

# ANALISIS FORENSIK *RECOVERY* DENGAN KEAMANAN *FINGERPRINT* PADA *SMARTPHONE* ANDROID

Sahiruddin, Imam Riadi, Sunardi

Magister Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta, Indonesia  
sahiruddinbuton@gmail.com

## ABSTRACT

*Smartphone is a seluler phone that is currently growing rapidly. The position of the smartphone can be said to help the activities of its users on office work, business, e-banking, and to interact with other users in social media. Smartphone security is a top priority for users to secure data from others who are not responsible. One of the security systems that can be applied by the user is with the fingerprint code. Security is a challenge for information technology forensics and law enforcement to investigate the smartphone of someone who commits a crime as a suspect in a case. The way that can be done to penetrate the security is to attack the security system part. The purpose of this study is to develop the security of smartphones from others who access without permission. The method used in this study is the National Institute of Justice (NIJ) that is by identifying, proposing solutions, obtaining solutions, conducting trials of solutions offered, evaluating and completing procedures and reporting on results. This study is expected to provide a solution of data loss recovery.*

**Keyword:** *Forensic, Fingerprint Code, Recovery, Android.*

## 1. PENDAHULUAN

Kemajuan teknologi dan industri merupakan hasil dari budaya manusia. Kemajuan teknologi tidak hanya membawa dampak positif tetapi terdapat dampak atau efek negatif. Misalnya, kemajuan tersebut dimanfaatkan untuk memudahkan kegiatan-kegiatan yang melanggar aturan, seperti tindak kejahatan. Salah satu bentuk teknologi yang kemajuannya bisa langsung dinikmati dan diaplikasikan dalam kehidupan sehari-hari adalah telepon genggam (*smartphone*).

*Smartphone* memiliki perkembangan teknologi yang sangat pesat yang mana dahulu hanya dapat digunakan untuk berkomunikasi via suara maupun pesan singkat (*Short Message Service*). *Smartphone* kini telah berkembang dengan fitur-fitur yang disesuaikan dengan perkembangan zaman dan kebutuhan dari penggunanya. *Smartphone* dapat membantu aktifitas penggunanya baik dalam melakukan pekerjaan kantor, bisnis, *E-Banking*, maupun untuk berinteraksi dengan pengguna lain-nya di media sosial seperti *Facebook*, *Twitter*, *Path*, *Blackberry Messenger*, *Instagram*, dan lain-lain.

Dibalik perkembangan *smartphone* juga membawa dampak negatif terhadap perkembangan dan peradaban. Dampak negatif yang dimaksud adalah berkaitan dengan dunia kejahatan. Faktor keamanan *smartphone* merupakan perhatian utama para penggunanya, untuk menjaga data pribadi dari resiko pencurian data terhadap *smartphone* tersebut.

Saat ini pencurian data pada *smartphone* menjadi hal yang banyak diperbincangkan oleh banyak orang, hal ini disebabkan karena sistem keamanan yang diterapkan pada layar *smartphone* tersebut dianggap belum maksimal. Untuk pencegahan dari pihak yang tidak bertanggung jawab, para pembuat *smartphone* merilis versi terbaru dengan menerapkan kode keamanan *fingerprint* yang hanya mengenali sidik jari pemilik yang ditempelkan pada *smartphone* tersebut.

Keamanan menjadi tantangan bagi Information Tecnology forensik dan penegak hukum untuk melakukan penyelidikan terhadap *smartphone* dari seseorang yang dijadikan tersangka dalam sebuah kasus kejahatan. Banyak cara untuk menghilangkan kode akses

keamanan layar pada *smartphone*, salah satu cara yaitu dengan melakukan *factory data reset* atau mengembalikan *smartphone* ke kondisi awal dari pabrik. Akan tetapi, cara yang dilakukan ini dapat menghapus semua data-data yang tersimpan di memory internal *smartphone*. Pada suatu penyidikan, data didalam *smartphone* yang dijadikan barang bukti digital tidak boleh hilang satu pun selama proses penyidikan dilakukan.

Penelitian ini diharapkan bisa memberikan gambaran umum bagaimana teknik-teknik yang bisa dilakukan untuk mengembalikan data yang hilang akibat dari dilakukannya *factory data reset*. Penelitian ini sejenis dengan penelitian yang dilakukan oleh Okta Riandi, Zaniel Mazalisa dan Helda Yudiastuti pada tahun 2015 dengan judul Analisis Forensik Recovery dengan Keamanan Kode Pola Pada *Smartphone* Android untuk mengembalikan data yang hilang pada *smartphone* setelah dilakukan *factory data reset*, tetapi pada penelitian tersebut menggunakan keamanan dengan kode pola sedangkan penelitian ini menggunakan sistem keamanan fingerprint.

## 2. KAJIAN PUSTAKA

### Kajian Penelitian Terdahulu

Kajian penelitian terdahulu dapat dilihat pada gambar 1.

No	Nama Peneliti	Judul	penelitian	keterangan
1.	Roni Anggara Putra, Abdul Fadlil, Imam Riadi (2017)	Analisis Forensik <i>Recovery</i> pada <i>Smartwatch</i>	Melakukan Uji Coba serta analisa forensik menggunakan <i>tool Mobile edit forensic &amp; tool</i> yang ada pada kalilinux metasploit	Program studi Teknik informatika Univ. Ahmad Dahlan Yogyakarta. JURTI. Vol.1 No.1. ISSN 25798790

2.	Okta Riandy, Zaniel Mazalisa, Helda Yudiastuti (2015)	Analisis forensik <i>recovery</i> dengan keamanan kode pola	Penelitian ini menggunakan <i>recovery mode</i> dan menggunakan <i>Android Debug Bridge</i>	Teknik Informatika (SC-SITI), Palembang 21-22 Agustus 2015
3.	Syukur Iksani dan Bekti Cahyo Hidayanto (2016)	Analisis forensik WhatsApp dan Line Messenger pada <i>smartphone</i> android	Bukti digital pada aplikasi whatsapp dan Line Messenger berhasil didapatkan dari perangkat android dengan cara manual dan aplikasi tambahan dengan kondisi aktifitas perubahan aplikasi perangkat yang digunakan	Institut Teknologi Sepuluh Nopember (ITS) jurusan Sistem Informasi. Fakultas Teknologi Informasi Surabaya JURNAL TEKNIK ITS Vol. 5 No.2 (2016)
4.	Riky Ramadhana, A Haidar Mirza, Ilman Zuhri Yadi	Analisis forensik untuk aplikasi blackberry Messenger dan Blackberry	<i>Software</i> EBBE data yang didapat pada <i>Blackberry</i> berupa PIN dan Kontak sedangkan Android tidak ada	Universitas Bina Darma Jl. Ahmad Yani No. 3 Palembang.

			data. Data manual yang didapat hanya percakapan manual baik android ataupun blackberry	
5.	Anggie Khristian, Yesi Novaria Kunang, Siti Sa'uda	Analisis forensik whatsapp artefak pada Platform Android	Clock Word Mod (CWM) merupakan metode recovery yang sangat membantu dalam pengambilan data pada partisi sistem android tanpa melakukan rooting pada smartphone	Universitas Bina Darma jl. Ahmad Yani No. 3 Palembang
6.	Rahmat Novienda, Yesi Novaria Kunang, P.H. Shaksono (2014)	Analisis Malware pada Platform Android	Penelitian ini dilakukan dengan mengambil 3 sampel aplikasi android yang mengandung malware	Universitas Bina Darma jl. Ahmad Yani No. 3 Palembang Konferensi Nasional Ilmu Komputer

				(KONIK) 2014 ISSN :2338-2899
--	--	--	--	------------------------------

Gambar 2. Kajian penelitian terdahulu

### 3. METODOLOGI PENELITIAN

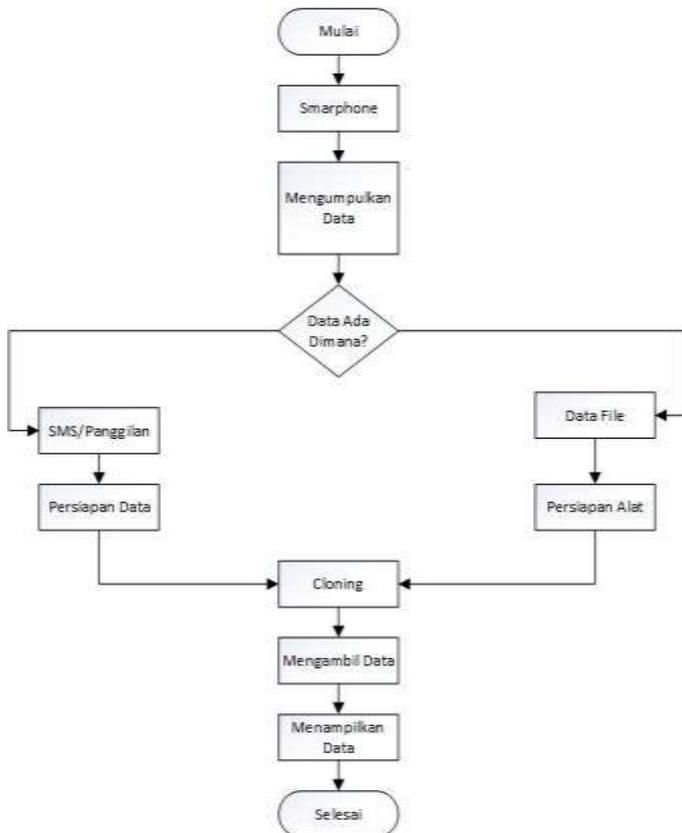
Metode penelitian yang digunakan berdasarkan pedoman forensik perangkat mobile yang dibuat oleh *National Institute of Justice (NIJ)* dengan langkah-langkah sebagai berikut :

1. *Identifying the task or problem*  
Peneliti mengidentifikasi masalah dan mengumpulkan informasi tentang masalah yang akan dihadapi.
2. *Proposing Possible Solutions*  
peneliti Mengajukan solusi yang mungkin untuk dilakukan dalam pemecahan masalah dari hasil identifikasi masalah dan informasi dari hasil tahap pertama.
3. *Testing each solution on an identical test device and under known control conditions*  
Setelah mendapatkan solusi yang mungkin dilakukan dari tahap kedua, peneliti kemudian melakukan uji coba terhadap *smartphone* dari setiap solusi yang mungkin dilakukan untuk pemecahan masalah.
4. *Evaluating the result of test*  
Melakukan evaluasi dari hasil yang di dapat dari hasil uji coba yang dilakukan dari setiap solusi agar di lakukan untuk pemecahan masalah
5. *Finalizing the procedure*  
Menyelesaikan prosedur dari setiap langkah yang telah di lakukan pada tahapan sebelumnya dan melaporkan hasil yang di dapat dari pemecahan masalah dalam penelitian ini.

Subjek penelitian ini adalah *smartphone* android Xiaomi Redmi 3S, dengan objek penelitian yaitu analisis forensik *recovery* dengan keamanan *fingerprint* dimana hal yang akan dilakukan yaitu mengembalikan data yang hilang pada *smartphone* akibat dilakukannya *factory data reset*. Adapun alat dan bahan yang dibutuhkan dalam penelitian ini adalah sebagai berikut :

1. Laptop Asus X454Y
2. Aplikasi *Recuva*
3. USB konektor
4. *Oxygen Forensic*
5. *Handphone* Xiaomi Redmi 3S

Perancangan sistem yang akan dilakukan dapat dilihat pada gambar 2



Gambar 2. Perancangan sistem

Penjelasan gambar 2 adalah sebagai berikut :

1. Menyediakan bahan  
Pada tahap ini adalah penyediaan bahan berupa sebuah *smartphone* Xiaomi Redmi 3S yang dijadikan sebagai subjek penelitian
2. Mengumpulkan data  
Pengumpulan data dimaksudkan untuk mengumpulkan informasi-informasi tentang *smartphone* tersebut dan mengumpulkan informasi data yang akan diforensik.
3. Mencari informasi data  
Pada tahap ini adalah pencarian bentuk data sms/panggilan, atau data file lain yang tersimpan pada *smartphone*.
4. Melakukan persiapan alat

Setelah proses pencarian selesai dan ditentukan bentuk file yang akan dikembalikan selanjutnya mempersiapkan alat dan bahan serta teknik yang bisa dilakukan untuk mengembalikan data. Hal ini dimaksudkan untuk memudahkan kegiatan pengembalian data dengan cepat dan efisien.

5. Melakukan cloning  
Tahap selanjutnya yaitu melakukan cloning terhadap data yang sudah berhasil dikembalikan.
6. Mengambil data  
Pada tahap ini yaitu pengambilan data hasil dari kegiatan cloning
7. Menampilkan data untuk dilaporkan  
Pada tahap akhir yaitu data yang sudah diambil dari hasil cloning selanjutnya dilaporkan sebagai hasil temuan dalam penelitian ini.

#### 4. HASIL PENELITIAN

Hasil yang diharapkan dari penelitian ini adalah sebagai berikut :

1. Mengetahui teknik-teknik yang bisa dilakukan untuk mengembalikan data yang hilang pada *smartphone*
2. mengetahui cara data bisa dikembalikan dengan menggunakan *tool* yang ada setelah dilakukan *factory* data reset pada *smartphone*.
3. Mengetahui tingkat keberhasilan dari setiap teknik yang dilakukan

#### DAFTAR PUSTAKA

- Okta Riandy. (2015). Analisis forensik recovery dengan keamanan kode pola. Student Colloquium Informasi & Teknik Informatika (SC-SITI). Palembang.
- Roni Anggara Putra. (2016). Analisis Forensik Recovery pada Smartwatch. JURTI. Vol.1 No.1. ISSN 25798790. Yogyakarta
- Syukur Iksani. (2016). Analisis Forensik Whatshap dan Line Messenger Pada Smartphone Android. JURNAL TEKNIK ITS Vol. 5 No.2
- Riky Ramadhan, A Haidar Mirza , Ilman Zuhri Yadi. Analisis forensik untuk aplikasi blackberry Messenger dan Blackberry. Universitas Bina Darma.

- Anggie Khristian, Yesi Novaria Kunang, Siti Sa'uda. Analisis forensik whattApp artefak pada Platform Android. Universitas Bina Darma.
- Rahmat Novianda, Yesi Novaria Kunang, P.H. Shaksono. (2014). Analisis Malware pada Platform Android. Konferensi Nasional Ilmu Komputer (KONIK) ISSN :2338-2899. Palembang
- Raharjo. (2013). "Sekilas Mengenai Forensik Digital". *Jurnal*. Bandung: Fakultas Teknik Elektro Dan Informatika. Institut Teknologi Bandung, Jawa Barat.
- Carvey, Harlan. (2005). "Windows Forensics And Incident Recovery," Addison Wesley.
- Ferdiana, Ridi, St, Mt. (2008). "Membangun Aplikasi Smartclient Pada Platform Windows Mobile" . Jakarta: Pt Elex Media Komputindo.
- Gary B, Thomas J Dan Misty E. 2007. *Discovering Computers: Fundamentals*, 3thed. Terjemahan. Salemba Infotek. Jakarta.
- Williams, B. K., Sawyer, C. (2011) *Using Information Technology: A Practicional Introduction To Computers & Communications (9th Ed.)*. New York: Mcgrawhill
- Casey, (2011) "terdapat empat tahapan dalam pembuktian bukti digital"  
<https://www.google.co.id/search?q=hasil+voters+iPhone+5s&source>