Prosiding Seminar Nasional Kahuripan I Tahun 2020
ISBN : 978-602-60606-3-1

PENGOLAHAN DATA UNTUK MENEMUKAN BUKTI PADA MOBILE FORENSIK

Muhammad Syarif Hartawan[1], Amat Damuri[2], Arman Syah Putra[3]

[1]Universitas Krisnadwipayana, syarifhartawan@gmail.com
[2]AMIK AL Muslim, amatdamuri@gmail.com
[3]STMIK Insan Pembangunan, armansp892@gmail.com

ABSTRAK

Pada penelitian ini penulis meneliti tentang Forensik digital, serta data yang dikumpulkan untuk menganalisis dan menghasilkan bukti pada *mobile forensik*, data harus dipastikan terintegrasi dan disimpan selama proses investigasi, proses ini dikenal sebagai validasi data. Metode penelitian ini dengan pengujian menggunakan black box dan pendekatan yang memvalidasi forensik seluler pada data yang disimpan di perangkat yang akan dikembangkan. Tujuan dari penelitian ini adalah mengembangkan pendekatan yang memvalidasi forensik ponsel dan data yang disimpan di perangkat. Aplikasi akan diimplementasikan secara forensik dengan menggunakan pendekatan, yang terdiri dari metode validasi yang kuat. Penelitian ini akan fokus pada transmisi data, sedangkan pengumpulan data dilakukan di perangkat, data ditransfer ke laptop untuk validasi. Kesimpulan penelitian ini bukti bisa ditemukan dari kumpulan data yang di simpan, dengan kumpulan bukti maka penelusuran data akan berhasil mencari data yang diinginkan

Kata kunci : Data, Forensik Seluler, Validasi, Bukti.

ABSTRACT

In this study the authors examined digital forensics, as well as data collected to analyze and produce evidence on mobile forensics, data must be ensured that it is integrated and stored during the investigation process, this process is known as data validation. This research method uses black box testing and an approach that validates cellular forensics on data stored on the device to be developed. The aim of this study is to develop an approach that validates mobile forensics and data stored on the device. The application will be implemented forensically using an approach, which consists of a strong validation method. This study will focus on data transmission, while data collection is carried out on the device, the data is transferred to a laptop for validation. The conclusion of this study, evidence can be found from the data set that is stored, with a collection of evidence, data tracing will be successful in finding the desired data

Keywords: *Data, Cellular Forensics, Validation, Evidence.*

PENDAHULUAN

Di era era informasi digital sekarang ini, penggunaan perangkat mobile khususnya smartphone sudah menjadi kebutuhan sehari-hari. Faktanya, sekitar tiga perempat orang Amerika (77%) sekarang memiliki smartphone. Perangkat seluler telah menjadi bagian penting dari dunia berbasis teknologi. Dalam berbagai jenis skenario, ponsel cerdas menyimpan data yang dapat digunakan sebagai bukti sebagai bagian dari penyelidikan. Untuk alasan tertentu, penegakan hukum untuk menyita dan melakukan analisis forensik pada perangkat tersebut menjadi komoditas yang sedang hangat. Perangkat forensik seluler untuk membantu penegak hukum melakukan investigasi yang melibatkan barang bukti elektronik banyak diminati dan terus berkembang karena kemunculan dan kemunculan teknologi smartphone yang pesat. Jenis media dan data seperti foto, video, pesan, dll. Yang menjadi minat yang signifikan bagi peneliti forensik digital adalah alat forensik seluler yang sangat dibutuhkan untuk membantu penegakan hukum dalam penyelidikan yang melibatkan bukti elektronik. Dengan menggunakan alat ini bersama dengan data yang dikumpulkan, integritas data harus dijaga selama proses investigasi. Data harus divalidasi agar dapat diterima, istilah hukum

Diterima:	Dipresentasikan:	Disetujui terbit:
20 Oktober 2020	24 Oktober 2020	30 Oktober 2020

untuk menentukan apakah bukti diterima, di pengadilan [11].

Artikel tersebut memeriksa dan memperoleh 24 gambar forensik, masing-masing dari ponsel FxOS internal dan memori volatil. Gambar yang diperoleh kemudian diekstraksi berdasarkan tindakan yang diambil, didokumentasikan dalam langkah-langkah terperinci, dan diberi nama yang sesuai. Gambar-gambar ini kemudian dianalisis dan hasilnya disajikan dan diserahkan. Hasil penelitian ini menunjukkan bahwa informasi forensik yang paling berharga berada di dalam memori volatile. Temuan penelitian ini juga menunjukkan bahwa memori pada ponsel FxOS tidak dienkripsi, sehingga dapat dibaca dengan perangkat forensik. Karenanya, penulis artikel berhasil memulihkan dan melacak kredensial akun media sosial, terutama di layanan Facebook dan Twitter. Sebaliknya, semua informasi yang tidak disimpan dalam gambar telepon seperti nama profil di Google+ dan nomor telepon yang digunakan selama pendaftaran untuk Telegram dan Pathways, dapat dilacak dalam gambar memori. mitranya di web seluler. Oleh karena itu, penulis artikel berhasil mendapatkan jejak dan bukti forensik yang sama persis ketika menganalisis layanan yang sama, baik di aplikasi web seluler maupun platform. Misalnya, aplikasi Facebook, Twitter dan Telegram menghasilkan jejak forensik yang sama dengan web seluler [1].

Dalam artikel ini membahas analisis forensik artefak yang tertinggal di WhatsApp dan artikel ini menunjukkan bagaimana artefak tersebut dapat memberikan banyak informasi. Artikel ini menunjukkan cara menafsirkan data yang disimpan ke dalam kontak dan obrolan database untuk menyusun kembali daftar kontak dan kronologi pesan yang telah dipertukarkan oleh pengguna. Sementara analisis dari basis data kontak memungkinkan untuk merekonstruksi daftar kontak, korelasi dengan kejadian disimpan dalam file log yang dikelola oleh WhatsApp memungkinkan vestigator untuk menyimpulkan juga ketika kontak tertentu telah ditambahkan, atau untuk memulihkan kontak yang dihapus dan waktu penghapusan. Demikian pula, menghubungkan konten database obrolan dengan informasi yang disimpan dalam file log memungkinkan penyelidik untuk menentukan pesan mana yang telah dihapus, kapan pesan ini telah dipertukarkan, dan pengguna yang menukarnya [2].

Pada penelitian ini dilakukan analisis komparatif terhadap empat perangkat forensik mobile pada lima ponsel android dengan menggunakan sistem operasi yang berbeda. Hasil evaluasi dari penelitian ini menunjukkan bahwa FTK Imager dan Paraben Seizure mobile forensic tools AccessData tools memberikan hasil yang lebih baik daripada Encase dan Mobiledit. Selain itu, FTK Imager dan Paraben Access Data dapat mengambil data yang dihapus seperti video, musik, gambar, dokumen dari memori telepon tetapi tidak memiliki akses ke kartu SIM. Oleh karena itu, kebutuhan akan alat forensik yang efektif dan efisien untuk tujuan pembuktian data dari perangkat seluler tidak dapat terlalu ditekankan [3].

Smartphone merupakan salah satu teknologi yang sedang berkembang pesat dewasa ini, dengan berbagai fungsi yang menunjang produktivitas. Fungsi utama smartphone adalah komunikasi. WhatsApp merupakan aplikasi chat open source yang dapat digunakan di setiap sistem operasi smartphone seperti Android. WhatsApp memiliki fitur pengiriman teks, gambar, video, audio, pesan dokumen. Beberapa penelitian sebelumnya melakukan eksperimen forensik seluler di WhatsApp sebagai bukti, dengan menggunakan metode berbeda. Bedanya dengan penelitian sebelumnya, penelitian ini melakukan serangan Remote Access Trojan (RAT) pada smartphone yang melakukan pertukaran informasi menggunakan aplikasi Sypnote. Spynote membangun aplikasi dengan ekstensi .apk yang mengandung malware. Serangan tersebut berhasil mengontrol perangkat smartphone sehingga dapat mengunggah database WhatsApp dari File Management smartphone. Basis data WhatsApp diperoleh, diekstraksi menggunakan WhastApp Viewer dan DB.Browser.for.SQLite untuk menghasilkan artefak digital dan mengembalikan pesan yang dihapus [4].

Berdasarkan hasil tes yang dilakukan di aplikasi dengan enkripsi crypt12, bukti belkasoft dan kunci whatsapp / DB ekstraktor telah memenuhi uji validasi pengulangan dan reproduktifitas, kunci whatsapp / ekstrctor DB mendominasi kemampuannya untuk mengekstrak pesan teks artefak, kemudian belkasoft memiliki keuntungan dari mengekstraksi video, gambar dan dokumen [5].

Bukti digital diperoleh dengan prosedur analisis forensik, penelitian telah

mampu menemukan bukti artefak berupa sesi chat untuk pesan teks whatsapp atau dalam bentuk file media lain yang dienkripsi oleh crypt12. Proses analisis bukti digital yang diperoleh dengan menggunakan bahasa pemrograman python mampu menganalisis data dari pelaku pesan untuk dicocokkan berdasarkan kesamaan dokumen pesan sebelum disaring dengan tahapan tokenisasi [6].

Kecanggihan teknologi saat ini sangat membantu manusia dalam segala hal. Salah satunya adalah penggunaan investigasi forensik digital yang dapat menunjukkan akses ke Whatsapp. Tentu kita sudah tidak asing lagi dengan aplikasi chat whatsapp dan hampir semua orang memilikinya, aplikasi ini sangat membantu kita untuk berkomunikasi dengan orang lain. Oleh karena itu, kita dapat menggunakan aplikasi ini untuk mendapatkan informasi yang dapat digunakan di dalam investigasi forensik [7].

Analisis forensik memang membutuhkan bukti berupa text message chat untuk digunakan dalam menganalisis data pelaku. Aplikasi Whatsapp dapat kita gunakan untuk melacak data aktor yang dapat dicocokkan berdasarkan dokumen sebelumnya [8].

Dalam penelitian yang dilakukan oleh artikel di atas, dilakukan analisis komparatif perangkat forensik seluler pada lima ponsel android yang menggunakan sistem operasi berbeda. Hasilnya, alat forensik mobile FTK Imager dan Paraben Seizure memiliki hasil yang lebih maksimal dibandingkan Encase dan Mobiledit. Selain itu, AccessData FTK Imager dan Paraben dapat mengambil data yang telah dihapus, misalnya Video, Gambar, musik, dan dokumen. Sedangkan Encase hanya menunjukkan bahwa perangkat terhubung dan tidak ada data yang dihapus atau diambil. Mobiledit memberikan informasi status seluler dan beberapa informasi dasar pada kartu SIM seperti IMEI, ICCID, IMSI. Sehingga jika digunakan di pengadilan, perangkat tersebut sangat berguna untuk menemukan alat bukti yang akurat, walaupun datanya telah terhapus, namun pengguna dapat mengambil data yang terhapus tersebut untuk dijadikan alat bukti. AccessData FTK Imager dan Paraben perangkat forensik seluler dapat digunakan secara efektif dan efisien [9].

Kemajuan teknologi saat ini membuat kita semakin bergantung pada perangkat seluler kita dalam kehidupan sehari-hari. Sisi negatifnya akan menyebabkan peningkatan jumlah penipuan dan aktivitas berbahaya lainnya dengan bantuan seluler. Perangkat Mobile Forensik dapat digunakan untuk kepentingan negara, seperti intelijen militer, investigasi perusahaan, pertahanan kriminal dan sipil, Alat forensik seluler dapat lebih ditingkatkan untuk mengekstrak dan menganalisis Log Panggilan, Informasi Kontak, pesan teks, dan Email yang dapat digunakan lebih efisien efektif [10].

METODE PENELITIAN

Cabang ilmu forensik dalam forensik digital harus dilihat dengan konsep umum yang konsisten dan memungkinkan peneliti forensik memiliki pedoman saat melakukan penyelidikan. Proses standar forensik digital diilustrasikan pada Gambar 1. Proses forensik terdiri dari empat tahap dasar

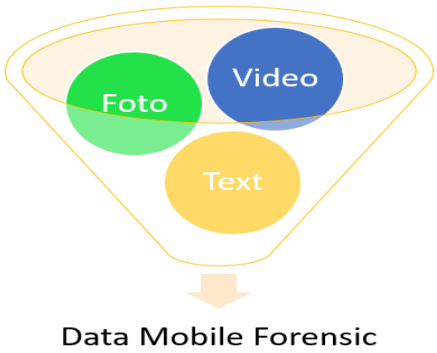
Gambar 1 Metode Penelitian

Seperti yang terlihat pada gambar 1, kita dapat melihat bagaimana cara mendapatkan data ke forensik seluler:

1. Data: Data merupakan hal terpenting dalam pencarian data di mobile forensic.
2. Eksekusi: Eksekusi data merupakan hal yang sangat diperlukan karena akan dilakukan pengecekan data apakah benar-benar dapat menjadi bukti mobile forensic.
3. Analisis: Analisis adalah pengolahan data menjadi bukti ke arah mobile forensic.
4. Mobile Forensic: bila semua data sudah pasti dan dapat menjadi bukti dalam bukti forensik mobile.

HASIL DAN PEMBAHASAN

Data yang dapat dijadikan bukti dalam mobile forensic adalah beberapa data, data tersebut adalah:

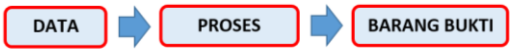


Gambar 2 Pengolahan Data

1. Video: Gambar bergerak yang bisa membuat bukti di mobile forensic.
2. Foto: Gambar yang tidak bergerak yang bisa membuat bukti di forensik mobile.
3. Text: Huruf yang di rangkai yang menjadi tulisan, yang bisa membuat bukti di mobile forensic.

Dengan ketiga cara mendapatkan data tersebut, penulis menyimpulkan:

1. Software membantu penelitian ini.
2. seberapa mudah mendapatkan data dari ponsel dan kita dapat mengolah data.
3. Metode yang mudah digunakan dan mendapatkan hasil yang maksimal.



Gambar 3 Alur Penelitian

Berdasarkan gambar diatas maka alur penelitian ini berdasarkan 3 tahapan, yaitu data, proses dan barang bukti.

a. Data
   Data yang berasal dari smartphone sebagai dasar pencarian data.
b. Proses
   Tahapan ini pencarian data yang bisa dijadikan barang bukti pemeriksaan.
c. Barang Bukti
   Barang bukti adalah data yang di temukan guna mendukung bukti hasil kejahatan dan bisa digunakan dalam hal penuntutan.

SIMPULAN

Kesimpulan yang diperoleh dalam makalah ini adalah bahwa data dengan beberapa proses yang dapat dianalisis dapat digunakan sebagai bukti dalam ilmu forensik, dengan beberapa data yang dapat digunakan sebagai proses pembuktian, dengan banyaknya data dalam pembuktian, yang akan sangat membantu kepolisian dalam melaksanakan tugas di cabang ilmu forensik keliling.

DAFTAR PUSTAKA

[1] (Wirara, Hardiawan, & Salman, 2020)[1] Mohd Najwadi Yusoff, Ali Dehghantanha, Ramlan Mahmod,*"Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as Case Studies"2018*

[2] DiSIT - Computer Science Institute, Universit_a del Piemonte Orientale, Alessandria (Italy) *"Forensic Analysis of WhatsApp Messenger on Android Smartphones"*. Cosimo Anglano. 28 july 2015

[3] J. K. Alhassan, R. T. Oguntoye, Sanjay Misra, Adewole Adewumi, Rytis Maskeliūnas, and Robertas Damaševičius on 08 January 2018.

[4] Comparative Evaluation of Mobile Forensic Tools Anang Marfianto1, Imam Riadi2 on 10 August 2018. *WhatsApp Messenger Forensic Analysis Based on Android Using Text Mining Method*

[5] Rusydi Umar, Imam Riadi, Guntur Maulana Zamroni "Mobile Forensic Tools Evaluation for Digital Crime Investigation" 2018

[6] Anang Marfianto, Imam Riadi "Whatsapp Massenger Forensic Analysis Based on Android Using Text Mining Method" 2018

[7] Bery Actoriano and Imam Riadi "*Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2*" (2018)

[8] Anang Marfianto and Imam Riadi "*WhatsApp Messenger Forensic Analysis Based on Android Using Text Mining Method*" (2018)

[9] J. K. Alhassan et al. 2018. *"Comparative Evaluation of Mobile Forensic Tools*"

[10] Shahana Shamim.2018. "*Design And Implementation Of mobensic Tool To Aid MOBILE FORENSICS"*

[11] Wirara, A., Hardiawan, B., & Salman, M. (2020). Identifikasi BuktiDigital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan "WhatsApp". *eknoin Vol. 26, No. 1, Maret2020:* , 66-74.