REPUBLIK INDONESIA
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

SURAT PENCATATAN
CIPTAAN

Dalam rangka pelindungan ciptaan di bidang ilmu pengetahuan, seni dan sastra berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dengan ini menerangkan:

Nomor dan tanggal permohonan	:	EC00202333676, 9 Mei 2023
Pencipta		
Nama	:	**Drs. Ir. Faisal Syafar, M.Si., M.InfTech., Ph.D., IPU.**
Alamat	:	BTN Tabaria Tower E10/23 Kelurahan Mannuruki, Kecamatan Tamalate, Makassar, Sulawesi Selatan, 90221
Kewarganegaraan	:	Indonesia
Pemegang Hak Cipta		
Nama	:	**Universitas Negeri Makassar**
Alamat	:	Jln. A. P. Pettarani, Makassar, Sulawesi Selatan, 90222
Kewarganegaraan	:	Indonesia
Jenis Ciptaan	:	**Program Komputer**
Judul Ciptaan	:	**Simulation Of General Mobile Forensic Process**
Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia	:	10 Januari 2023, di Makassar
Jangka waktu pelindungan	:	Berlaku selama 50 (lima puluh) tahun sejak Ciptaan tersebut pertama kali dilakukan Pengumuman.
Nomor pencatatan	:	000466597

adalah benar berdasarkan keterangan yang diberikan oleh Pemohon.
Surat Pencatatan Hak Cipta atau produk Hak terkait ini sesuai dengan Pasal 72 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

a.n. MENTERI HUKUM DAN HAK ASASI MANUSIA
Direktur Hak Cipta dan Desain Industri

Anggoro Dasananto
NIP. 196412081991031002

Disclaimer:
Dalam hal pemohon memberikan keterangan tidak sesuai dengan surat pernyataan, Menteri berwenang untuk mencabut surat pencatatan permohonan.

SIMULATION OF GENERAL MOBILE FORENSIC PROCESS

Tinjauan proses forensik seluler

Mobile forensics merupakan bidang forensik digital yang difokuskan pada perangkat mobile yang berkembang sangat pesat. Karena pertumbuhan pasar seluler yang eksponensial, pentingnya forensik seluler juga meningkat. Ponsel umumnya milik satu orang sehingga analisisnya dapat mengungkapkan banyak informasi pribadi.

Karena pertumbuhan yang cepat, itu juga menimbulkan tantangan. Rasio model baru yang dirancang dan diluncurkan sangat tinggi sehingga sangat sulit untuk mengikuti prosedur serupa. Setiap kasus atau investigasi model baru perlu dipertimbangkan secara berbeda dan memerlukan langkah-langkah berikut yang mungkin berbeda dan unik untuk kasus tersebut. Dengan adanya tantangan dalam forensik seluler ini, menyinkronkan ponsel ke komputer menggunakan perangkat lunak menjadi mudah. Seseorang dapat mengekstraksi data seperti SMS, kontak, aplikasi yang terinstal, data GPS dan email, data yang dihapus.

Koleksi

Langkah-langkah di bawah ini disarankan untuk diikuti selama pengumpulan perangkat seluler

- Perhatikan lokasi tempat ponsel yang akan dikerjakan. Merupakan praktik yang baik untuk mengambil gambar menggunakan kamera lokasi dan ponsel sebelum memulai proses apa pun.
- Perhatikan status perangkat. Entah itu dimatikan atau dihidupkan. Jika dihidupkan, periksa status baterai, status jaringan. Periksa di mana layar terkunci.
- Cari paket SIM dan jika ada kabel di sekitarnya

Kelestarian Bukti

Pelestarian bukti adalah langkah yang sangat penting dalam forensik digital. Jika sangat penting untuk menjaga integritas bukti selama penyelidikan. Untuk forensik seluler, langkah-langkah di bawah ini adalah praktik yang baik untuk diikuti:

- Ada kemungkinan penyerang dapat menghapus data dari jarak jauh atau aktivitas baru apa pun dapat menimpa data yang ada. Jadi, langkah pertama adalah mengisolasi perangkat seluler dari jaringan.
- Ada beberapa cara yang bisa diikuti sesuai skenario,
- Melepaskan kartu SIM
- Beralih ke mode Pesawat
- Gunakan Tas Faraday atau Jammer
- Chain of Custody – Chain of Custody adalah dokumen untuk menjaga setiap rekaman bukti digital dari pengumpulan hingga presentasi. Ini mencakup detail seperti no seri, no kasing, no loker,
- Nama penyidik, waktu dan tanggal setiap tahapan, Rincian pengangkutan barang bukti. Ini penting karena melacak bukti Digital.
- Hashing – Hashing adalah metode yang digunakan untuk membuktikan integritas bukti. MD5 atau SHA adalah algoritma yang banyak digunakan untuk menghitung nilai Hash dari bukti. Seperti disebutkan sebelumnya, hampir tidak mungkin untuk berinteraksi dengan perangkat seluler tanpa mengubahnya. Tapi kita bisa menghitung nilai hash dari data yang diekstraksi melalui ekstraksi logis atau file gambar yang diekstraksi melalui ekstraksi fisik.

Akuisisi

Ada tiga metode yang digunakan untuk ekstraksi data dari perangkat iOS. Tinjauan di bawah ini telah diberikan tentang masing-masing.

- Fisik – Ini adalah salinan perangkat sedikit demi sedikit dan memungkinkan pemulihan data yang dihapus. Sayangnya, dengan mobile forensic selalu tidak memungkinkan untuk menggunakan metode ini.
- Sistem file – Metode ini akan mengekstrak file yang terlihat di tingkat sistem file.
- Logis – Metode ini memungkinkan untuk mengekstrak file tertentu dari sistem file seperti cadangan yang diambil menggunakan iTunes

Terkadang perlu melakukan teknik ofensif seperti cracking password, Jail Breaking.

Perangkat iOS dan sistem file

Apple mengembangkan sistem operasi untuk iPhone, iPad dan iPod Touch yang dikenal sebagai sistem operasi IOS. Perangkat yang berjalan pada sistem operasi IOS disebut perangkat IOS.

Sistem file HFS+

Apple mengembangkan Hierarchical File System (HFS) yang menyediakan kumpulan data besar. Disk yang diformat dengan HFS memiliki Blok 512-byte pada tingkat Fisik.

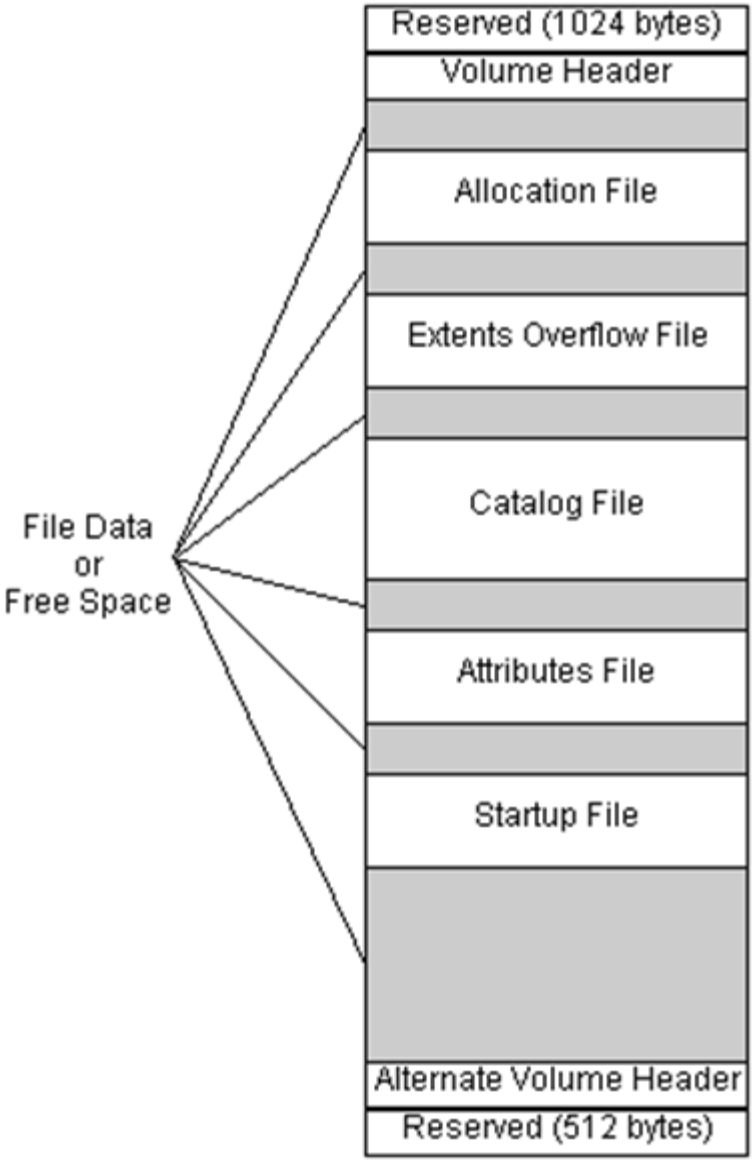
Ada dua jenis Blok di HFS.

Blok Logis, yang diberi nomor dari pertama hingga terakhir dalam volume. Mereka juga berukuran 512 byte sama dengan blok fisik.

Blok alokasi adalah sekelompok blok logis yang digunakan untuk melacak data. Blok alokasi selanjutnya dikelompokkan bersama yang disebut rumpun untuk mengurangi fragmentasi pada volume.

HFS menggunakan waktu absolut (waktu lokal) serta waktu UNIX sehingga seseorang dapat mengidentifikasi lokasi sistem.

Sistem file HFS menggunakan sistem file katalog untuk mengatur data. Ini menggunakan struktur B * tree (Balanced tree) untuk mengatur data. Pohon terdiri dari node. Saat data ditambahkan atau dihapus, algoritme dijalankan untuk menjaga keseimbangan.



Gambar 1. Struktur sistem file HFS+

Seperti yang terlihat pada gambar di atas, 1024 byte pertama adalah blok boot yang dicadangkan.

- Volume Header: Berisi informasi tentang struktur HFS Volume. Itu melacak Penomoran ID Katalog dan meningkatkannya satu setiap kali file ditambahkan. Header volume HFS+ juga berisi tanda tangan "H+."
- File alokasi: Ini melacak blok alokasi yang digunakan oleh sistem file. Ini pada dasarnya termasuk bitmap. Setiap bit mewakili status blok alokasi. Jika diset ke 1, itu berarti Blok alokasi digunakan, dan jika 0, itu berarti blok alokasi tidak digunakan.
- Extent Overflow file: Ini terdiri dari penunjuk sejauh mana. Jika file lebih besar dari delapan blok alokasi yang berdekatan, maka file tersebut menggunakan luasan.

- File Katalog: Ini mengatur data menggunakan sistem pohon seimbang seperti yang disebutkan sebelumnya. Ini digunakan untuk menemukan lokasi file atau folder di dalam volume. Itu juga berisi metadata file, termasuk tanggal pembuatan dan modifikasi serta izin.
- File Atribut: Berisi atribut file yang dapat disesuaikan.
- File Startup: Ini membantu sistem booting yang tidak memiliki dukungan ROM bawaan.
- Data aktual disimpan dalam sistem file dan dilacak oleh sistem file.
- Header Volume Alternatif: Ini adalah header Volume Cadangan yang terletak di 1024 byte terakhir dari volume. Panjangnya 512 byte.
- 512 Byte terakhir dicadangkan.
- Sistem Berkas HFSX

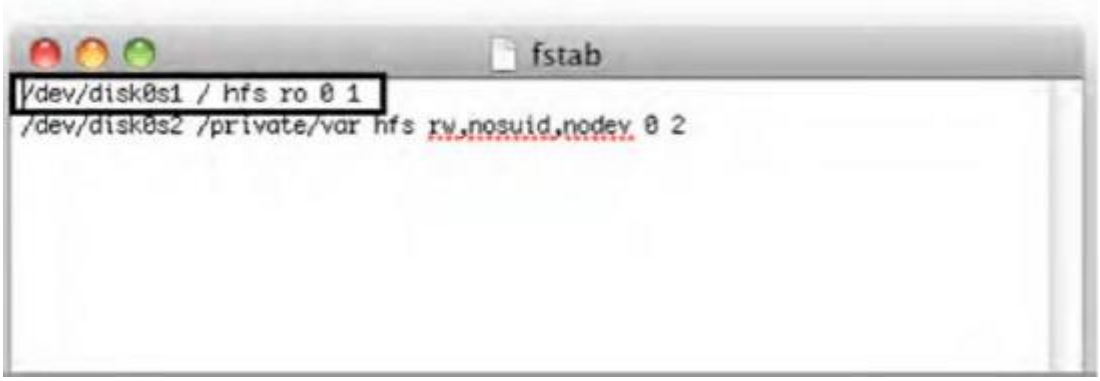
Sistem file HFSX adalah variasi dari sistem file HFS+ yang digunakan di perangkat seluler Apple. Hanya ada satu variasi yaitu peka terhadap huruf besar-kecil dan memungkinkan memiliki dua file dengan nama yang mirip tetapi huruf besar-kecil berbeda.

Partisi

Perangkat iOS memiliki dua jenis partisi. Partisi sistem dan Partisi Data

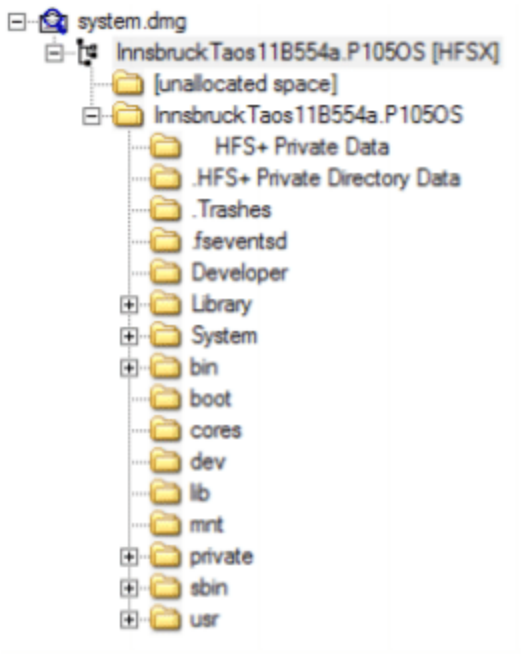
Partisi Sistem

Partisi sistem tidak berisi lebih banyak artefak yang terkait dengan penyelidikan karena sebagian besar berisi informasi terkait sistem seperti sistem operasi iOS dan aplikasi pra-instal. Partisi sistem adalah Read-only seperti yang terlihat pada output Private/etc./fstab di bawah ini.



Gambar 2. Fstab

IPhone memiliki satu disk, oleh karena itu dilambangkan sebagai Disk0. Partisi sistem adalah Disk0s1, dan Partisi Data adalah Disk0s2.



Gambar 3. Partisi Sistem

Kita dapat menemukan kata sandi yang dikonfigurasi pengguna dari file /private/etc./passwd seperti yang ditunjukkan di bawah ini.

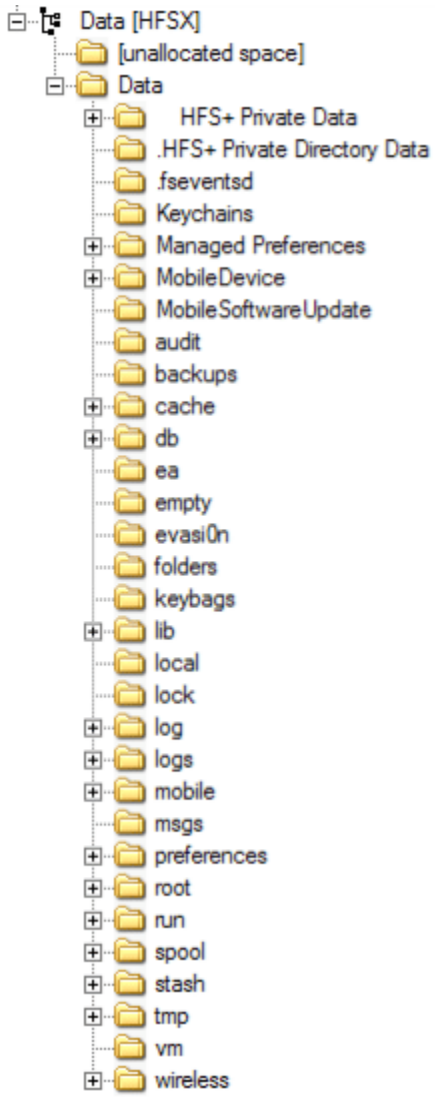

```
##
# User Database
#
# This file is the authoritative user database.
##
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:/smx7MYTQIi2M:0:0:System Administrator:/var/root:/bin/sh
mobile:/smx7MYTQIi2M:501:501:Mobile User:/var/mobile:/bin/sh
```

Gambar 4. File sandi

Seperti yang terlihat pada tangkapan layar di atas, hash kata sandi seluler dan root dapat diambil dari file passwd. Selanjutnya dengan menggunakan alat pembobol kata sandi seperti "John the Ripper" orang bisa mendapatkan kata sandinya. Kata sandi root adalah "Alpine" dan merupakan default untuk semua perangkat iOS.

Partisi Data

Partisi data berisi data pengguna dan dapat memberikan banyak artefak selama penyelidikan. Ini adalah partisi Baca/Tulis. Struktur partisi ini telah diubah dengan versi iOS yang berbeda. Di bawah ini adalah tangkapan layar dari perangkat iOS yang berjalan di iOS 7.



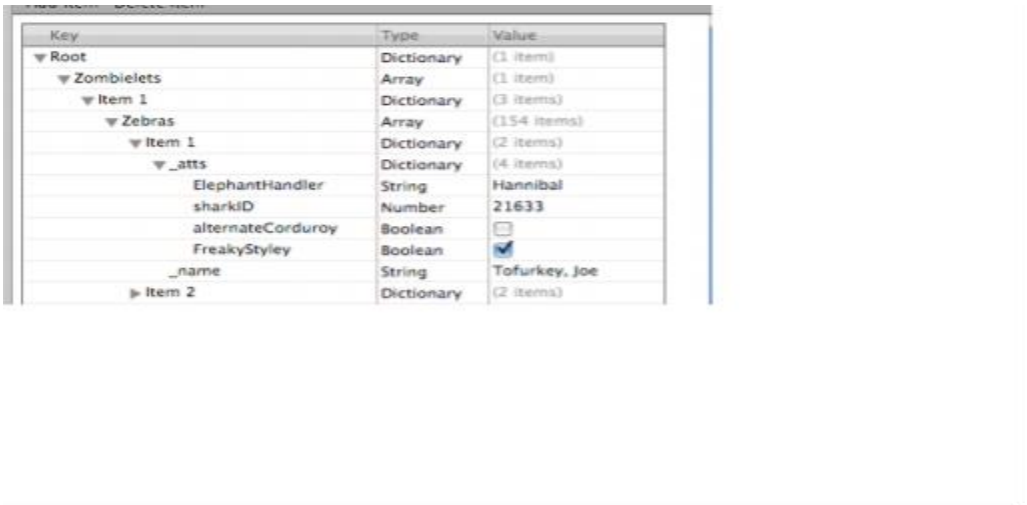
Gambar 5. Partisi Data

Direktori di bawah ini terdaftar yang mungkin menarik untuk artefak.

- Keychains – Keychain.db, yang berisi kata sandi pengguna dari berbagai aplikasi
- Log – General.log: Versi OS dan nomor seri, Lockdown.log – Log Daemon Lockdown

- Seluler – Data Pengguna
- Preferensi – konfigurasi sistem
- Jalankan – log sistem
- Tmp -manifest.Plist: Pencadangan Plist.
- Root – Cache, Lockdown, dan Preferensi
- File Daftar Properti

Daftar properti adalah file XML yang digunakan dalam pengelolaan konfigurasi OS dan aplikasi. File-file ini berisi artefak berguna yang terkait dengan cookie web, akun email, rute Peta GPS dan preferensi konfigurasi sistem pencarian, riwayat penelusuran, dan bookmark. File-file ini dapat dibuka untuk editor teks sederhana untuk melihat isinya.



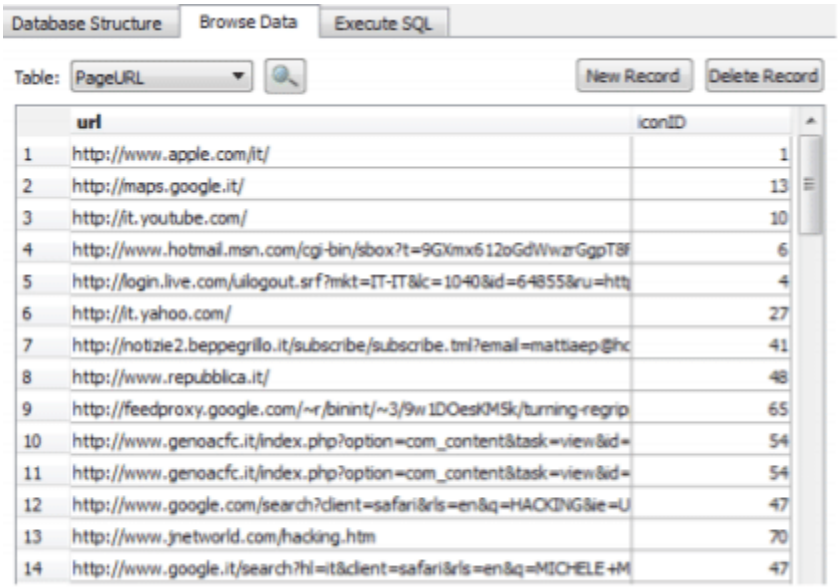
Gambar 6. Plist

Database SQLite

Ekstraksi logis dari iPhone dapat menyediakan banyak file database SQLite karena menggunakan database SQLite untuk menyimpan data pengguna, alat browser SQLite digunakan untuk menjelajahi dan membaca database SQLite yang dapat diunduh dari http://sqlitebrowser.org/

Tiga database utama adalah Call History, Address Book, dan database SMS.

Basis data ini dapat diekstraksi melalui aplikasi yang tersedia seperti Peramban basis data SQLite seperti yang terlihat pada gambar di bawah.



	url	iconID
1	http://www.apple.com/it/	1
2	http://maps.google.it/	13
3	http://it.youtube.com/	10
4	http://www.hotmail.msn.com/cgi-bin/sbox?t=9GXmx612oGdWwzrGgpT8f	6
5	http://login.live.com/uilogout.srf?mkt=IT-IT&lc=1040&id=64855&ru=htt	4
6	http://it.yahoo.com/	27
7	http://notizie2.beppegrillo.it/subscribe/subscribe.tml?email=mattiaep@hc	41
8	http://www.repubblica.it/	48
9	http://feedproxy.google.com/~r/binint/~3/9w1DOesKMSk/turning-regrip	65
10	http://www.genoacfc.it/index.php?option=com_content&task=view&id=	54
11	http://www.genoacfc.it/index.php?option=com_content&task=view&id=	54
12	http://www.google.com/search?client=safari&rls=en&q=HACKING&ie=U	47
13	http://www.jnetworld.com/hacking.htm	70
14	http://www.google.it/search?hl=it&client=safari&rls=en&q=MICHELE+M	47

Gambar 7. Browser Basis Data SQLite