Analisis Remote Wipe sebagai Kegiatan Anti Forensik pada Smartphone Android

Mia Amelia[1], Niken Dwi Wahyu Cahyani[2], Rahmat Yasirandi[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]miaamelia@students.telkomuniversity.ac.id, [2]nikencahyani@telkomuniversity.ac.id,
[3]batanganhitam@telkomuniversity.ac.id

Abstrak

Digital forensics adalah cabang dari ilmu forensik untuk melakukan proses identifikasi, akuisisi, analisa serta menampilkan informasi barang bukti digital yang didapat dari media digital atau perangkat digital. Digital Forensics difokuskan pada proses investigasi bukti digital oleh pihak penyidik. Disisi lain, anti-forensics adalah teknik yang digunakan untuk menghalangi pihak penyidik dalam mendapatkan barang bukti untuk melakukan proses investigasi. Teknik *anti-forensics* penting dilakukan guna mengamankan informasi sensitif yang tidak ingin diketahui pihak lain seperti, informasi personal/data diri, informasi bisnis, dll. Smartphone merupakan salah satu jenis perangkat digital yang sering digunakan untuk menyimpan informasi sensitif. Dimana di dalam smartphone tersimpan data-data pribadi berupa foto, video, email, chat, SMS, dan lain sebagainya. *Remote wipe* merupakan penerapan teknik *anti-forensics* yang biasa diterapkan pada smartphone. *Remote wipe* mampu menghapus seluruh data yang tersimpan di dalam sebuah smartphone dari jarak jauh serta mengembalikan smartphone dalam kondisi pabrikan / *factory reset*. Masalah yang terjadi ketika melakukan proses remote wipe adalah smartphone target tidak terhubung dengan jaringan Internet, sehingga proses remote wipe tidak dapat dilakukan. Penelitian ini bertujuan untuk melakukan proses Remote Wipe pada smartphone android dengan memanfaatkan jaringan Internet dan SMS sebagai media transmisi. Berdasarkan hasil pengujian, jaringan SMS dapat digunakan untuk melakukan proses Remote Wipe, sehingga bisa dijadikan alternatif lain ketika device target tidak terhubung melalui jaringan Internet.

Kata kunci : remote wipe, anti forensic, digital forensics, SMS wipe

Abstract

Digital forensics is a branch of forensic science to carry out the process of acquisition, acquisition, analysis and display of information on digital evidence obtained from digital media or digital devices. Digital forensics is focused on processing digital evidence by investigators. On the other hand, anti-forensics is a technique used to prevent investigators from obtaining evidence to carry out the filling process. Anti-forensic techniques are important for sensitive information that other parties don't want to know, such as personal information / personal data, business information, etc. Smartphones are a type of digital device that is often used to store sensitive information. Where on the smartphone is stored personal data in the form of photos, videos, e-mails, chats, SMS, and others. Remote wipe is an application of anti-forensics techniques commonly applied to smartphones. Remote wipe is able to remotely save all data stored in a smartphone and restore the smartphone to its factory condition / factory reset. The problem that occurs when performing the remote wipe process is that the target smartphone is not connected to the Internet network, so the remote wipe process cannot be done. This study aims to perform the Remote Wipe process on an android smartphone by utilizing the Internet and SMS networks as transmission media. Based on the test results, the SMS network can be used to perform the Remote Wipe process, so that it can be used as an alternative when the target device is not connected via the Internet network.

Keywords: remote wipe, anti forensic, digital forensics, SMS wipe

1. Pendahuluan

Pada bab pendahuluan ini dibagi menjadi 5 bagian yang terdiri dari latar belakang, rumusan masalah, tujuan, batasan masalah, dan organisasi tulisan.

Latar Belakang

Digital forensics adalah cabang dari ilmu forensik untuk melakukan proses identifikasi, akuisisi, analisa serta menampilkan informasi barang bukti digital yang didapat dari media digital atau perangkat digital [11]. Digital Forensics difokuskan pada proses investigasi bukti digital oleh pihak penyidik. Disisi lain, anti-forensics adalah teknik yang digunakan untuk menghalangi pihak penyidik dalam mendapatkan barang bukti untuk melakukan proses investigasi. Teknik *anti-forensics* penting dilakukan guna mengamankan informasi sensitif yang tidak ingin

diketahui pihak lain seperti, informasi personal/data diri, informasi bisnis, dll. Smartphone merupakan salah satu jenis perangkat digital yang sering digunakan untuk menyimpan informasi sensitif. Dimana di dalam smartphone tersimpan data-data pribadi berupa foto, video, email, chat, SMS, dan lain sebagainya[1]. Ketika smartphone jatuh ke tangan pihak yang tidak memiliki wewenang untuk mengakses data smarpthone, maka perlu diterapkan teknik *anti-forensics* guna mengamanankan data smartphone tersebut. Berdasarkan paper [2], teknik *anti-forensics* tahap pertama adalah *elimination source.* Tahap *elimination source* bertujuan untuk menghilangkan jejak data digital sebagai barang bukti yang digunakan pihak penyidik pada tahapan akuisisi atau data preservation. Terdapat dua metode yang digunakan pada tahap *elimination source* , yaitu melakukan modifikasi metadata (changing MAC Attributes) dan wiping. Metode modifikasi metadata memungkinkan untuk melakukan perubahan seperti *ekstensi* atau informasi *timestamp* pada setiap data, tetapi pihak penyidik masih memungkinkan untuk mengakses data. Metode *wiping* berkaitan dengan istilah *data sanitization* yaitu menghapus data dari perangkat digital dan kemungkinan proses pemulihan data tidak dapat dilakukan, sehingga data digital tidak dapat diakses oleh pihak penyidik.

Remote wipe merupakan penerapan teknik *anti-forensics* yang biasa diterapkan pada smartphone. *Remote wipe* mampu menghapus seluruh data yang tersimpan di dalam sebuah smartphone dari jarak jauh serta mengembalikan smartphone dalam kondisi pabrikan / *factory reset*. Beberapa perusahaan smartphone seperti Google, menyediakan fitur remote wipe pada smartphone android, dikenal dengan nama *Android Device Manager*[16]. Masalah yang terjadi ketika melakukan proses remote wipe menggunakan *Android Device Manager* adalah smartphone target tidak terhubung dengan jaringan Internet, sehingga proses remote wipe tidak dapat dilakukan. Selain itu perlunya dilakukan percobaan *remote wipe* untuk mengetahui efektifitas penggunaan metode *wiping* pada smartphone android, sebagai bentuk perlindungan akses data dari pihak yang tidak berwenang.

Rumusan Masalah

Berdasarkan latar belakang yang telah di uraikan, maka rumusan masalah pada tugas akhir ini adalah sebagai berikut:

1. Sejauh mana remote wipe pada smartphone android efektif diterapkan di kegiatan anti forensik?

Tujuan

Tujuan yang ingin dicapai dari tugas akhir ini adalah sebagai berikut:

1. Melakukan implementasi *remote wipe* sebagai pada smartphone android.
2. Melakukan analisis metode *remote wipe*, dengan melihat perbedaan data yang tersimpan pada *internal storage* sebelum dan sesudah dilakukan proses *wipe*.

Batasan Masalah

Batasan masalah pada tugas akhir ini adalah sebagai berikut:

1. Menggunakan Bahasa pemrograman java dalam impelementasi aplikasi remote wipe.
2. Data yang disimpan pada internal storage berupa data dokumen dan multimedia.
3. Device administrator menggunakan emulator android sebagai device untuk mengirimkan perintah wipe, sedangkan device target menggunakan device real atau asli.

Organisasi Tulisan

Laporan tugas akhir ini terbagi menjadi 5 bagian, bagian 1 berisi latar belakang tentang kegiatan *anti forensic* dan *remote wipe.* Pada bagian 2 menjelaskan studi terkait mengenai penelitian yang telah dilakukan sebelumnya serta ringkasan materi yang berkaitan dengan *remote wipe.* Pada bagian 3 menjelaskan sistem yang dibangun mencakup alur kerja sistem, spefisikasi kebutuhan penelitian, dan skenario pengujian. Kemudian pada bagian 4 dijelaskan mengenai hasil dan analisis pengujian yang didapat, serta pada bagian 5 berisi kesimpulan dan saran.