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	:	EC00202339980, 31 Mei 2023
Pencipta		
Nama	:	**Drs. Ir. Faisal Syafar, M.Si., M.InfTech., Ph.D., IPU.**
Alamat	:	Kompleks 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	:	**Logical Acquisition Of IoS Devices**
Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia	:	31 Mei 2023, di Makassar
Jangka waktu pelindungan	:	Berlaku selama 50 (lima puluh) tahun sejak Ciptaan tersebut pertama kali dilakukan Pengumuman.
Nomor pencatatan	:	000472901

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.

METODE PENGAMBILALIHAN PERANGKAT IOS-LOGICAL ACQUISITION

Identifikasi telepon

Selama penyelidikan dan penyitaan, pemeriksa perlu mengidentifikasi model Telepon.

• Salah satu caranya adalah dengan memeriksa bagian belakang perangkat yang berisi nomor model yang tercetak

Gambar 1. Nomor model tercetak di bagian belakang perangkat

• Pendekatan lain adalah menghubungkan iPhone ke workstation forensik. Instal perpustakaan libimobiledevice di workstation Anda, ini mendukung Windows, MAC dan Linux hingga 10.3 dapat diunduh dari URL http://www.libimobiledevice.org/ langkah-langkah instalasi secara rinci dijelaskan di sini http://krypted.com/ mac-os-x/use-libimobiledevice-to-view-ios-logs/

• Terlepas dari Telepon terkunci atau tidak terkunci; beberapa informasi dapat dikumpulkan tentang iDevice yang terhubung menggunakan perintah ideviceinfo seperti yang ditunjukkan pada tangkapan layar di bawah ini.

Gambar 2. iDeviceinfo

Seperti yang terlihat pada gambar di atas, kami dapat mengekstrak informasi penting berikut tentang iDevice

Kelas Perangkat, Nama Perangkat, Alamat WiFi, Kemampuan Telepon, dan Model Perangkat Keras, versi iOS

Mode pengoperasian perangkat iOS

Perangkat iOS dapat dioperasikan dalam tiga mode. 1) Mode normal 2) Mode pemulihan dan 3) Mode DFU. Pemeriksa atau Penyelidik harus menyadari mode ini karena pengetahuan ini diperlukan untuk memutuskan selama investigasi bahwa perangkat mode mana yang harus dioperasikan untuk mengekstraksi data atau ekstraksi data yang efisien.

Mode normal

Saat iPhone dinyalakan, iPhone melakukan booting dalam sistem operasi, ini adalah mode normal. Dalam mode normal, pengguna dapat melakukan semua aktivitas rutin.

Proses boot mode normal terdiri dari tiga langkah: Bootloader Tingkat Rendah, iBook, dan kernel iOS. Langkah-langkah boot ini ditandatangani untuk menjaga integritas proses.

Mode pemulihan

Perangkat masuk ke mode pemulihan jika selama proses boot normal jika ada langkah yang gagal memuat atau memverifikasi. Tangkapan layar di bawah ini menunjukkan layar selama mode pemulihan.

Gambar 3. Layar selama mode Pemulihan

Mode ini digunakan untuk melakukan upgrade atau restore perangkat iPhone. iPhone bisa masuk ke recovery mode dengan mengikuti langkah-langkah di bawah ini:

• Matikan perangkat dengan menahan tombol daya di bagian atas perangkat

• Tahan tombol home telepon dan sambungkan ke komputer menggunakan kabel USB

• Tetap tahan tombol home sampai Connect ke layar iPhone tidak muncul dan kemudian tombol home bisa dilepaskan.

• Nyalakan ulang perangkat untuk keluar dari mode pemulihan

modus DFU

Mode Peningkatan Firmware Perangkat digunakan untuk melakukan peningkatan iOS, dan ini adalah mode tingkat rendah untuk diagnosis. Saat boot up, jika Boot ROM tidak dimuat atau diverifikasi, maka iPhone menampilkan layar Hitam.

Ponsel harus dalam mode DFU saat menggunakan sebagian besar teknik akuisisi. Langkah-langkah di bawah ini perlu dilakukan untuk memasukkan iPhone dalam mode DFU.

• Instal iTunes di stasiun kerja Forensik dan sambungkan Ponsel ke stasiun kerja forensik menggunakan USB.

• Matikan Telepon

• Tahan tombol daya selama 3 detik

• Tahan tombol home dengan tombol power tahan selama 10 detik

• Lepas tombol power dan tahan tombol home tetap tidak ada pemberitahuan di iTunes bahwa iPhone dalam mode recovery telah terdeteksi oleh iTunes.

Melanggar kode sandi

Ada berbagai metode untuk memecahkan kode sandi iOS. Tergantung pada versi IOS pilih metode yang sesuai. Ada berbagai alat yang dapat melakukan aktivitas tersebut seperti IP-Box, alat pemulihan kunci UFED sebagai alat komersial dan skrip python di sumber terbuka. Kami akan mendemonstrasikan beberapa metode untuk memecahkan kode sandi untuk iOS.

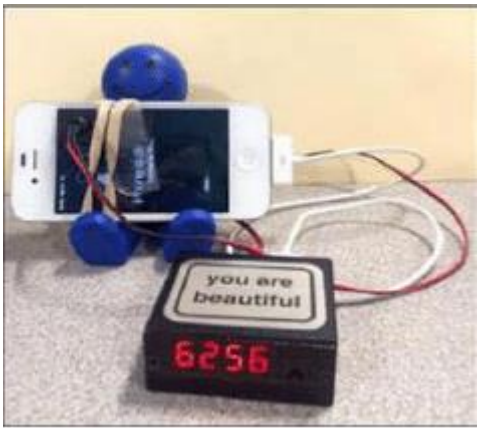
Menggunakan IP-Box untuk memecahkan kode sandi Telepon

Jika perangkat dikunci menggunakan kode sandi empat digit, maka ada beberapa alat yang tersedia yang dapat memecahkan kode sandi ini.

Perangkat IP-BOX melakukan tugas serupa untuk informasi lebih lanjut Anda dapat mengunjungi URL

IP-BOX didukung untuk perangkat hingga iOS versi 8.1.2. Kit ini berisi Box, kabel iPhone, kabel USB, perangkat lunak IP-BOX yang digunakan untuk mengonfigurasi pola dan menggunakan firmware IP-BOX yang dapat diperbarui.

IP-BOX setelah terhubung ke iPhone seperti yang ditunjukkan pada gambar di bawah ini, itu akan mengirimkan kode sandi yang telah ditentukan sebelumnya ke telepon. Kode-kode ini dari 0000 hingga 9999. Tangkapan layar di bawah ini menunjukkan kode sandi iPhone yang terdeteksi menggunakan IP-BOX



Gambar 4. Passcode terdeteksi menggunakan IP-BOX

Menggunakan skrip Python ke kode sandi Bruteforce

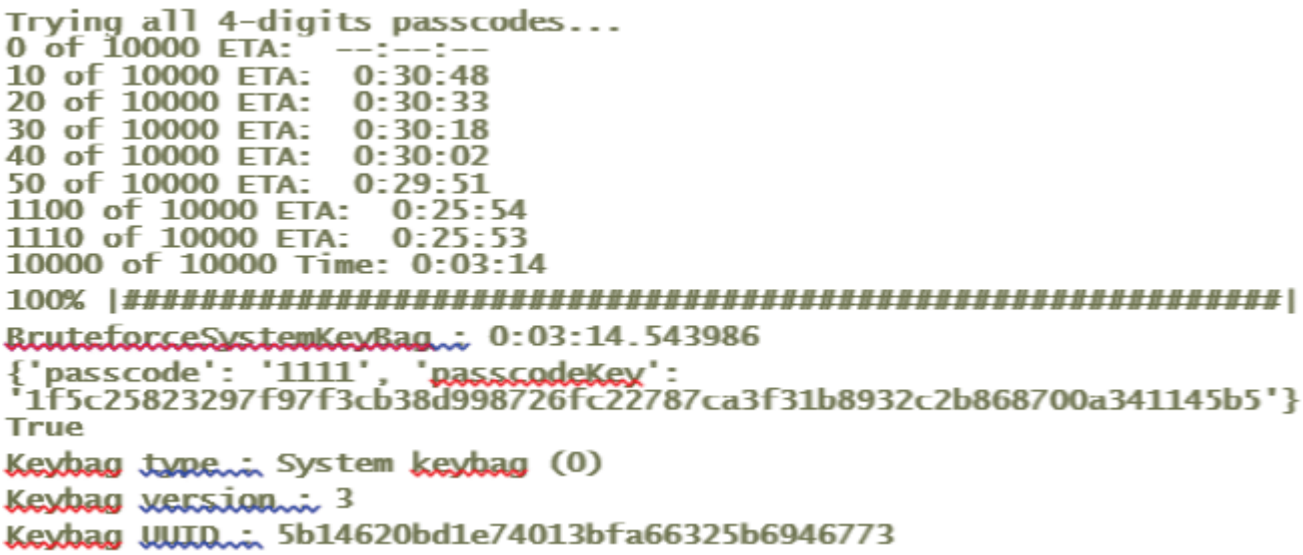
Melakukan serangan Bruteforce pada iPhone pada level batu loncatan dapat menyebabkan penghapusan data di dalam ponsel. Tetapi mekanisme perlindungan ini tidak diterapkan pada ekstensi kernel. Beberapa alat dapat mengakses workstation forensik tempat iPhone terhubung dan dapat melakukan serangan brute force dengan mengakses kunci pasangan melalui file escrow untuk mendekripsi telepon.

Untuk melakukan pemeriksa ini bisa mengikuti langkah-langkah di bawah ini:

• Hubungkan iPhone ke sistem Mac

• Dapatkan file script dari link dan jalankan script python

Skrip ini berkomunikasi dengan disk RAM di Telepon melalui Tcprelay.py dengan port terbuka 1999. Ini membuang kunci perlindungan data ke direktori bernama UDID oleh Brute memaksa kode sandi sistem dan mendekripsi Kantong Kunci Sistem. Menjalankan skrip akan memberikan hasil seperti yang ditunjukkan di atas. Sekarang untuk memaksa kita perlu menekan enter seperti yang disebutkan oleh skrip.



Gambar 5. Script Bruteforce performed

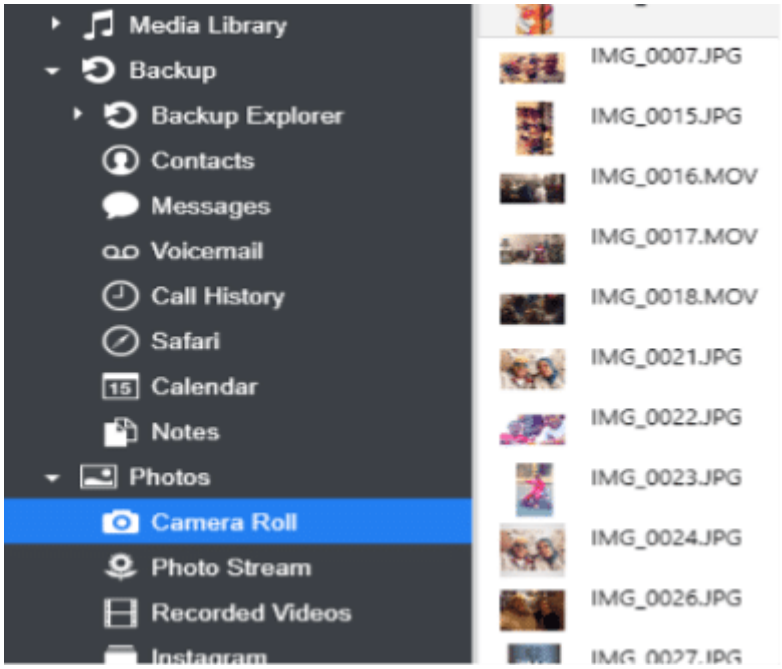
Pemulihan Kode Kunci Pengguna UFED

Ini adalah alat komersial yang dilisensikan di bawah Cellebrite yang menggunakan teknik yang sama seperti IP-BOX. Diperlukan kabel dan kamera untuk merasakan layar Ponsel yang terhubung. Sesuai tangkapan layar di bawah, ini dapat memecahkan kode sandi perangkat iOS dan juga Android.

Gambar 6. Alat Pemulihan Kode Kunci Pengguna UFED

Akuisisi langsung

Peramban iDevice dapat digunakan untuk memperoleh data secara langsung jika ponsel tidak terkunci atau sertifikat penguncian diketahui. Ini adalah metode yang sangat sederhana karena saat menghubungkan ponsel ke workstation forensik, Browser iDevice mencantumkan file seperti yang ditunjukkan di bawah ini.



Gambar 7. Browser iDevice

Perangkat lunak semacam itu bekerja pada platform forensik yang berarti mereka dapat mengubah data atau secara tidak sengaja mengesampingkan bukti. iMazing, iFunBox, iExplorer, Wondershare Dr. Fone adalah alat yang menggunakan perpustakaan dari iTunes sehingga memerlukan versi iTunes yang diperbarui. Alat-alat ini berjalan pada platform Windows atau MAC. Sebelum menghubungkan iPhone ke perangkat, pastikan opsi penyelarasan otomatis diaktifkan di iTunes.

Metode ini adalah cara yang sangat sederhana untuk menyalin data menggunakan browser. Seseorang dapat menggunakan metode akuisisi logis menggunakan browser iDevice sebagai alternatif, dan itu tergantung pada skenarionya. Alat lain yang dapat melakukan akuisisi logis dijelaskan di bawah ini.

Akuisisi logis

Akuisisi logis dapat dilakukan dengan bantuan berbagai alat komersial seperti Oxygen Forensic Suite, UFED physical analyzer, Cellebrite, Blacklight, XRY. Kami akan mendemonstrasikan Akuisisi Logis dengan bantuan rangkaian oksigen forensik dan alat penganalisa fisik UFED di bawah ini.

Akuisisi Logis menggunakan Oxygen Forensic Suite

Menggunakan Oxygen Forensic Suite yang merupakan alat komersial, kami dapat melakukan akuisisi logis terhadap iPhone. Langkah-langkah seperti yang dijelaskan di bawah ini

• Luncurkan Oxygen Forensic Suite. Pilih opsi Sambungkan perangkat untuk memulai ekstraksi.

• Ini akan meminta untuk memilih menghubungkan perangkat secara otomatis atau menghubungkan perangkat secara manual. Disarankan untuk menggunakan opsi Pertama yang menghubungkan telepon secara otomatis. Suite oksigen forensik akan mulai mencari telepon setelah memilih opsi koneksi otomatis.

• Perangkat lunak akan memberikan UUID dari ponsel yang terdeteksi dan jika ponsel dilindungi kata sandi dan dikunci, ia akan meminta untuk memberikan kata sandi atau sertifikat penguncian.

Seperti yang ditunjukkan pada gambar di bawah ini, jika kata sandi diketahui maka pemeriksa harus memasukkan dan mengotorisasi kata sandi pada perangkat dan memilih opsi “Saya memasukkan kode sandi. Tekan untuk menghubungkan” atau pilih daftar kuncian.

Gambar 8. Masukkan kode sandi atau pilih sertifikat kuncian

• Setelah koneksi berhasil dibuat, perangkat lunak akan menampilkan informasi tentang perangkat yang terhubung. Informasi tersebut seperti model, nomor IMEI, boot loader, dan informasi versi iOS.

• Jendela berikutnya menyediakan opsi untuk memasukkan data terkait kasus seperti Nama perangkat, Pemilik Perangkat, Nomor Bukti. Itu juga menanyakan kata sandi untuk Cadangan.

• Jendela berikutnya akan memungkinkan memilih jenis data yang ingin diekstrak. Tindakan yang disarankan adalah memilih semua.

Gambar 9. Data yang akan diekstrak

• Software sekarang mulai mengekstrak data, dan pada saat yang sama, mem-parsing data yang diekstraksi. Jika cadangan Telepon dilindungi kata sandi, maka ekstraktor akan meneruskan data ke kit Passware untuk melakukan serangan.

• Jika pemeriksa mengetahui password backup, maka langkah cracking password dapat dilewati oleh pemeriksa dan dapat memberikan password. Jika peretasan kata sandi berhasil maka itu akan mengekstrak semua data dari Cadangan jika tidak hanya data multimedia seperti Gambar, Video yang akan diekstraksi, dan pemeriksa tidak akan dapat memperoleh informasi apa pun tentang aplikasi yang diinstal atau diinstal sebelumnya.