.si/janes/wp-content/uploads/2014/09/develothers01.pdf>. Comments on key findings.

The article: Mining E-mail Content for Author Identiﬁcation Forensics tries to identify the origin of an e-mail content for forensic investigation purposes. To accomplish this goal, the researchers carefully differentiate and examine both aggregated and widespread email topics. The motive for the research lies in the dominance of email usage daily. That is, with email being the significant form of internal and external means of written communication for many organizations, the researchers assert that it can be misused for the distribution of unsolicited and inappropriate messages and documents. Hence, identifying the source of these emails becomes critical to solves cases such as sexual harassment, racial vilification, threats, bullying, and so on. Unfortunately, this is not an easy task since the sender can spoof his or her email address or masquerade as another user.

However, according to the researchers, regardless of how complex the investigation can be, e-mail forensics consists of unique characteristics. These include the identification of the email author, and analysis of the email body, header, attachments, traceroute, file stamps, and so on. Hence, in order to mine the phases of email forensics and classify a wide range of e-mails as belonging to an individual, the unique characteristics were considered when conducting the study.

After analyzing data from various sources, the researchers conclude that the information they gathered, in conjunction with e-mail document features, highlights that there are limitations in their approach to classify and identify email authors due to the small sample of author categories used in the investigation. Additionally, they couldn’t pinpoint the set of characteristics that remain relatively constant for a large number of e-mails written by the author.

That being said, to comment more on the article, I firmly believe that the number of author categories sampled in the study is not small enough in the context of forensics. However, in my opinion, a better approach to the continuously growing e-mail misuse problem is to require the employment of unique automated methods for analyzing the content of e-mail messages and identifying or categorizing the authors of these messages. In fact, most of the enterprise email content security solutions employ automated procedures to log suspicious emails and provide a clear report of the possible source of the message.