

ABSTRAK

Lonjakan kasus anomali lalu lintas siber di Indonesia, terutama kejahatan *Phishing* berbasis rekayasa social (*social engineering*) via email, mengancam kerahasiaan data sensitif para pengguna perangkat bergerak. Keterbatasan pengguna awam dalam melihat visualisasi metadata secara utuh pada antarmuka Gmail Mobile kerap dimanfaatkan oleh aktor ancaman untuk menyisipkan manipulasi tautan. Guna mengatasi masalah tersebut, penelitian ini dilaksanakan untuk mengkaji alur investigasi taktis serangan *Phishing* di platform Gmail Mobile lewat implementasi kerangka kerja forensik digital *National Institute of Standards Technology* (NIST) SP 800-86, sekaligus mengevaluasi performa platform *Cisco Threat Intelligence* (CTI) *Cisco Talos Intelligence* dalam memverifikasi indikator bahaya siber. Menggunakan metode eksperimen laboratorium terisolasi, simulasi serangan dirancang memakai Gophish dan Google SMTP Realy demi mendistribusikan tautan berbahaya aktif dari PhisTank menuju smartphone POCO M3. Pengujian *Live Forensic* ini diterapkan secara ketat mencakup empat tahapan utama NIST SP 800-86 (*Collection, Examination, Analysis, Reporting*) dengan mematuhi panduan *Safety Handling* melalui isolasi string teks mentah (*Raw String*). Temuan riset mengonfirmasi bahwa penerapan metode NIST SP 800-86 bekerja sangat optimal dalam mengekstraksi artefak bukti digital secara aman. Selain itu, verifikasi melalui *Cisco Talos Intelligence* terbukti presisi dalam memetakan reputasi siber dan klasifikasi ancaman siber, di mana kalkulasi kuantitatif pada *Threat Scoring Matrix* domain rekaya menghasilkan skor tinggi (+5) berstatus *Untrusted* dan dikategorikan sebagai *Phishing/Malicious Sites*. Secara menyeluruh, studi ini membuktikan bahwa investigasi taktis mampu menutupi celah minimnya visibilitas metadata pada Gmail Mobile, sehingga identifikasi ancaman dapat dilakukan secara dini, valid, dan aman guna meminimalkan Risiko insiden kebocoran data.

Kata kunci: Digital Forensik, *Phishing*, NIST SP 800-86, Gophish, Gmail Mobile, Cisco Talos Intelligence.

ABSTRACT

The surge in cyber traffic anomalies in Indonesia—particularly social engineering-based phishing attacks via email—threatens the sensitive data of mobile device users. Threat actors often exploit the limitations of average users in fully viewing metadata visualizations on the Gmail Mobile interface to embed manipulated links. To address this issue, this study investigates the tactical workflow of phishing attacks on the Gmail Mobile platform by implementing the National Institute of Standards and Technology (NIST) SP 800-86 digital forensics framework, while also evaluating the performance of the Cisco Talos Intelligence (CTI) platform in verifying cyber threat indicators. Using a controlled laboratory experiment, attack simulations were designed using Gophish and Google SMTP Relay to distribute active malicious links from PhishTank to a POCO M3 smartphone. This live forensic testing strictly adhered to the four main stages of NIST SP 800-86 (Collection, Examination, Analysis, and Reporting) and followed safe handling guidelines through the isolation of raw text strings. Research findings confirm that the NIST SP 800-86 method operates optimally for the secure extraction of digital evidence. Furthermore, verification via Cisco Talos Intelligence proved precise in displaying cyber reputation and threat classifications; quantitative calculations within the Threat Scoring Matrix yielded a high score (+5), resulting in an "Untrusted" status and a classification of "Phishing/Malicious Site." Overall, this study demonstrates that tactical investigation can overcome the lack of metadata visibility in Gmail Mobile, enabling early, valid, and secure threat detection to minimize the risk of data breaches.

Keywords: Digital Forensics, Phishing, NIST SP 800-86, Gophish, Gmail Mobile, Cisco Talos Intelligence.