PEMERIKSAAN MOBILE FORENSIK TERHADAP *HANDPHONE* SECARA *PHYSICAL EXTRACTION* DENGAN PERBEDAAN JENIS SOFTWARE

Hasta Saputra*, Tris Zenno Al Kindi, Hery Priyanto, Agus Dwi Setiono, Panji Zulfikar Sidik
Puslabfor Bareskrim Polri, Indonesia

*Correspondence E-mail: hastasaputragunawan@gmail.com

ARTICLE INFO

Article history:

Received 21 Juny 2021

Revised 22 August 2021

Accepted 25 September 2021

Available online 19 October 2021

Keywords: mobile, forensic, nokia

Kata kunci: mobile, forensik, nokia

DOI:

<https://doi.org/10.54579/jfe.v1i3.12>

ABSTRACT

One of the electronic evidence found at the crime scene or related to cases, both criminal and civil, is cellphone evidence. To prove the presence or absence of the perpetrator's involvement with the use of mobile forensic examination techniques by physical extraction through analysis of digital traces in the form of call logs, SMS, phonebooks and other files where the data has been deleted. Several factors affect the physical extraction method, namely the software used. Mobile forensic examination software used to examine electronic evidence such as cellphones in forensic laboratories is Ufed Cellebrite 4 PC and XRY Microsystem. In this study, the level of success of the physical extraction method was investigated on evidence of a Nokia 105 (TA-1174) mobile phone with different software, namely Ufed Cellebrite 4 PC and XRY Micro Systemation. Extraction was carried out using the physical boot loader method on the memory in the Nokia 105 (TA-1174) mobile phone IMEI 1: 353810821569303 IMEI 2: 353810821569306. by using Ufed 4 Pc software and XRY Microsystemation, where the extraction results obtained, especially call logs, SMS and data that have been deleted using XRY Microsystemation software, have the most complete success rate. This relates to the ability of each software in parsing/dumping and decoding processes.

ABSTRAK

Salah satu barang bukti elektronik yang ditemukan di TKP atau yang berkaitan dengan kasus, baik pidana maupun perdata adalah barang bukti handphone. Untuk membuktikan ada atau tidaknya keterlibatan pelaku dengan pemanfaatan teknik pemeriksaan mobile forensik secara physical extraction melalui analisa jejak digital berupa call logs, SMS, phonebooks dan file-file lain yang mana data-data tersebut telah terhapus. Beberapa faktor mempengaruhi dengan metode physical extraction, yaitu software yang digunakan. Software pemeriksaan mobile forensik pada Laboratorium forensik adalah Ufed Cellebrite 4 PC dan XRY Microsystem. Dalam penelitian ini, diteliti tingkat keberhasilan metode physical extraction pada pada barang bukti handphone merk Nokia 105 (TA-1174) dengan software yang berbeda yaitu Ufed Cellebrite 4 PC dan XRY Micro Systemation. Ekstraksi dilakukan dengan metode physical boot loader terhadap memory yang berada di dalam handphone Nokia 105 (TA-1174) IMEI 1 : 353810821569303 IMEI 2 : 353810821569306. Berdasarkan hasil penelitian ini, pemeriksaan secara physical extraction terhadap barang bukti handphone Nokia 105 (TA-1174) dengan menggunakan software Ufed 4 Pc dan XRY Microsystemation, yang mana hasil ekstraksi yang di dapat khususnya call logs, sms dan data yang sudah terhapus menggunakan software XRY Microsystemation mempunyai tingkat keberhasilan yang paling lengkap. Hal ini berkaitan dengan kemampuan masing-masing software dalam melakukan parsing/dumping dan proses decoding.

How to Cite :

Saputra, H. AlKindi T. Z.,
Priyanto, H., Setiono, A. D., Sidik,
P. Z. (2021). Pemeriksaan Mobile
Forensik Terhadap Handphone
Secara Physical Extraction dengan
Perbedaan Jenis Software
. *Journal of Forensic Expert*, 1(3),
39-47.

Pendahuluan

Mobile forensik merupakan cabang dari digital forensik yang dilakukan untuk memperoleh dan menganalisis bukti-bukti digital dari perangkat mobile (*handphone/smartphone*). Sedangkan, *Physical Extraction* merupakan ekstraksi yang paling lengkap karena bisa mendapatkan data atau informasi yang masih ada (*intact*), maupun yang sudah terhapus (*deleted* dan *lost*) (Muhammad Nuh Al Azhar, 2021). Kejahatan atau tindak pidana umum dan khusus sering kali melibatkan barang bukti elektronik, yang mana barang bukti elektronik tersebut menyimpan data-data atau informasi-informasi digital, salah satunya adalah barang bukti *handphone*. Dari barang bukti tersebut menyimpan data-data yang berkaitan dengan sejarah penggunaan *handphone* berupa call logs (*incoming*, *outgoing* dan *missed calls*), SMS (*inbox*, *sent* dan *draft*), phonebooks/contacts dan *file-file* lain seperti gambar, *video*, *audio* dan *email*.

Pemeriksaan mobile forensik dapat dijadikan acuan untuk membuat terang suatu tindak pidana dengan menyajikan bukti – bukti digital, yang mana bukti tersebut dapat dijadikan salah satu bukti yang sah di depan pengadilan yaitu melalui keterangan ahli dan surat (Berita Acara Pemeriksaan Laboratoris Kriminalistik Barang Bukti) yang mengacu ke dalam Pasal 184 ayat (1) Kitab Undang Undang Hukum Acara Pidana (KUHAP) disebutkan bahwa alat bukti yang sah adalah keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Dikarenakan pentingnya barang bukti tersebut dalam memberikan petunjuk atau pengungkapan kasus kejahatan yang berhubungan dengan *handphone*, untuk itu penanganan dan pemeriksaan secepatnya analisa barang bukti *handphone* harus sesuai dengan prinsip-prinsip dasar digital forensik yang mengacu kepada guidelines internasional seperti yang diterbitkan oleh Association of Chief Police Officers (ACPO) dan 7Safe di Inggris, dan oleh National Institute of Justice yang berada di bawah Department of Justice, Amerika Serikat. Dengan penanganan barang bukti *handphone* yang benar, diharapkan hasil pemeriksaan dan analisa bidang mobile forensik dapat menunjukkan secara ilmiah data-data atau informasi digital yang ada di dalam suatu *handphone* baik data yang masih ada ataupun yang sudah terhapus untuk mendukung tugas penyidik dalam mengungkap kejahatan.

Pada penelitian ini menggunakan barang bukti *handphone* merk Nokia dengan sistem operasi Symbian, Saat ini Symbian OS jumlah telah digunakan oleh bermacam vendor produk peralatan komunikasi mobile pada bermacam jenis produk mereka yang bervariasi. Variasi dari sisi hardware ini dimana Symbian OS diimplementasi bisa dimungkinkan karena sistem operasi ini memiliki antarmuka pemrograman aplikasi (Application Programming Interface; API). API mendukung terhadap komunikasi dan tingkah laku yang umum pada hardware yang bisa digunakan oleh objek aplikasi lain. Hal ini dimungkinkan karena API yaitu objek antarmuka yang didefinisikan pada level aplikasi, yang berisikan prosedur dan fungsi (dan juga variabel serta struktur data) yang mengelola/memanggil kernel dimana sebagai penghubung selang software dan hardware. Dengan keadaan standar API ini menolong pihak pengembang bagi melakukan penyesuaian atas aplikasi yang diciptakannya supaya bisa diinstal pada produk telepon melakukan usaha yang berjenis-jenis.

Mirip seperti sistem operasi desktop, Symbian OS mampu melakukan operasi secara multithreading, multitasking dan pengamanan terhadap memori. Dan semua pemrograman pada Symbian dipertontonkan secara event-based, gunanya hardware CPU menjadi tidak aktif ketika

tidak mempunyai inputan berupa cara tertentu. Namun perlu dimengerti sistem operasi ini memang ditujukan bagi diinstal pada peralatan mobile dengan keterbatasan sumber daya. Multithread dan multitasking memberikan kemampuan Symbian OS bagi menjalankan semakin dari satu aplikasi sekaligus. Namun khusus ini, keadaan preemptive multitasking kernel akan memberi tiap-tiap program suatu pembagian waktu pemrosesan yang dipertontonkan bergantian dengan cepat sehingga nampak bagi pemakai seolah-olah bagian ini dieksekusi secara bersamaan. Bagi itu telah dirumuskan penjadwalan berdasar prioritas tertentu bagi menentukan bagian mana yang berlanjut terlebih dahulu dan bagian apa berikutnya serta berapa jumlah waktu akan berlaku diberi.

Symbian OS sendiri bukanlah software yang sifatnya open source secara penuh karena meskipun terdapat ketersediaan API dan dokumentasinya, yang jumlah menolong pihak pengembang aplikasi bagi membuat software yang berlanjut di atas sistem operasi ini, dipublikasi bagi umum namun tidak bagi kode source sendiri (Nokia Buys Rest of Symbian, Will Make Code Open Source", PC World, 24 Juni 2008).

Pemeriksaan mobile forensik dengan metode *physical extraction* dipengaruhi oleh beberapa faktor, yaitu ; jenis handphone dan software yang digunakan untuk melakukan ekstraksi. *physical extraction* sangat mirip dengan proses akuisisi post-mortem forensik komputer. *physical extraction* akan membuat replika bit-demi-bit dari semua data yang ada di dalam perangkat seluler, termasuk file yang disembunyikan dan dihapus. Selain informasi yang diperoleh dari ekstraksi logis, ekstraksi fisik dapat menghasilkan yang berikut: kata sandi yang dihapus, file, foto, dan video yang dihapus, foto Snapchat yang dihapus, pesan teks, kontak, log panggilan yang dihapus, tag lokasi & perbaikan GPS (Milwaukee Private Detective, 2018). *physical extraction* data ponsel tidak meninggalkan tanda-tanda penyelidikan terjadi setelah ekstraksi selesai. Dalam penelitian ini faktor yang akan dianalisis adalah software yang digunakan untuk melakukan ekstraksi terhadap barang bukti handphone Nokia 105. Hal ini dikarenakan masing-masing software mempunyai perbedaan khususnya terhadap hasil ekstraksi. Diharapkan dalam penelitian ini dapat diketahui software mana yang memiliki tingkat keberhasilan analisis *physical extraction* yang paling lengkap.

Metode

Extraction atau proses ekstraksi terhadap isi dari barang bukti handphone dilakukan setelah proses identifikasi dan koneksi terhadap handphone tersebut selesai, kedua proses ini saling terkait untuk dapat membaca dan mengekstraksi isi dari barang bukti handphone. Proses ekstraksi tersebut terbagi menjadi 3 (tiga) jenis yaitu Logical, File System dan Physical Extraction. Dalam penelitian ini dilakukan *physical extraction* untuk mendapatkan data atau informasi yang masih ada dan yang telah terhapus. Dalam penelitian ini juga menggunakan 5 (lima) tahapan proses forensik dari *National Institute of Justice* (NIJ) yaitu :

Gambar 1. Lima tahapan proses forensik dari *National Institute of Justice* (NIJ)

Pemeriksaan mobile forensik dapat dilakukan dengan beberapa tools baik yang bersifat open source maupun closed source. Tools tersebut juga bervariasi ada yang hanya bisa logical extraction dan tidak bisa jenis ekstraksi yang lain, namun ada juga yang bisa mencakup semua jenis ekstraksi. Tools ekstraksi yang digunakan dalam penelitian ini yaitu tools yang bersifat software yaitu Ufed Cellebrite 4 PC version 7.48.0.49 dan XRY XRY Micro Systemation version.

Sampel

Sampel dalam penelitian ini adalah barang bukti 1 (satu) unit *handphone* Nokia 105 (TA-1174) IMEI 1 : 353810821569303 IMEI 2 : 353810821569306. Pemilihan sampel dalam penelitian ini dilakukan dikarenakan saat ini tindak pidana kasus narkoba banyak menggunakan *handphone* jenis ini.

HASIL DAN PEMBAHASAN

Hasil

Tahapan proses ekstraksi terhadap barang bukti *handphone* dengan menggunakan metode *physical extraction* yaitu tahapan *Identification* : melakukan identifikasi terhadap barang bukti yaitu berupa *handphone* Nokia 105 (TA-1174) IMEI 1 : 353810821569303 IMEI 2 : 353810821569306; *Collection* : melakukan cloning terhadap file dump barang bukti dan menjaga integritas barang bukti dari perubahan dengan verifikasi nilai *hash*, Menurut Barbara J. Roshtein (2007) dalam sebuah bukunya yang berjudul *Managing Discovery of Electronic Information : A Pocket Guide for Judges*, fungsi hash atau yang biasa disebut hash saja yaitu : “A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. ‘Hashing’ is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production” Yang jika diterjemahkan ke dalam bahasa Indonesia yaitu : “Suatu pengkodean unik yang diberikan ke file, kelompok file, atau bagian dari file, menggunakan standard algoritma matematika untuk memberikan karakteristik atau semacam identitas pada

kumpulan data tersebut. Algoritma yang paling sering digunakan yaitu MD5 dan SHA, yang mana akan menghasilkan nilai angka khusus dan probabilitas munculnya angka yang sama untuk 2 buah data tersebut 1 berbanding 1 miliar. 'hashing' digunakan untuk menjamin keaslian data original (sebelum di akuisisi) dan dapat digunakan sebagai cap digital seperti cap atau stempel yang digunakan pada dokumen kertas". ; Examination : melakukan pemeriksaan/akuisisi dengan proses ekstraksi dari barang bukti digital akun media sosial facebook dan melakukan verifikasi dengan hash analysis SHA1; Analysis : Melakukan proses analisa terhadap hasil ekstraksi atau parsing dari barang bukti digital akun media sosial yang sesuai dengan data-data investigatif kasus dan Reporting : Pembuatan report dalam bentuk PDF files yang menjelaskan proses tahapan atau tindakan yang dilakukan oleh pemeriksa digital forensik

Dokumentasi dan koneksi dari sampel barang bukti

Menggunakan Software Ufed Cellebrite 4 PC *version 7.47.0.247*

Melakukan proses pencarian jenis handphone dengan cara meng klik menu bertuliskan Mobile Device dan mengetikkan pada menu search by name : TA-1174, maka tampilan pada gambar bertuliskan Nokia GSM TA-1174 DS 105 (2019) (gambar 1) yang selanjutnya di cocokkan dengan Barang bukti *handphone* Nokia 105 (TA-1174). Setelah pencarian sesuai dengan barang bukti fisik yang akan diperiksa, selanjutnya melakukan pemilihan jenis ekstraksi yaitu Physical dan memilih jenis kabel yang sesuai yaitu Cable A with black tip T-100 (Gambar 2). Selanjutnya memilih mode yaitu "Boot Loader", lalu mempersiapkan Ufed Device Adapter yang berada pada port Source dan koneksikan adapter tersebut ke barang bukti handphone (Gambar 4). Koneksikan barang bukti dengan memperhatikan hal-hal sebagai berikut : 1) *Remove the battery and SIM*; 2) *Connect the device without battery*; 3) *Press continue*. Selanjutnya *software* akan mendeteksi secara otomatis barang bukti tersebut (Gambar 5)

Gambar 2. Barang bukti handphone Nokia 105 (TA-1174) IMEI 1 : 353810821569303 IMEI 2 : 353810821569306

Gambar 3. Tahapan ekstraksi handphone menggunakan Ufed Cellebrite 4 PC

Gambar 4. Tahapan koneksi adapter ke barang bukti handphone menggunakan Ufed Cellebrite 4 PC

Gambar 5. Tahapan pendeteksian barang bukti secara otomatis

Setelah berhasil terkoneksi maka dilakukan tahapan koneksi kedua dengan cara mengikuti instruksi yaitu *“press and hold the scroll key button and the # or * button (located opposite of the mini USB side) Do not releases until the extraction starts”* dan proses ekstraksi berjalan sesuai dengan waktu ekstraksi serta proses ekstraksi selesai (Gambar 6).

Gambar 6. Tahapan proses ekstraksi sampai dengan selesai

Menggunakan software XRY Micro Systemation version

Melakukan proses pencarian jenis *handphone* dengan cara meng klik *menu device* dan mengetikkan pada menu search Nokia 1174, maka tampilan pada device found bertuliskan Nokia 105 Dual SIM (2019) (TA-1174) yang selanjutnya di cocokkan dengan Barang bukti *handphone* Nokia 105 (TA-1174). Setelah pencarian sesuai dengan barang bukti fisik yang akan diperiksa, selanjutnya melakukan pemilihan jenis ekstraksi yaitu Physical dan memilih jenis kabel yang sesuai yaitu Cable A microUSB (Gambar 7).

Gambar 7. Tahapan pemilihan jenis kabel (Cable A micro USB)

Selanjutnya melakukan tahapan ekstraksi secara physical dengan ketentuan sebagai berikut:
 1) *Disconnect the device*; 2) *Remove the battery and SIM card from the phone*; 3) *Attach the cable to the XRY device USB port*; 4) *Click “OK” to continue*, Lalu klik tombol *ok*.

Gambar 8. Tahapan instruksi ekstraksi

Selanjutnya proses ekstraksi dapat di teruskan dengan ketentuan sebagai berikut : 1) Press and hold the “*” button on the device; 2) Press and hold all options in the center button, so all directions are pressed; 3) Connect device to computer; 4) Release the button(s) after the dumping process continues

Analisis Data

Perhitungan tingkat keberhasilan dilakukan dengan menghitung jumlah data hasil ekstraksi berupa *call logs*, *SMS* dan jumlah data yang telah terhapus (deleted) yang berhasil di *recovery*. Hasil parsing pemeriksaan *mobile* forensik menggunakan metode *physical extraction* terhadap barang bukti *handphone* Nokia 105 (TA-1174) IMEI 1 : 353810821569303 IMEI 2 : 353810821569306 dengan menggunakan 2 (dua) *software* yaitu :

Ufed Cellebrite 4 PC *version* 7.47.0.247 dan Physical Analyzer *version* 7.48.0.49

Analisa terhadap *file* jedec0.bin dengan nilai HASH SHA256 : 4E489CD90F9C98BAFD68ABC1DD689237FDAA3D6E572B0318D367DE6A7FD051C4, dengan Time Code UTC+7 hasil ekstraksi sebagai berikut :

Tabel 1. Tabel hasil pemeriksaan menggunakan Ufed Cellebrite 4 PC

Type	Total Data	Total data terhapus (deleted)
Call Log	131	12
Instant Messages	75	

XRY Micro Systemation *version* dan XAMN 5.2.0 Build 55851

Analisa terhadap *file* jedec0.bin dengan nilai HASH SHA256 : 4E489CD90F9C98BAFD68ABC1DD689237FDAA3D6E572B0318D367DE6A7FD051C4, Time Code UTC+7 hasil ekstraksi sebagai berikut :

Tabel 2. Tabel hasil pemeriksaan menggunakan XRY Micro Systemation

Type	Total Data	Total data terhapus (deleted)
Call Log	130	12
Instant Messages	85	

Tingkat keberhasilan analisis secara *physical extraction* dihitung dari jumlah data-data yang berhasil di *recovery* dan di *decoding* yaitu pada jumlah SMS. Berikut merupakan tabel hasil perhitungan tingkat keberhasilan berupa data-data SMS pada barang bukti *handphone* Nokia

105 (TA-1174) IMEI 1 : 353810821569303 IMEI 2 : 353810821569306.

Tabel 3. Tingkat keberhasilan *recovey SMS* pada barang bukti.

NO	Jenis Software	Jumlah SMS
1.	<i>Ufed 4 Pc</i>	75
2.	<i>XRY Micsrosystemation</i>	85

Pembahasan

Metode physical extraction merupakan metode yang paling efektif dikarenakan data-data dan informasi yang di dapat lebih banyak dan lengkap baik yang sifatnya *intact* maupun *deleted*. Terdapat banyak data-data yang berhasil di ekstraksi menggunakan metode ini. Pada penelitian ini menggunakan 2 (dua) software yang berbeda dengan 1 (satu) metode yaitu physical extraction. Berdasarkan hasil yang didapatkan dari analisa parsing dan decoding terhadap barang bukti yang sama khususnya pada jumlah SMS menggunakan software *Ufed 4 Pc* dan *XRY Micsrosystemation*, didapatkan bahwa data berupa SMS yang berhasil di recovery lebih banyak menggunakan software *XRY Micsrosystemation* pada barang bukti *handphone* Nokia 105 (TA-1174). Perbedaan hasil recovery ini terjadi pada proses akuisisi atau dumping terhadap isi dari memori *handphone* barang bukti, masing-masing software mempunyai keunggulan terhadap kecepatan mengakses EEPROM (*Electronically Erasable and Programmable read – Only Memory*) dan kemampuan melakukan proses decoding terhadap data berupa *file dumping*.

Penutup

Berdasarkan penelitian ini, disimpulkan bahwa pemeriksaan secara *physical extraction* terhadap barang bukti *handphone* Nokia 105 (TA-1174) dengan menggunakan software *Ufed 4 Pc* dan *XRY Micsrosystemation*, yang mana hasil ekstraksi yang di dapat khususnya data berupa SMS menggunakan software *XRY Micsrosystemation* mempunyai tingkat keberhasilan yang paling lengkap.

Daftar Pustaka

- ACPO 7Safe. (2008). Good Practice Guide for Computer-Based Electronic Evidence. UK ACPO and 7Safe.
- Al-Azhar, M.N. (2012). Digital Forensic: Panduan Praktis Investigasi Komputer". Salemba Infotek, Jakarta.
- Al-Azhar, M.N. (2021). Seri 1 Digital Forensik Panduan Umum Digital Forensik pada Platform Windows, Linux, Mac & Mobile.
- Cellebrite UFED 4PC User Guide - 7.49. Universal Forensic Extraction Device (UFED) V7.49; Cellebrite.(2021). Universal Forensic Extraction Device (UFED). Dapat diakses di <https://www.cellebrite.com/en/ufed/>.
- ISO/IEC 27037. (2014). Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.
- J Roshtein Barbara. (2007). Managing Discovery of Electronic Information.
- MSAB.2021.XRY help. XRY version 9.6.0 build 9.060.328.

MSAB.2021.XRY. Dapat di akses di <https://www.msab.com/products/xry/>.

National Institute of Justice. (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. US National Institute of Justice.

Nokia 105 2019 dual sim manual book. Dapat di akses di <https://manual-user-guide.com/nokia-105-2019-dual-sim-manual>.

Peraturan Kepala Pusat Laboratorium Forensik Badan Reserse Kriminal Polri Nomor 1. (2014). Standar Operasional Prosedur Pemeriksaan dan Analisa Digital Forensik.