FORENSIK MOBILE PADA SMARTWATCH BERBASIS ANDROID

Roni Anggara Putra*[1], Abdul Fadlil[2], Imam Riadi[3]
[1]Magister Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
[3]Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta
e-mail: *[1]ronianggara79@gmail.com, [2] fadlil@mti.uad.ac.id , [3] imam.riadi@is.uad.ac.id

Abstrak

Perkembangan teknologi pada saat ini berkembang sangat pesat. Salah satu contoh berkembangnya alat telekomunikasi yang dipadukan dengan jam tangan yang dikenal sebagai smartwatch. Perkembangan smartwatch telah menyamai kemampuaan yang ada di smatphone, sehingga tidak menutup kemungkinan smartwatch dapat digunakan sebagai alat tindak kejahatan. Hal ini merupakan tantangan bagi IT forensik dan penegak hukum untuk melakukan penyelidikan terhadap smartwatch dari seseorang yang melakukan kejahatan dijadikan tersangka dari sebuah kasus. Caranya adalah dengan menerapkan pengembangan metode-metode forensic yang ada, sehingga dari hasil yang didapatkan dari metode forensic yang dilakukan diharapakan menjadi hasil yang berguna bagi IT forensic dan penegak hukum.

***Kata kunci**, Smartwatch, Mobile forensic, telekomunikasi, kejahatan*

1. PENDAHULUAN

Perkembangan teknologi saat ini berkembang sangat pesat. Pada saat ini telah berkembang alat telekomunikasi yang dipadukan dengan jam tangan yaitu jam tangan pintar atau yang lebih dikenal dengan nama *smartwatch*. Dahulu fungsi jam tangan hanya sebatas untuk mengetahui waktu saja, saat ini smartwatch kini berkembang dengan fitur-fitur yang disesuaikan dengan kebutuhan penggunanya. Bahkan beberapa vendor jam tangan pintar, kini melengkapi fitur-fitur yang sama dengan smartphone. Jam tangan pintar ini dapat membantu aktifitas kita sehari-hari, seperti 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.

Seiring berkembangnya dan bertambahnya pengguna smartwatch tersebut tidak menutup kemungkinan dapat membawa efek buruk terhadap perkembangan dan peradaban manusia itu sendiri, seperti meningkatnya tindak kejahatan yang memanfaatkan fitur-fitur yang ada di *smartwatch*, meningkatnya tindakan menyontek, dan lain sebaginya, faktor ukuran dan banyaknya fitur-fitur yang ada di *smartwatch* merupakan kelebihan utama dibandingkan mengunakan *smartphone*.

Hal ini merupakan tantangan baru bagi IT *forensic* dan penegak hukum untuk melakukan penyidikan terhadap *smartwatch* dari seorang yang melakukan tindakan kejahatan yang dapat dijadikan tersangaka dari sebuah kasus berdasarkan bukti-bukti yang ada seperti sms, telepon, kontak telepon, file-file, dan sebagainya yang ada di dalam smaratwatch tersebut.

Penelitian ini merupakan lanjutan dari penelitian sebelumnya yaitu Ilman Zuhri Yadi, Yesi Novaria Kunang. Program Studi Sistem Informasi, Ilmu Komputer Universitas Binadarma pada tahun 2014 dengan judul Analisis Forensik Pada Platform Android. Namun penelitian sebelumnya ini mengunakan smartphone Android sehingga jika

pengguna menggunakan *smartwatch*, maka tim dari *investigator* IT Forensik tidak dapat menjalankan metode-metode yang ada.

Penulis tertarik untuk melakukan analisis terhadap *smartwatch* android, dengan menggunakan pengembangan metode forensik. Berdasarkan latar belakang yang telah diuraikan diatas maka penulis tertarik untuk menulis artikel ini dengan judul " Forensik Mobile pada smartwatch Berbasis Android" [1]. Agar pembahasan penelitian ini lebih terarah dan tak melebar dari pembahasan maka penulis membatasi permasalahan yang ada hanya pada kemungkinan berhasil atau tidaknya data sms, data kontak telepon, dan data history panggilan yang ada dismartwatch ditampilkan dan dijadikan sebagai barang bukti tindak kejahatan.

2. METODE PENELITIAN

2.1 IT Forensik

Menurut Budhisantoso, digital forensik adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum, Sedangkan menurut Marcella (2002), secara terminologi, komputer forensik atau forensik TI adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan atau penyaringan, dan dokumentasi bukti komputer dari sebuah kejahatan komputer [2].

2.2 Mobile Forensik

Mobile forensik merupakan cabang dari forensik digital yang berkaitan dengan pemulihan bukti digital atau data dari perangkat mobile di bawah forensik kondisi suara. Perangkat selular frase biasanya merujuk ke ponsel, namun juga dapat berhubungan dengan perangkat digital yang memiliki baik memori internal dan komunikasi kemampuan.

Penggunaan ponsel dalam kejahatan secara luas diakui untuk beberapa tahun, tetapi studi forensik perangkat mobile merupakan bidang yang relatif baru, berasal dari awal 2000-an. Sebuah proliferasi ponsel (terutama smartphone) di pasar konsumen menyebabkan permintaan untuk pemeriksaan forensik dari perangkat, yang tidak dapat dipenuhi oleh ada komputer forensik teknik.

Proses investigasi biasanya difokuskan pada data yang sederhana seperti data panggilan, dan komunikasi seperti email atau sms, dan juga data yang sudah terhapus dari media penyimpanan mobile device. *Mobile devices* biasanya juga bisa digunakan untuk menemukan informasi mengenai lokasi, yaitu mengunakan GPS atau alat pencari lokasi atau melalui *cell site logs*, yang melacak perangkat yang masuk di dalam *range*-nya. Informasi yang diambil dari perangkat mobile dapat berguna dalam berbagai masalah hukum, administratif dan investigasi seperti: pencurian kekayaan intelektual, penipuan perusahaan, penyalahgunaan properti, perceraian & hukum keluarga, geo-lokasi kontroversi, bukti kejahatan [3].

2.3 Smartwatch

Selama ini sudah ada smartphone, telpon pintar. Kemudian smart TV, TV pintar dan sekarang Smartwatch, jam pintar. Istilah Smart yang dilekatkan pada sebuah objek elektronik umumnya berarti perangkat tersebut dapat terkoneksi dengan internet atau perangkat elektronik yang lain. Istilah *smartwatch* secara umum berarti sebuah jam tangan yang dapat terhubung ke internet dan juga perangkat elektronik yang lain (smartphone atau tablet) untuk mendapatkan informasi yang akurat dari perangkat tersebut. Smartwatch dapat menjalankan fungsi dasar layaknya smartphone. Dengan smartwatch kita bisa memiliki akses ke berita, cuaca, gps, email, sms dan telpon masuk dan banyak lagi [4].

2.4 Mobiledit

Versi lite MOBIL edit didownload dari Internet. Installasi MOBILedit tidaklah terlampau sulit. Seperti juga Oxygen, MOBILedit membutuhkan kondisi USB *debugging mode* enabled di ponsel. Ponsel bisa terkoneksi baik menggunakan kaebl langsung maupun menggunakan koneksi *wireless*. Hal ini memberikan keuntungan untuk jensi ponsel yang tidak bisa didetekesi menggunakan software ini bisa diutilisasi menggunakan koneksi wireless. MOBILedit akan menginstall aplikasi kecil di ponsel untuk menarik data. Data yang iekstrak dibatasi hanya contacts, call lists, messages dan file

2.5 Metasploit

Metasploit merupakan sofware security yang sering digunakan untuk menguji coba ketahanan suatu sistem dengan cara mengeksploitasi kelemahan software suatu sistem. Metasploit diciptakan oleh HD Moore pada tahun 2003 sebagai sebuah alat jaringan portabel menggunakan bahasa scripting Perl. Kemudian, Metasploit Framework benar-benar ditulis ulang dalam bahasa pemrograman Ruby. Pada tanggal 21 Oktober 2009, Proyek Metasploit mengumumkan yang telah diakuisisi oleh Rapid7, sebuah perusahaan keamanan yang menyediakan solusi kerentanan manajemen terpadu.

Seperti produk komersial yang sebanding seperti kanvas Imunitas atau Inti Dampak Core Security Technologies, Metasploit dapat digunakan untuk menguji kerentanan sistem komputer untuk melindungi mereka atau untuk masuk ke sistem remote. Seperti alat-alat keamanan banyak informasi, Metasploit dapat digunakan untuk kegiatan baik yang sah dan tidak sah. Sejak akuisisi dari Metasploit Framework.

Metasploit biasanya digunakan untuk menyerang application layer dengan 0 day attack yang merupakan metode penyerangan pada software yang belum di patch. Metasploit biasa dikaitkan dengan istilah remote exploitation, maksudnya penyerang berada pada jarak jangkauan yang jauh dapat mengendalikan komputer korban. Metasploit menyerang dengan cara mengirimkan exploit pada komputer korban. Exploit ini berisi payload yang sudah ditentukan oleh penyerang. Exploit adalah software yang berfungsi untuk memanfaatkan kelemahan pada software korban(misal web browser), setelah berhasil mengeksploitasinya exploit tersebut memasukkan payload ke dalam memori korban. Payload merupakan sebuah executable milik penyerang yang akan di run pada komputer korban dengan tujuan dapat mengendalikan komputer tersebut secara remote atau memasang backdoor, trojan, virus, worm, dan lain-lain. Terlepas dari penggunaan metasploit yang disalah gunakan untuk kejahatan, software ini juga membantu System Security untuk memperkuat pertahanan jaringannya dari ulah penyerang dari luar.

2.6 Metode Penelitian

Metode penelitian yang digunakan berdasarkan pedoman forensik perangkat mobile yang saya kembangkan dari National Institute of Justice (NIJ) pada Gambar 1. Berdasarkan Gambar 1 diperoleh langkah-langkah forensic sebagai berikut :

a. Identifikasi
   Pada tahap ini peneliti mengidentifikasi masalah yang ada dengan cara mengumpulkan informasi sebanyak banyaknya terhadap alat yang akan peneliti forensik.
b. Solusi
   Pada tahap ini peneliti akan mengumpulkan atau menyiapkan solusi solusi yang mungkin akan kita lakukan selama proses forensic dilakukan.
c. Mempersiapkan

Pada tahap ini peneliti melakukan persiapan apa saja yang bakal peneliti lakukan berdasarkan solusi solusi yang kita temuin.

d. Mengamankan
   Pada tahap ini peneliti akan melakukan pengaman data pada barang bukti yang ada.
e. Menguji
   Pada tahap ini peneliti akan menguji alat dan bahan yang dimiliki oleh penulis.
f. Evaluasi
   Pada tahap ini penulis akan melakukan evaluasi apakan hasil pengujian berjalan baik dan akan digunakan untuk melakukan forensic selanjutnya.
g. Melaporkan
   Pada tahap ini penulis melaporkan hasil yang di dapat oleh peneliti kepada pihak yang membutuhlan data tersebut.

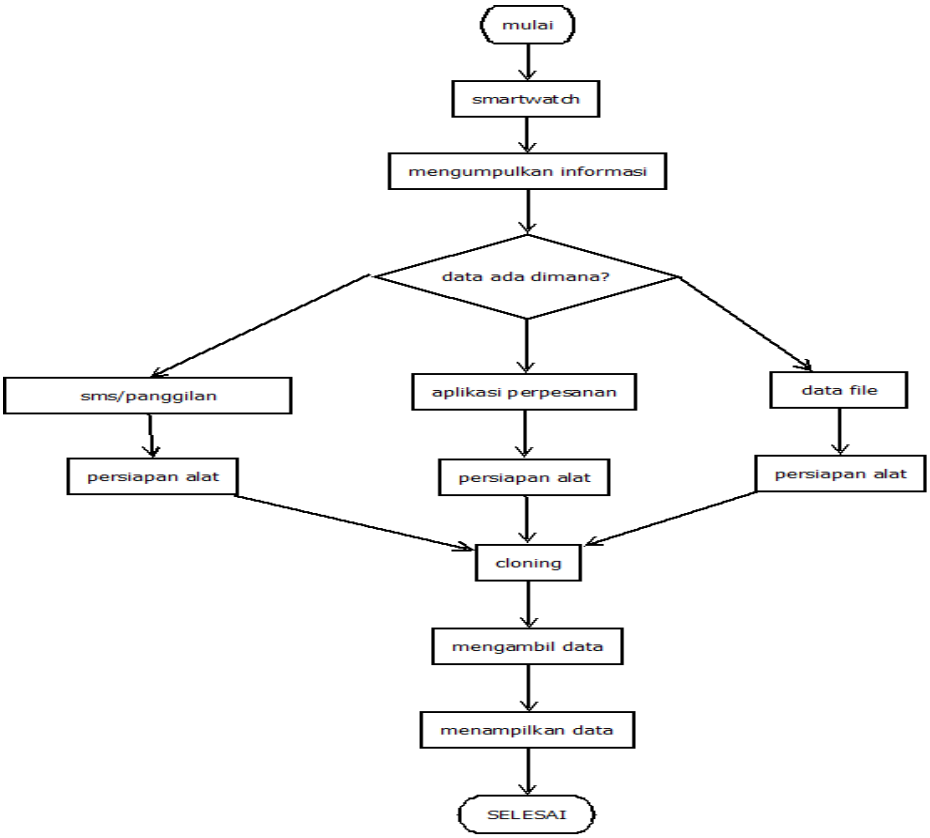
Gambar 1. Metode Pengembangan NIJ

2.7 Metode Analisis

Adapun metode analisis smartwatch pada proses uji coba pengambilan barang bukti yang ada dismartwatch yaitu dengan cara menerapkan metode forensic pada alur diagram yang terdapat pada Gambar 2. Alur proses melakukan forensic pada smartwatch sebagai berikut :

a. Peneliti mengumpulkan informasi informasi tentang smartwatch tersebut dan mengumpulan informasi data apa yang akan di forensic
b. Mencari informasi data tersebut berbentuk apa? Apakah data sms/panggilan, data yang ada di aplikasi perpesanan, file file yang disimpan di smartwatch tersebut
c. Melakukan persiapan alat berdasarkan apa data apa yang kita ambil
d. Melakukan cloning terhadap barang bukti yang berupa smartwatch

e. Mengambil data
f. Menampilkan data kemudia kita laporkan

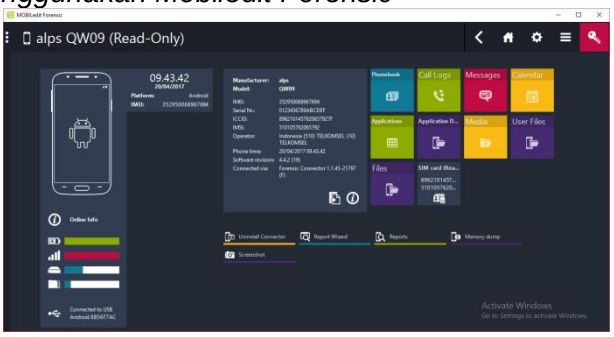


Gambar 2. Alur Metode Forensik

3. HASIL DAN PEMBAHASAN

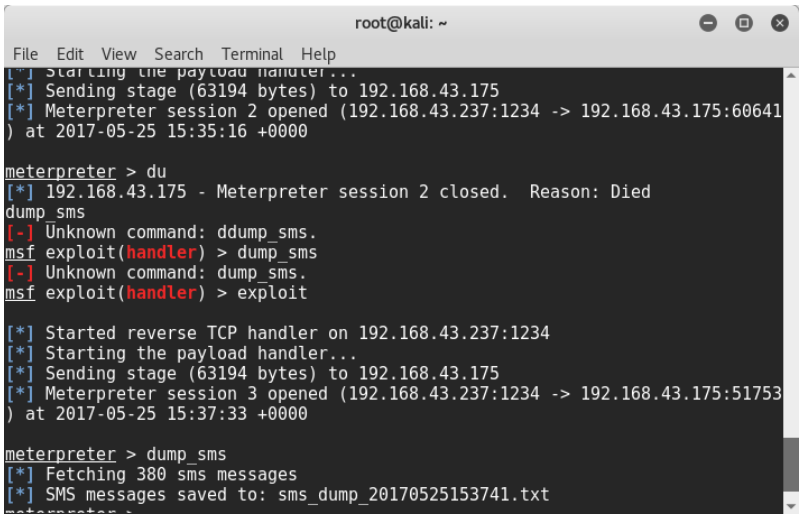
Hasil pengujian ini merupakan hasil uji coba dari pengembangan metode yang telah dibuat dimana pertama kali penulis lakukan adalah melakukan identifikasi masalah yang terjadi, pada tahap ini merupakan tahap dimana penulis mengumpulkan informasi-informasi tentang data apa yang akan dicari, pada tahap selanjutkan penulis mencari dan mengumpulkan solusi-solusi apa saja yang akan dilakukan dalam mengumpulkan bukti bukti yang ada di smartwatch, pada tahap selanjutnya penulis mempersiapkan alat apa saja yang akan digunakan dalam mengumpulkan bukti-bukti yang ada di smartwatch.

3.1 Hasil uji coba menggunakan Mobiledit Forensic



Gambar 3. Tampilan data-data yang bisa ditampilkan di smartwatch

3.2 Hasil UJi Coba Menggunakan tool Metasploit di kali linux



Gambar 5. Tampilan Metasploit Berhasil Mengambil Data-data sms di Smartwatch

3.3 Hasil Perbandingan penggunaan tool Mobiledit forensic dan Metasploit

Berikut tabel hasil uji co10a tool forensic yang penulis gunakan

Tabel 1. Perbandingan penggunaan tool forensik

Tool	Sms	Histori Panggilan	Kontak
Mobiledit Forensic	7	0	10
Metasploit	380	0	8

Dari tabel 1 didapatkan perbandingan antara tool mobiledit forensic yang cukup signifikan, hal ini dikarenakan pada saat penulis melakukan forensic menggunakan mobiledit forensic tool tersebut membutuhkan sambungan kabel data yang cukup baik. Sedangkan pada saat penulis menggunakan Metasploit membutuhkan sambungan wifi.

4. KESIMPULAN

Kesimpulan yang diperoleh berdasarkan hasil penilitian ini adalah:

1. Setelah melakukan uji coba serta Analisa forensic menggunakan tool Mobiledit forensik pada smartwatch maka disimpulkan
   a) Semua teknik yang dilakukan berdasarkan metode yang dikembangkan, memiliki keberhasilan hampir 100 % dalam mengumpulkan data-data yang ada berupa sms, data kontak, dan data pangilan yang ada dismartwatch
   b) Dari hasil uji coba menggunakan mobiledit forensic ditemukan kelemahan dari tool tersebut, yaitu tidak bisa mengembalikan data-data yang hilang pada smartwatch yang penulis teliti.
2. Setelah melakukan uji coba menggunakan tool forensic yang ada di kalilinux metasploit, dapat disimpulkan
   a) Semua teknik yang dilakukan berdasarkan metode yang dikembangkan, memiliki keberhasilan hampir 100 % dalam mengumpulkan data-data yang ada berupa sms, data kontak, dan data pangilan yang ada dismartwatch
   b) Dari hasil uji coba menggunakan metasploit ditemukan kelemahan dari tool tersebut, yaitu tidak bisa mengembalikan data-data yang hilang pada smartwatch yang penulis teliti.

5. SARAN

Dari metode forensik yang telah dikembangjkan, tentunya masih perlu pengembangan agar metode ini bisa lebih baik dari sebelumnya. Saran untuk pengembangan selanjutnya sebagai berikut.

1. Menggunakan tool-tool forensic yang lebih bagus lagi agar data-data yang hilang bisa dikembalikan.
2. Fitur-fitur yang ada di metasploit harus dikembangkan lagi agar bisa menampilkan data-data yang dibutuhkan .

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada civitas akademika Magister Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta

DAFTAR PUSTAKA

[1] Ilman Zuhri Yadi, Yesi Novaria Kunang, “ANALISIS FORENSIK PADA PLATFORM ANDROID,” Konferensi Nasional Ilmu Komputer, p. 1, 2014.
[2] Alamsyah, Zanial Mazalisa, Rasmila, “Analisis ForensikRecovery Dengan Keamanan Kode Password Pada Smartphone Android,” Jurnal Binadarma, p. 3, 2015.
[3] Ahmad Thufail A., Surya Michrandi N.,Budhi Irawan, “Analisis Dan Implementasi Mobile Forensik Pemulihan Data Yang Hilang Pada Smartphone Berbasis Sistem Operasi Android,” Epoc, vol. 6, p. 4, 2015.
[4] Shreyas Parikh1, IFS, GFSU, Dhaval Chavda, IFS, GFSU, Shourjo Chakraborty, systools Software Pvt. Ltd. Dr. Parag H. Rughani, IFS, GFSU, Dr. M. S. Dahiya, IFS, GFSU, "Analysis of Android Smart Watch Artifacts," International Journal of Scientific & Engineering Research, vol. 6, p. 2, 2015.
[5] A. Hoog, “Introduction to Android forensic”, DFI, April 30 2010.
[6] E.C., Turnbull, “Digital Evidence on Mobile Devices”,In E. Casey, Digital Evidence and Computer Crime (3rd Edition ed.), Academic Press, 2011.
[7] L. Novitasari, et al., "Geographic information systems of android-based residential locations," in 4th International Conference on Information Technology and Engineering Application 2015 (ICIBA2015), Bina Darma University, Palembang, 2015.
[8] http://swarmnyc.com/whiteboard/building-android-wear-watch-face-with-live-weather-data-3/
[9] Saminath, “Power of Android Wearable Technology”, International Journal of Scientific and Research Publications, Volume 5, Issue 2, February 2015.
[10] https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf