

Achmad Benny Mutiara
***Panduan Komputer Forensik Dalam
Penanganan Bukti Digital Pada Personal Digital
Assistants (PDA)***



Penerbit Universitas Gunadarma

Korespondensi:

Dosen Universitas Gunadarma

Alamat: Jl. Walet No.24, Bogor 16161

Telp: 0251 321796

Hp: 08159116055

e-mail: amutiara@staff.gunadarma.ac.id ,
amutiara@gmail.com

Blog: <http://abmutiara.info/> ,

Kontributor: Irma Widyaningsih mahasiswa bimbingan
penulisan ilmiah, Jurusan Teknik Informatika Universitas
Gunadarma

Kata Pengantar

Sebuah komputer dan alat elektronik lain kini telah hadir disetiap aspek kehidupan modern. Hari ini, sebuah komputer dapat berada dalam telapak tangan kita sendiri. Pada suatu waktu mungkin sebuah komputer tunggal nantinya dapat mengisi keseluruhan ruang. Namun seiring dengan kemajuan teknologi tersebut, banyak sekali teknologi telah dimanfaatkan untuk melakukan kejahatan, seperti penyebaran virus melalui internet, penyebaran video porno, dan sebagainya.

Seperti halnya komputer, sebuah alat elektronik yang digunakan untuk melakukan kejahatan dapat berisi bukti kejahatan, dan bahkan dapat menjadi target kejahatan itu sendiri. Pemahaman mengenai aturan dan peran dari bukti elektronik alami inilah yang perlu diperhatikan dalam menangani sebuah peristiwa kejahatan. Pemahaman mengenai bagaimana cara memproses suatu peristiwa kejahatan yang didalamnya berisi bukti elektronik yang penting serta bagaimana seorang agen dapat bereaksi terhadap situasi seperti ini.

Dalam hal ini *Personal Digital Asistants* (PDA) yang merupakan salah satu dari contoh nyata sebuah teknologi berkembang yang terbaru. Dalam penulisan ini akan dijelaskan tiga keluarga dari PDA *device* yang sering dipakai, seperti *Pocket PC*, *Palm OS*, dan PDA berbasis Linux serta karakteristik dari sistem operasi mereka yang saling terhubung. Penulisan ini juga akan mendiskusikan prosedur yang harus dilalui dalam menangani permasalahan bukti digital, antara lain: *preservation* (pemeliharaan), *acquisition* (perolehan), *examination* (pengujian), *analysis* (analisa), dan *reporting* (pelaporan) tentang informasi digital yang disajikan pada PDA, seperti tersedianya perangkat lunak *forensic tools* yang mendukung aktivitas tersebut.

Penulisan buku ini dapat bertindak sebagai suatu *guidelines* untuk menjawab pertanyaan dari sikap yang cukup rumit tersebut. Dalam suatu peristiwa kejahatan digital, suatu responder pertama mungkin bertanggung jawab dalam prosedur *recognition* (pengenalan), *collection* (pengumpulan), *preservation* (pemeliharaan), *transportation* (transportasi), dan penyimpanan bukti elektronik.

Hal ini dapat dilakukan oleh hampir semua orang yang sedang berada dalam pelaksanaan hukum profesi. Seorang pegawai dapat menggunakan alat elektronik selama tugas mereka sehari-hari. Seorang penyelidik dapat mengarahkan pengumpulan bukti

elektronik dan dapat melakukan pengumpulan bukti dengan diri sendiri. Pemeriksa forensik dapat menyediakan bantuan pada suatu peristiwa kejahatan dan dapat melakukan pengujian pada bukti tersebut. Para manajer mempunyai tanggung jawab dalam memastikan bahwa personil yang berada dibawah arahan mereka cukup terlatih dan dilengkapi dengan peralatan yang baik dalam hal penanganan bukti elektronik. Setiap responder dapat memahami bukti elektronik yang rapuh dan prosedur serta prinsip yang berhubungan dengan pengumpulan dan pemeliharaan sebuah bukti. Segala tindakan yang berpotensi untuk mengubah, merusak, atau menghancurkan bukti asli nantinya akan lebih diteliti di lapangan.

Prosedur pada dasarnya adalah untuk mengarahkan proses penyelidikan dari sebuah peristiwa kejahatan elektronik. Para personil yang terlibat dari awal harus dilengkapi dengan teknik dan pelatihan yang berkelanjutan.

Seringkali, kasus tertentu akan membutuhkan tingkat keahlian yang lebih tinggi, pelatihan, serta peralatan, dan para manajer harus mempunyai rencana bagaimana cara bereaksi terhadap kasus tersebut. Permintaan untuk menjawab bukti elektronik diharapkan dapat ditingkatkan untuk masa depan yang tidak dapat diduga tersebut. Penggunaan jasa seperti ini akan memerlukan sumber daya yang tepat untuk dialokasikan pada tujuan ini.

Tujuan dari penulisan buku ini ialah memberikan suatu standar panduan (*guide lines*), supaya kita dapat mengambil suatu tindakan yang tepat apabila kita berada pada suatu peristiwa yang membutuhkan penanganan bukti digital didalamnya, ataupun tindakan yang dapat diambil jika kita terlibat dalam bidang pekerjaan tersebut. Karena hal ini merupakan bagian dari proses penanganan bukti digital.

Ucapan terima kasih penulis sampaikan pada Pimpinan Universitas Gunadarma, Mahasiswa Teknik Informatika, serta isteri dan anak-anakku tercinta, karena atas dorongan dan semangat dari mereka buku ini tertulis.

Buku ini masih jauh dari sempurna. Kritik dan saran yang membangun dapat para pembaca sampaikan ke penulis.

Semoga buku ini bermanfaat bagi para ahli di bidang teknologi informasi yang berminat pada bidang spesifik forensik digital. Amin.

Depok, 2007

Penulis
ABM

DAFTAR ISI

RINGKASAN EKSEKUTIF	7
1. PENGENALAN	8
1.1 OTORITAS	8
1.2 LINGKUP DAN TUJUAN	8
1.3 PENDENGAR DAN ASUMSI	9
1.4 STRUKTUR DOKUMEN	10
2. LATAR BELAKANG	11
2.1 KARAKTERISTIK DEVICE	11
2.2 PALM OS	14
2.3 POCKET PC	17
2.4 LINUX	21
2.5 STATUS GENERAL ATAU UMUM	24
3. FORENSIC TOOLS	27
3.1 PALM DD (PDD)	28
3.2 PILOT-LINK	29
3.3 POSE	29
3.4 PDA SEIZURE	30
3.5 ENCASE	31
3.6 DUPLICATE DISK (DD)	31
3.7 MISCELLANEOUS TOOLS	32
4. ATURAN DAN PROSEDUR	34
4.1 ATURAN – ATURAN DAN TANGGUNG JAWAB	34
4.2 PRINSIP – PRINSIP DALAM PEMBUKTIAN	35
4.3 MODEL – MODEL PROSEDUR	37
5. PEMELIHARAAN	41
5.1 PENCARIAN	43
5.2 PENGENALAN	44
5.3 DOKUMENTASI	45
5.4 KOLEKSI	46
5.4.1 EXACERBATING CONDITIONS / KONDISI YANG BURUK	48
5.4.2 MODIFIKASI DEVICE	50
5.4.3 TRANSPORTASI DAN MEDIA PENYIMPANAN	51
6. AKUISISI	53

6.1 UNOBSTRUCTED DEVICE (DEVICE YANG TIDAK DIHALANGI)	55
6.2 OBSTRUCTED DEVICES (DEVICE YANG DIHALANGI)	58
6.2.1 METODE INVESTIGASI	58
6.2.2 METODE SOFTWARE-BASED	59
6.2.3 METODE HARDWARE-BASED	60
6.3. TANGENTIAL EQUIPMENT	62
6.3.1 SYNCHED DEVICES	63
6.3.2 MEMORY CARDS	64
6.3.3 USB MEMORY DRIVES	67
 7. PENGUJIAN DAN ANALISIS	 69
 7.1 LOKASI BUKTI	 70
7.2 PENERAPAN TOOLS	71
 8. PELAPORAN	 76
 9. CONTOH PENERAPAN	 78
 9.1 BUKTI ELEKTROIK	 78
9.2 PROSES FORENSIK	78
9.3 PENANGANAN BUKTI ELEKTRONIK	79
9.4 PROSEDUR DAN PRINSIP DALAM PENANGANAN BUKTI	80
9.4.1 ATURAN DAN TANGGUNG JAWAB	80
9.4.2 PRINSIP – PRINSIP DALAM BUKTI DIGITAL	81
9.4.3 MODEL – MODEL PROSEDUR	82
9.5 PRESERVATION (PEMELIHARAAN)	84
9.5.1 PENCARIAN	87
9.5.2 PENGENALAN	87
9.5.3 DOKUMENTASI	88
9.5.4 PENGUMPULAN	89
9.5.5 BERBAGAI KONDISI DALAM KOLEKSI	90
9.6 ACQUISITION (PEROLEHAN)	91
9.6.1 DEVICE TANPA HALANGAN	94
9.6.2 DEVICE YANG DIHALANGI	96
9.7 PENGUJIAN DAN ANALISIS	102
9.7.1 LOKASI BUKTI	103
9.7.2 PENGGUNAAN TOOL	105
9.8 REPORTING (PELAPORAN)	109
9.9 RINGKASAN PADA PDA SEIZURE	110
9.9.1 LANGKAH ACQUISITION	113
9.9.2 FUNGSI PENCARIAN	114
9.9.3 GRAPHICS LIBRARY	116
9.9.4 BOOKMARKING	116
9.9.5 ADDITIONAL TOOLS	117
9.9.6 REPORT GENERATION	118
9.9.7 PASSWORD CRACKING	119
DAFTAR PUSTAKA	121
APENDIKS A	122
APENDIKS B	124

Ringkasan Eksekutif

Personal Digital Asistants (PDA) merupakan suatu perwujudan teknologi terbaru, tidak seperti biasa yang didapat didalam komputer forensik klasik. Panduan ini mencoba menjembatani sebuah *gap* dengan menyediakan tampilan kedalam PDA dan menjelaskan teknologi yang terlibat serta hubungan PDA ke prosedur forensik. Panduan ini akan menjelaskan tiga keluarga dari *device* - *Pocket PC*, *Palm OS*, dan PDA berbasis Linux - serta karakteristik dari sistem operasi mereka yang terhubung. Panduan ini juga akan mendiskusikan prosedur untuk *preservation* (pemeliharaan), *acquisition* (perolehan), *examination* (pengujian), *analysis* (analisa), dan *reporting* (pelaporan) mengenai informasi digital yang disajikan pada PDA, seperti tersedianya perangkat lunak *forensic tools* yang mendukung aktivitas tersebut.

Sasaran dari panduan ini ada dua sekaligus : pertama, untuk membantu organisasi meningkatkan kebijakan yang sesuai dan prosedur yang berhubungan dengan PDA, dan untuk menyiapkan spesialis forensik yanga berhubungan dengan situasi baru yang menyertakan PDA apabila mereka ditemui. Panduan ini tidak semuanya termasuk perintah untuk pelaksanaan hukum dan penanganan insiden pada masyarakat. Bagaimanapun, dari penguraian prinsip dan informasi lain yang disajikan, organisasi perlu menemukan panduan yang sangat menolong didalam pengaturan kebijakan dan prosedur.

Informasi didalam panduan ini baik diterapkan dalam konteks teknologi sekarang dan prakteknya. Setiap situasi adalah unik, seperti adanya pengalaman dari spesialis forensik dan *tools* serta fasilitas dalam penyelesaiannya. Pertimbangan dari spesialis forensik harus dilihat berbeda dalam penerapan sebuah prosedur yang diusulkan didalam panduan ini. Keadaan dari suatu kasus individu dan internasional, pemerintah pusat, bagian, peraturan lokal dan kebijakan organisasi khusus memerlukan tindakan selain yang diuraikan didalam panduan ini. Sebagaimana biasa, menutup dan melanjutkan konsultasi dengan dewan mengenai undang-undang adalah disarankan.

1. Pengenalan

1.1 Otoritas

Institut Teknologi Nasional dan Standard (NIST) mengembangkan panduan ini kedalam kemajuan menurut Undang-undang dibawah tanggung-jawab Federal Information Security Management Act (FISMA) 2002, Hukum publik 107-347.

NIST bertanggung jawab untuk mengembangkan standard dan *guidelines*, termasuk persyaratan minimum, untuk menyediakan keamanan informasi yang cukup untuk semua asset dan operasi agen Pemerintah pusat, tetapi standard dan *guidelines* seperti itu seharusnya tidak berlaku bagi sistem keamanan nasional. *Guidelines* ini tetap dengan adanya persyaratan dari Office of Management and Budget (OMB) Lingkar A-130, Bagian 8b(3), "Sistem informasi Pengamanan Agen" seperti dianalisa didalam A-130, Catatan tambahan IV: Analisa Bagian Kunci. Informasi bersifat tambahan disiapkan dalam bentuk A-130, Catatan tambahan III.

Panduan ini telah disiapkan untuk digunakan oleh para agen Pemerintah pusat. Mungkin saja digunakan oleh organisasi Non Pemerintah berbasis sukarela yang tidak melihat hak cipta, meskipun sifatnya diharuskan.

Tidak ada apapun didalam panduan ini yang harus diambil untuk membantah standard dan *guidelines* yang dijadikan wajib dan mengikat para agen Pemerintah pusat oleh Sekretaris Perdagangan di bawah Undang-undang Otoritas, petunjuk inipun ditafsirkan ketika mengubah atau menggantikan otoritas yang ada dari Sekretaris Perdagangan, Direktur OMB, atau pejabat Pemerintah pusat lain.

1.2 Lingkup Dan Tujuan

Panduan ini menyediakan informasi dasar atas *preservation* (pemeliharaan), *examination* (pengujian), dan *analysis* (analisa) dari bukti digital pada PDA, yang pantas dalam pelaksanaan hukum, penanganan insiden, dan jenis penyelidikan lain. Panduan juga memusatkan sebagian besar pada karakteristik dari keluarga-keluarga PDA seperti : *Pocket PC*, *Palm OS*, dan PDA berbasis Linux. Panduan juga mempunyai ketentuan untuk

dipertimbangkan dengan baik sepanjang keadaan suatu penyelidikan peristiwa, mencakup *evidence handling* (penanganan bukti), *device identification* (identifikasi alat), *content acquisition* (perolehan), *documentation* (dokumentasi), and *reporting* (pelaporan).

Panduan dimaksudkan untuk menunjuk ke keadaan umum yang mungkin ditemui oleh staf keamanan dan organisasi pelaksanaan hukum penyidik, menyertakan data digital yang ada pada PDA dan berhubungan dengan media elektronik. Panduan ini juga menerima petunjuk yang ada dan menyelidiki lebih dalam mengenai isu yang berhubungan dengan PDA dan *examination* (pengujian) mereka dan *analysis* (analisa) mereka.

Prosedur dan teknik yang diperkenalkan didalam dokumen ini adalah mengumpulkan hal-hal yang menyangkut petunjuk dan pendapat pengarang yang diambil dari petunjuk forensik yang ada. Penerbitan tidak digunakan sebagai *step-by-step* dalam memandu dalam pelaksanaan suatu penyelidikan forensik yang sesuai apabila berhadapan dengan teknologi baru seperti PDA atau seperti yang dijelaskan oleh penasehat hukum yang resmi. Hal ini bertujuan untuk menginformasikan pembaca mengenai berbagai teknologi dan potensi jalan untuk mendekatinya dari segi pandangan forensik. Pembaca disarankan untuk menerapkan praktek yang direkomendasikan hanya setelah konsultasi dengan manajemen dan pejabat resmi mengenai Undang-undang untuk pemenuhan peraturan dan hukum (yaitu, lokal, bagian, pemerintah pusat, dan internasional) yang lebih mendekati situasi mereka.

1.3 Pendengar dan Asumsi

Pendengar yang diharapkan bervariasi dan terbentang dari tim anggota respon yang menangani suatu peristiwa keamanan komputer ke organisasi pejabat keamanan yang menyelidiki suatu keterkaitan antara karyawan ke pemeriksa forensik yang dilibatkan dalam penyelidikan penjahat. Praktek yang direkomendasikan didalam panduan ini dirancang untuk menyoroti kunci prinsip yang dihubungkan dengan penanganan dan pengujian dari bukti elektronik, secara umum, dan PDA khususnya. Pembaca diasumsikan mempunyai suatu dasar landasan dalam komputer forensik klasik yang menyertakan sistem komputer individu (contohnya, komputer pribadi) dan *network servers*. Oleh karena terjadi perubahan alami *handheld devices* secara konstan dan hubungan *tools* dengan prosedur forensik, pembaca diharapkan untuk mengambil keuntungan yang lain dari sumber daya yang ada, mencakup hal-hal yang didaftarkan didalam panduan ini dan untuk lebih memerinci arus informasi yang sekarang .

1.4 Struktur Dokumen

Panduan ini dibagi menjadi sembilan bagian berikut:

1. Bagian 1 menjelaskan penulis, lingkup dan tujuan, pendengar dan asumsi dari dokumen, dan menguraikan secara singkat strukturnya.
2. Bagian 2 adalah suatu ikhtisar atas PDA, mencakup suatu ikhtisar tentang sistem operasi umum dan bagian operasi umum.
3. Bagian 3 mendiskusikan *tools* forensik PDA sekarang ini dengan tipe jenis *device* yang mereka pakai.
4. Bagian 4 menyediakan keterangan umum pada prinsip dan prosedur yang berlaku bagi PDA forensik.
5. Bagian 5 mendiskusikan pertimbangan untuk pemeliharaan bukti digital yang dihubungkan dengan PDA.
6. Bagian 6 menguji proses pengadaan bukti digital dari PDA, seperti halnya tipe – tipe umum dari jenis peralatan disekitarnya.
7. Bagian 7 garis besar sumber bukti yang umum pada PDA, ciri dan kemampuan *tools* untuk pengujian.
8. Bagian 8 mendiskusikan pelaporan penemuan.
9. Bagian 9 berisi daftar acuan digunakan didalam panduan ini.
10. Catatan tambahan A berisi suatu daftar singkatan yang digunakan dalam panduan ini.
11. Catatan tambahan B berisi suatu daftar kata yang melukiskan terminologi yang digunakan di dalam panduan ini.

2. Latar Belakang

Masyarakat digital forensik menghadapi suatu tantangan untuk tetap berada diatas jika menyangkut teknologi terakhir yang mungkin digunakan untuk membuka petunjuk dalam suatu penyelidikan. *Personal Digital Assistants* (PDA) adalah hal yang biasa didalam masyarakat saat ini, yang digunakan oleh banyak individu untuk keduanya baik yang pribadi dan profesional. PDA berubah dalam disain dan secara terus menerus mengalami perubahan sebagai teknologi yang berkembang dan teknologi baru yang diperkenalkan. Apabila suatu PDA ditemui selama suatu penyelidikan, banyak pertanyaan yang muncul: Apa yang sebaiknya dilakukan untuk *maintaining* (pemeliharaan)? Bagaimana cara PDA ditangani? Seberapa berharga atau berpotensi data pada *device* yang diuji? Kunci untuk menjawab pertanyaan ini adalah pemahaman menyangkut karakteristik perangkat keras dan perangkat lunak PDA.

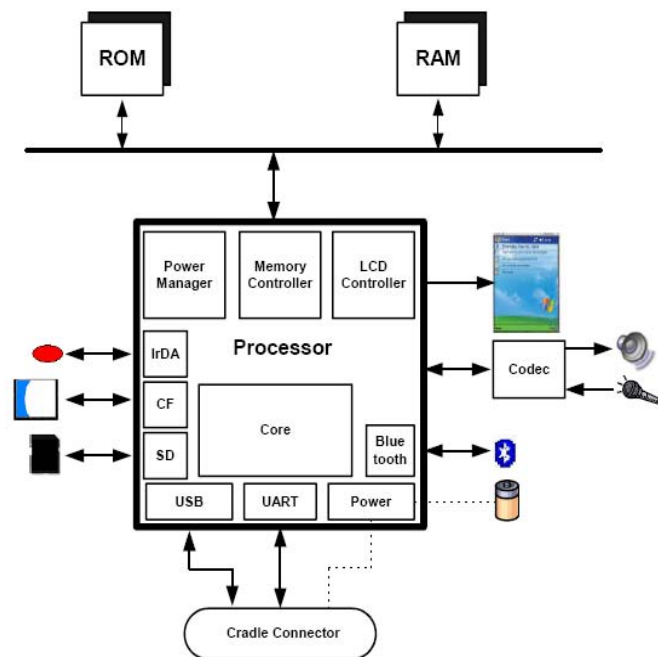
Bagian ini memberi suatu ikhtisar menyangkut kemampuan perangkat keras dan perangkat lunak Palm OS, Pocket PC, dan PDA berbasis Linux. Ikhtisar ini menyediakan suatu ringkasan tentang karakteristik umum dan dimana manfaatnya, berpusat pada perangkat lunak versi atau model tertentu terbaik yang menggambarkan ciri kunci produk. Pengembangan suatu pemahaman menyangkut komponen dan bagian dalam yang aktif dari alat ini (contohnya, organisasi memori dan penggunaannya) adalah suatu prasyarat pemahaman yang terlibat apabila berhadapan dengan perangkat ini secara forensil. Sebagai contoh, memori PDA dulu menyimpan data pemakai yang pada umumnya mudah hilang (yaitu, RAM) dan memerlukan kekuatan lebih untuk memelihara isi, tidak sama dengan *data residing* pada suatu *hardisk* computer pribadi. Teknologi *handheld device* berubah dengan cepat, dengan produksi baru dan ciri yang diperkenalkan secara teratur. Karena langkah yang cepat dimana teknologi *handheld device* sedang berkembang, diskusi ini akan menghadirkan suatu *snapshot* menyangkut area *handheld* di waktu saat ini.

2.1 Karakteristik Device

Kebanyakan jenis PDA mempunyai kemampuan dan ciri yang dapat diperbandingkan.

Rumah mereka adalah suatu *microprocessor*, *read only memory* (ROM), *random access memory* (RAM), dan berbagai kunci perangkat keras dan *interfaces*, dan *touch sensitive, liquid crystal display*. Sistem operasi (OS) *device* ini disimpan di ROM. Beberapa variasi ROM digunakan, mencakup *Flash ROM*, yang dapat dihapus dan diprogramkan kembali secara elektronis dengan membaharui OS atau memberi OS yang berbeda. RAM yang secara normal berisi data pemakai, dijaga tetap aktif oleh baterai yang cepat habis yang dapat menyebabkan semua informasi yang ada dapat hilang.

PDA yang terbaru dengan *system-level microprocessors* dilengkapi dengan dukungan akan *chip* yang diperlukan dan meliputi kapasitas memori yang pantas dipertimbangkan. *Built-In Compact Flash* (CF) dan *combination Secure Digital* (SD), *MultiMedia Card* (MMC) slot pendukung kartu memori dan *peripherals*, seperti kamera digital atau kartu komunikasi *Wireless*. Komunikasi *Wireless* seperti *infrared* (yaitu, IrDa), *Bluetooth*, dan *Wifi* dapat juga dibangun didalam PDA. Gambar 1.1 menggambarkan suatu level sistem pengolah dan komponen inti yang umum pada PDA.



Gamabar 2.1 Diagram Umum Hardware

Device berbeda mempunyai teknis dan karakteristik fisik yang berbeda pula, misalnya, ukuran, berat, kecepatan prosesor, kapasitas memori. *Device* dapat juga menggunakan jenis kemampuan perluasan yang berbeda (contohnya, slot kartu memori dan I/O, *device expansion*

sleeves, dan perangkat keras penghubung eksternal) untuk menyediakan kemampuan tambahan. Selanjutnya, kemampuan PDA kadang dikombinasikan dengan *device* lain seperti telepon selular, *global positioning systems*, dan kamera untuk membentuk jenis *device* baru. Tabel 1.1 menyoroti karakteristik umum dari *Palm OS*, *Pocket PC* (yang di-rebrand seperti **Windows Mobile** tahun 2003), dan model Linux PDA, yang menyoroti keanekaragaman ini. Karakteristik dari suatu jangkauan yang lebih luas pada PDA dapat ditemukan pada pabrik dan *vendor Web sites*, seperti halnya produk yang ditinjau ulang.

	Tungsten T2	iPAQ H5555	Zaurus SL-5600
OS	Palm OS 5.12	Windows Mobile 2003 Premium	Linux Embedix v2.4.18, Qtopia v1.5.0
Processor	144 MHz TI OMAP 1510 Dual Core 192 Mhz DSP Enhanced ARM-based	400 MHz Intel PXA-255 XScale	400 MHz Intel PXA-255 XScale
ROM	8 MB Flash ROM	48 MB Flash ROM (17 MB tersedia untuk <i>user storage</i>)	64 MB Flash ROM (approx. 30-35 MB tersedia untuk <i>user filesystem</i>)
RAM	35 MB SDRAM	128 MB SDRAM	32 MB SDRAM
Size	4.0" Xx 3.0" x 0.6"	5.43" x 3.3" x .63"	5.4" x 2.9" x 0.9"
Display	320x320 Transflective Thin Film Transistor (TFT) LCD, 65,536 warna	240x230 transflective TFT LCD, 65,536 warna	240x230 transflective TFT LCD, 65,536 warna
Text Input	Touch-screen, pengenalan handwriting, soft keyboard	Touch-screen, pengenalan handwriting, soft keyboard	Touch-screen, pengenalan handwriting, memakai tipe QWERTY untuk keyboard
Wireless	IrDa, Bluetooth	IrDa, CIR, Bluetooth, Wi-Fi	IrDa
Card Slot	slot SD/MMC	slot SD/MMC tipe II slot CF	slot SD/MMC tipe II slot CF
Expansion	Tidak ada	Optional expansion sleeves untuk kartu PCMCIA, kartu CF, dan aksesoris	Expansion jacket dengan slot CF, dan baterai USB 1.1 host konektor (mini tipe A)
Baterai	1 baik, Lithium Ion Polymer untuk yang discharge	1 removable, Lithium Ion Polymer untuk yang discharge	1 removable, Lithium Ion Polymer untuk yang discharge

Tabel 2.1 Gambaran dari Representasi Model PDA

Di samping keluarga PDA, semua *device* mendukung satu set aplikasi berbasis dasar Personal Information Management (PIM), yang menyediakan *Address Book*, *Appointment*, *Mailbox*, dan Kemampuan *Memo Management*. Kebanyakan *device* juga menyediakan kemampuan untuk komunikasi secara *wireless*, peninjauan ulang dokumen elektronik, dan *surfing* ke internet. Data PIM yang berada pada PDA dapat disamakan dengan suatu komputer *desktop* dan secara otomatis akan disamakan dan ditiru oleh kedua *device*, dengan menggunakan sinkronisasi protokol seperti protokol **Microsoft's Pocket PC ActiveSync** dan protokol **Palm's HotSync**. Protokol sinkronisasi dapat juga digunakan untuk menukar data lain (seperti, teks individu, gambar, dan format arsip file). Informasi tidak dapat diperoleh secara langsung dari PDA dan terkadang didapat kembali dari suatu komputer pribadi *device* yang telah disamakan.

2.2 Palm OS

Palm berdiri sendiri di pasar PDA dengan membangun *device* disekitar sistem operasinya. Awalnya Palm OS menggunakan 16- dan 32-bit *prosesor* berdasarkan pada keluarga *mikroprosesor* Motorola DragonBall MC68328. *Device* terakhir menggunakan *StrongArm* dan *microprocessors Xscale*. *Device* Palm OS yang lama cenderung menggunakan baterai bersifat alkali sebagai ganti baterai lithium-ion, yang digunakan didalam mode yang baru.

Palm OS dan aplikasi *built-in* disimpan didalam ROM, sedang data pemakai dan aplikasi disimpan didalam RAM. Kegunaan *Add-On* juga ada untuk *membackup* data PIM (seperti, Alamat, Tanggal, *To Do List*, *Memo Pad*) kedalam ROM yang tersedia. Sistem perangkat lunak Palm OS secara logika mengorganisir ROM dan RAM kedalam satu *handheld device* atau lebih modul memori yang dikenal sebagai kartu. Masing-Masing kartu memori dapat berisi ROM, RAM, atau keduanya. Suatu *handheld device* dapat mempunyai satu kartu, banyak kartu, atau bahkan tanpa kartu. Deretan aplikasi yang utama dilengkapi dengan masing-masing *power handheld* Palm OS yang dibangun kedalam ROM. Disain ini memungkinkan pemakai untuk menggantikan sistem operasi dan keseluruhan deretan aplikasi dengan penerapan modul penggantian tunggal. Tambahan atau perluasan sistem dan aplikasi penggantian dapat terisi ke dalam RAM.

Palm OS membagi total RAM yang tersedia kedalam dua area logis: *dynamic* RAM dan *storage* RAM. *Dynamic* RAM digunakan sebagai ruang kerja untuk alokasi temporer, dan sebagai analisator RAM yang di *install* didalam suatu sistem *desktop*. Sisa dari RAM terdapat pada kartu yang ditunjuk *storage* RAM dan dianalisator ke disk penyimpanan pada suatu sistem *desktop*. Karena tenaga power selalu diberikan ke sistem memori, kedua area RAM mempertahankan muatan mereka apabila *device* diputar "**off**" (yaitu, dalam keadaan *low-power*). Semua memori penyimpanan dipertahankan bahkan ketika *device* dinyalakan lagi (yaitu, dengan menekan tombol reset secara manual untuk melakukan *booting*). Sebagai bagian dari *booting* (yaitu, sebuah *soft reset*), sistem perangkat lunak me-*reinitializes* area yang dinamis, dan meninggalkan area penyimpanan tetap utuh. Keseluruhan area *dynamic* RAM digunakan untuk menerapkan koleksi tunggal dari area penyimpanan cuma-cuma atau *heap* yang menyediakan memori untuk alokasi yang dinamis seperti *variabel* global, sistem *buffer* (seperti, TCP/IP, komunikasi IrDa), dan aplikasi *stack*. *Storage* RAM diatur seperti satu atau lebih tumpukan *storage* untuk menjaga data pemakai yang *non-volatile*. Tumpukan

storage dapat juga berbasis ROM. Sebagai bagian dari *cold boot* (yaitu, sesuatu *hard reset*), sebagai tambahan terhadap area *reinitializing* RAM yang dinamis, area *storage* barang dihapus.

Memori penyimpanan Palm OS diatur didalam potongan yang disebut "arsip" yang mana dikelompokkan kedalam "database." "Database" Palm OS dapat dikira sebagai file. Format file Palm OS (PFF) menyesuaikan diri menjadi salah satu dari ke tiga jenis yang digambarkan di bawah :

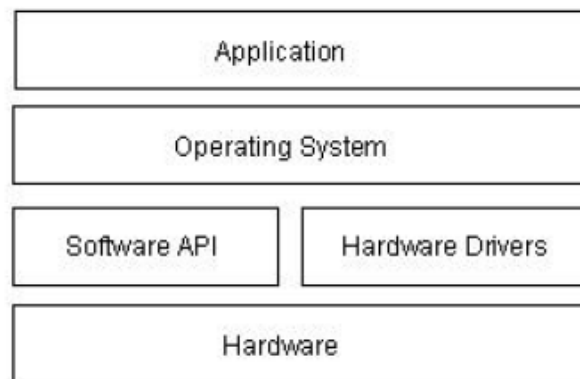
- 1 **Palm Database** - Suatu *record* database untuk menyimpan data aplikasi, seperti daftar kontak, atau data pemakai spesifik.
- 2 **Palm Resource** - Suatu database yang serupa **Palm Database** yang berisi kode aplikasi dan objek penghubung pemakai.
- 3 **Palm Query Application** - Suatu database yang berisi isi dari *world-wide-web* untuk penggunaan dengan **Palm wireless device**.

Dengan Palm OS, semua aplikasi berbagi *dynamic* RAM yang sama, mereka dapat bertentangan data satu sama lain. Serangan *Buffer overflow* juga dengan mudah diterapkan.

Palm OS terbaru menawarkan PDA dua gaya perluasan untuk menyediakan peningkatan kemampuan: *Palm Universal Connector System* dan *Palm Expansion Card Slot*. *Universal Connector System* mengijinkan GPS penerima, *modem wireless*, *keyboards*, dan perlengkapan lain untuk saling berhubungan dengan *device* melalui USB yang memungkinkan koneksi. *Palm Expansion Card Slot* mengakomodasi *Multimedia Card* (MMC) dan kartu *Secure Digital* (SD). Modul kartu MMC adalah memori *solid-state* yang dapat dipindahkan dari ukuran serupa dan disain ke SD memori kartu. Di samping memori, kartu SD dapat juga menyertakan jenis lain seperti kartu kamera atau komunikasi *wireless*.

Arsitektur untuk Palm OS *device* diorganisir kedalam lapisan berikut: *Application* (aplikasi), Sistem operasi, Perangkat lunak API dan *device* Perangkat keras, dan Perangkat keras. Gambar 2.2 menggambarkan hubungan antar lapisan. Perangkat lunak Application Programming Interface (API) yang memberi pengembang perangkat lunak suatu tingkatan perangkat keras yang bebas, membiarkan aplikasi melaksanakan eksekusi dibawah lingkungan perangkat keras berbeda dengan *merecompiling* aplikasi itu. Pengembang mempunyai kebebasan untuk melewati API dan secara langsung mengakses pengolah, menyediakan kendali lebih menyangkut pengolah dan kemampuannya. Bagaimanapun, hal ini

datang atas biaya dalam peningkatan aplikasi yang buruk. Palm OS tidak menerapkan ijin atas data dan kode. Oleh karena itu, aplikasi dapat mengakses dan memodifikasi data manapun.



Gambar 2.2 Arsitektur Palm OS

Perusahaan *handheld device* lain telah mengizinkan Palm OS untuk menggunakan garis peralatan mereka sendiri. Versi Palm OS dapat dibagi menjadi tiga cakupan : versi sebelumnya 4.0, versi dari itu 4.0 ke 5.0, dan yang maju ke depan dari 5.0 ke versi 6. Pada awalnya Palm OS didukung oleh sebuah *multitasking* sederhana dimana aplikasi dapat berjalan hanya sekali dalam satu waktu, dan *single-threaded*. Versi terakhir mendukung penuh aplikasi *multi-threaded* dan *multitasking*. Sejumlah sifat mudah diserang didalam versi sebelum 4.0 dan telah diperbaiki pada versi kemudian. Khususnya, pemakaian login *password* ditunjukkan untuk menjadi tidak mudah diserang dan dengan mudah dibalikkan. Versi 4.0 juga memperkenalkan awal dukungan untuk *filesystems* pada kartu memori yang dapat dipindahkan. Versi sebelum 5.0 hanya mengeksekusi program tunggal serentak dalam satu waktu, sedang 5.0 dan mendukung yang *multiprocessing*. Versi 5.0 dan diatas ditukar menjauh dari keluarga dari *microprocessors* DragonBall ke keluarga StrongArm, dengan dukungan emulasi dari aplikasi sebelumnya yang dikembangkan untuk Dragonball.

Palm OS *device* menawarkan ciri keamanan *built-in* untuk menyediakan perlindungan untuk *records* individu dan kemampuan untuk mengunci *device* apabila pemakai menekan *device* “**off**”. Penguncian *records* individu mengijinkan para pemakai untuk menandai *records* sebagai pribadi dan tidak dipertunjukkan kecuali jika *password* yang sesuai disajikan. Bagaimanapun, *records* yang ditandai pribadi dapat diakses, dibaca, dan dicopy melalui *device* lain. Kemampuan untuk mengunci suatu *device* diperlukan para pemakai untuk memasukan *password* yang benar sebelum akses diterima layar aplikasi. Didalam versi awal Palm OS,

password menjadi lemah, mudah dibalikkan dan blok data yang disandikan yang berisi *password* selama HotSync dapat diinterupsi. Pihak ketiga produk yang ada memberi para pemakai kemampuan untuk *encrypt* data sensitif dan meningkatkan keseluruhan keamanan.

Palm OS *device* meliputi sebuah RS232 berbasis "Palm Debugger" yang menyediakan tingkatan perakitan dan sumber *debugging*, yang dimasukkan dengan mengeluarkan suatu kombinasi tombol. Dua alat penghubung yang ada pada monitor adalah serial port untuk komunikasi. "**Console Mode**" saling berhubungan dengan suatu *debugger* tingkat tinggi dan digunakan kebanyakan untuk manipulasi database. "**Debug Mode**" secara khas digunakan untuk perakitan dan *register-level debugging*.

2.3 Pocket PC

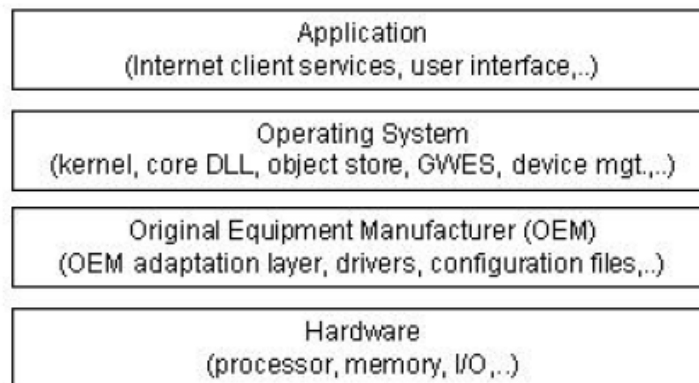
Pocket PC berkembang sukses dari Palm PDA dan permintaan bertambah untuk *device* yang serupa yang mempunyai daya proses lebih dan kemampuan *networking*. Microsoft memasukkan *handheld device* ke pasar dengan sistem operasi Windows CE (WinCE), yang kemudian ditambahkan dengan kemampuan untuk menghasilkan Pocket PC (PPC). Windows CE mendukung *multitasking*, lingkungan *multithreaded*, yang diwariskan oleh Pocket PC. Aplikasi berjalan dibawah Windows CE dilindungi dari pertentangan satu sama lain sampai ke manajemen memori. Windows CE dan PPC sudah meningkat didalam *tandem* dari WinCE versi 2.0/PPC 2000 ke WinCE 3.0/PPC 2002 ke WinCE 4.2/PPC 2003 (PPC 2003 seperti Windows Mobile 2003), melalui *pengupgradetan* sejumlah tampilan. Sebagai contoh, versi awal ActiveSync peka terhadap serangan kekuatan fisik *password* dan penolakan layanan menyerang apabila penyamaan diatas suatu jaringan dan sesudah itu dikoreksi. Menyajikan sifat mudah diserang pada *device* lebih awal dapat bermakna dalam melewati mekanisme keamanan, membiarkan penyelidik forensik mengakses ke data.

Pocket PC berjalan pada sejumlah *processors*, tetapi terutama terlihat pada *device* yang mempunyai Xscale, ARM, atau *processor* SHx. Berbagai Pocket PC *device* dengan mempunyai ROM berkisar antara 32 ke 64MB dan RAM berkisar antara 32 ke 128MB. PIM dan data pemakai lain secara normal berada pada RAM, sedang sistem operasi dan aplikasi pendukung berada pada ROM. Suatu *filestore* tambahan yang dapat dialokasikan didalam ROM tak terpakai yang tersedia dibuat untuk mem-*backup* file dari RAM. Satu atau lebih kartu slot, seperti suatu *Compact Flash* (CF) atau *Secure Digital* (SD) slot kartu, biasanya didukung. Apalagi, beberapa pembuat menyediakan perluasan kemampuan, seperti *extension*

sleeves atau perluasan modul yang memungkinkan teknologi lain untuk disatukan. Kebanyakan Pocket PC *device* menggunakan baterai lithium-ion. Untuk mencegah kerugian data apabila kekuatan baterai melemah, baterai lithium-ion harus di *charge* kembali dengan sebuah kabel listrik, atau dipindahkan dan digantikan dengan baterai yang di *charge*.

Arsitektur untuk Windows CE *device* terdiri dari empat lapisan: *Application* (Aplikasi), *Operating System* (Sistem Operasi), *Original Equipment Manufacturer* (OEM), dan *Hardware* (Perangkat keras). Suatu diagram yang disederhanakan menyangkut arsitektur Windows CE ditunjukkan didalam Gambar 2.3 di bawah. Jasa diorganisir kedalam modul, yang mana dapat dimasukkan atau dikeluarkan apabila membangun sebuah gambaran bangunan yang spesifik. Karena kebanyakan dari sistem operasi Windows CE ditulis dalam bahasa C, inti dan modul lain dapat dikirim ke pengolah berbeda dengan *recompiling* kode untuk suatu arsitektur perangkat keras yang spesifik (seperti, Strongarm, XSCALE, dan lain-lain).

Lapisan Equipment Manufacturer (OEM) yang asli adalah lapisan antara Lapisan Sistem Operasi dan Lapisan Perangkat keras. Lapisan itu berisi OEM Lapisan Adaptasi (OAL), yang mana terdiri dari satu set fungsi berhubungan dengan sistem *startup*, *interrupt handling*, *power management*, *profiling*, *timer and clock*. OAL memungkinkan suatu OEM untuk menyesuaikan Windows CE kepada suatu *platform* spesifik. Suatu OEM harus ditulis OAL untuk perangkat keras manapun sekarang ini.



Gambar 2.3 Arsitektur Windows CE

Didalam Lapisan Sistem operasi adalah inti Windows CE dan *device drivers*, yang bertujuan mengatur dan menghubungkan dengan *device* perangkat keras. *Device drivers* menyediakan *linkage* untuk *kernel* (inti) untuk mengenali *device* dan untuk memungkinkan komunikasi dibentuk antara perangkat keras dan aplikasi. Suatu *device drivers* dapat baik secara

monolithic maupun *layered*. Pengarah *monolithic* menerapkan *device* penghubung mereka secara langsung dalam kaitan dengan tindakan pada *device* yang mereka kendalikan. Pengarah Layer memisahkan implementasi kedalam dua lapisan: lapisan atas, yang mana menyingkapkan *driver's native* atau *stream interface* (penghubung arus), dan lapisan yang lebih rendah yang melaksanakan interaksi perangkat keras.

Grafik, *Windowing*, dan Events Subsystem (GWES) termasuk bagian dari Lapisan Sistem Operasi dan menyediakan *device* penghubung antar pemakai, aplikasi, dan sistem operasi itu. GWES adalah suatu *device* penghubung grafik terintegrasi (GDI), *window manager*, dan *event manager*. Modul GWES mempunyai dua subkomponen : Pemakai dan GDI. Pemakai mengacu pada bagian dari GWES *handles messages, events* (peristiwa), dan masukkan pemakai dari *keyboard* dan *mouse* atau *stylus*. GDI mengacu pada bagian dari GWES yang mengendalikan bagaimana grafik dan teks dipertunjukkan. GDI digunakan untuk menggambar garis, kurva, *closed figures*, teks, dan gambar bitmap.

Obyek mengacu pada tiga jenis penyimpanan yang didukung oleh Windows CE didalam Lapisan Sistem operasi : *file system*, *registry*, dan *property databases*. Standard Win32 berfungsi menyediakan akses ke file dan pencatatan, selagi Windows CE-Specific API baru berfungsi menyediakan akses ke hak milik database dan pencatatan ciri tertentu. Subset Win32 dan Microsoft lain API yang diterapkan dalam Pocket PC mengijinkan suatu sistem untuk memenuhi kebutuhan dari suatu aplikasi, sekalipun menyimpan program yang serupa dengan Windows PC. Ukuran Maksimum dari obyek adalah 256MB dalam Windows CE. Obyek dibangun pada suatu *internal heap* yang berada pada RAM, ROM, atau keduanya. *Heap* yang internal menyediakan suatu model transaksi penggunaan yang dibukukan untuk memastikan integritas dari obyek penyimpan data.

File system Windows CE mengijinkan suatu file untuk disimpan baik dalam RAM dan ROM. Ketika suatu file disimpan didalam RAM diberi nama yang sama seperti file yang disimpan dalam ROM. File RAM yang nyata membayangi file pada ROM. Seorang pemakai yang mencoba untuk mengakses suatu file bayangan akan mengakses ke hanya versi RAM. Bagaimanapun, ketika versi RAM dihapus, versi ROM dari file dapat diakses. Ciri ini bermanfaat untuk *upgrading* file yang datang dengan suatu *device* sebagai file ROM.

Properti database adalah tempat penyimpanan informasi yang dapat disimpan, dicari, dan didapat kembali oleh aplikasi yang dihubungkan. Untuk mengurangi ruang, teknik

pemampatan juga diterapkan secara otomatis. Database ini menyediakan suatu cara untuk manajemen informasi umum pada *device* itu.

Pencatatan Windows CE adalah suatu database yang menyimpan informasi tentang *applications* (aplikasi), *drivers*, *system configuration*, *user preferences* (pilihan pemakai), dan data lain. Tujuan pencatatan adalah menyediakan tempat tunggal untuk penyimpanan semua pengaturan untuk sistem, aplikasi, dan pemakai. Pencatatan selalu disimpan didalam RAM dan sebagai akibatnya bersifat *volatile*. Jika tidak ada pencatatan yang ada didalam RAM, Windows CE dapat memperbaharui kesalahan suatu file yang disimpan didalam ROM.

Sistem operasi Windows CE mendukung empat jenis memori :

1. *RAM* - RAM, dialokasikan kedalam dua area terpisah : obyek menyimpan dimana data dijaga dan memori program dimana program dilaksanakan. Partisi dari memori utama dapat dikendalikan oleh *end-user* (pemakai akhir) melalui *application level control* dan dapat disesuaikan tanpa *booting* kembali. Suatu manajemen sistem *virtual-memory* digunakan untuk mengalokasikan memori program.
2. *Expansion RAM* (Perluasan RAM) – Perluasan RAM didukung sebagai tambahan terhadap sistem RAM utama untuk menyediakan para pemakai dengan penyimpanan ekstra. Perluasan RAM dipetakan kedalam memori sebenarnya setelah *booting* dan terlihat sama didalam memori yang sebenarnya dipetakan kepada OS sebagai sistem RAM.
3. *ROM* - Ruang memori ROM berisi bermacam-macam data file seperti *audio files*, *fonts* dan *bitmaps*. ROM biasanya di *compress* dan di *decompress* apabila dibawa kedalam sistem RAM untuk pemakaian. Ruang memori ROM juga berisi dukungan untuk data yang tidak melakukan eksekusi *compress*, aplikasi, dan DLLS untuk operasi XIP (eXecute In Place). Sepanjang proses membentuk sebuah gambaran, unsur-unsur individu dapat ditunjuk baik untuk XIP maupun dipanggil atas permintaan operasi.
4. *Persistent Storage* - Sebagian besar dukungan untuk *persistent storage* diorientasikan di sekitar kartu penyimpanan yang dapat dipindahkan. Sebagai contoh, file-file (executables, data, file pemakai) yang disimpan didalam *persistent storage* adalah memori yang dipetakan kedalam sistem RAM untuk digunakan.

Pocket PC *device* menawarkan para pemakai kemampuan untuk menetapkan suatu *password* yang *power-on* yang terdiri dari 4-digit *numeric* atau *password alphanumeric* yang

lebih sampai 29 karakter panjangnya. Para pemakai dapat menetapkan suatu *timeout* yang mengunci *device* apabila tidak menggunakan sejumlah waktu yang telah ditetapkan. Jika *password* yang dimasukkan salah, usaha yang berikutnya akan dihukum dan mengambil lebih panjang proses, untuk menakuti penyerang. Jika *password* dilupakan, satu-satunya cara untuk membuka kunci *device* adalah dengan melakukan suatu *hard-reset* dan *resynching data*. Beberapa model Pocket PC *device* yang terbaru sudah mengintegrasikan suatu sidik jari biometric untuk keamanan tambahan yang dapat digunakan didalam *tandem* dengan 4-digit atau *password alphanumeric*.

Pocket PC memungkinkan pengembang perangkat keras, sistem integrator, atau pengembang untuk memutuskan jasa yang akan disatukan dalam versi Pocket PC mereka. Pocket PC *device* dapat menyertakan lingkungan yang dipercayai dimana OS *kernel* memverifikasi perpustakaan dan aplikasi sebelum pemuatannya. Ada tiga kemungkinan: modul perangkat lunak yang mungkin dipercayai tanpa syarat, tidak menanggung jaminan pembatasan fungsi akses pencatatan atau panggilan bisa dilakukan, atau tidak percaya sama sekali.

Pocket PC *device* mempunyai kemampuan *bootloader* yang berbeda. Perusahaan *device* menentukan cakupan kemampuan dengan dua pengecualian yaitu *bootloader* harus mampu mengisi OS dan meningkatkan mutunya untuk versi berikutnya. Beberapa versi awal Pocket PC *device* menyajikan dokumentasi pada urutan tali kunci spesifik (seperti, yang secara bersamaan menekan tombol 2 dan 4, tombol *power*, dan tombol *reset* pada model iPaq 38xx) yang akan *booting* kedalam suatu mode spesifik yang dikenal sebagai "Parrot mode". *Device* harus dihubungkan melalui *serial connector* dan suatu terminal emulator yang digunakan untuk menetapkan komunikasi dengan *bootloader* dan *issue commands*. Parrot mode mempunyai perintah meliputi kemampuan untuk menetapkan daftar menilai, menetapkan isi memori, menetapkan muatan memori, menetapkan tabel pemetaan alamat, backup memori ke kartu penyimpanan (CF/SD), dan mengembalikan memori dari *storage* penyimpanan.

2.4 Linux

Linux, suatu sistem operasi *open source* yang populer untuk komputer *desktop* dan *server* juga dapat dilihat pada beberapa PDA *device*. Linux adalah benar *multitasking*, 32-bit sistem operasi yang mendukung *multithreading*. Di samping distribusi komersil yang datang

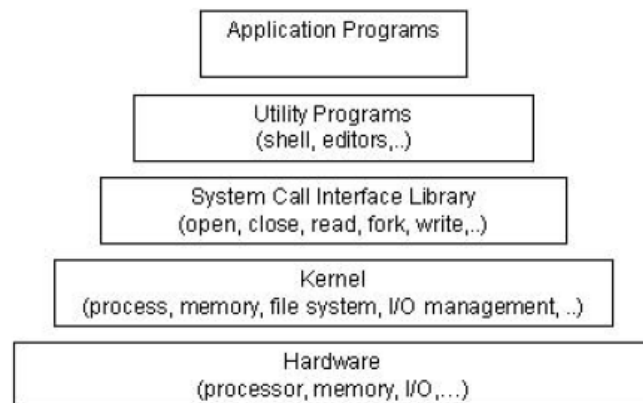
penginstallan ulang oleh perusahaan PDA, distribusi Linux juga tersedia untuk Pocket PC dan Palm OS *device*. Sukses dari PDA berbasis Linux dilihat pada model yang *open source* dan kemampuannya untuk melibatkan pengembangan masyarakat software untuk menghasilkan aplikasi yang bermanfaat.

Linux PDA yang paling umum di U.S. adalah **Sharp Zaurus**. Model Zaurus yang pertama, SL-5500, diperkenalkan di tahun 2002. Menggunakan *Embedix*, suatu kernel Linux yang ditempelkan dari *Lineo*, dan lingkungan *Qtopia desktop* dari Trolltech untuk *windowing* dan teknologi presentasi. *Embedix* didasarkan pada suatu *kernel network* dengan sistem *built-in* yang mendukung *Wifi*, *Bluetooth*, dan *modem* teknologi *wireless*, seperti halnya keamanan yang saling terhubung dan modul *encryption*. Alat ini mempunyai suatu *processor StrongARM*, 16 MB ROM, 64MB RAM, dan sebuah 3.5-inch 240x320-pixel LCD berwarna. Seperti pada Palm OS dan Pocket PC *device*, sumber kekuatan Zaurus adalah baterai lithium-ion. Keduanya *Compact Flash* (CF) dan SD slot kini (SD slot juga menerima MMC. Suatu tipe *keyboard QWERTY* yang terintegrasi ke dalam *device* dan menjadi kelihatan dengan meluncur ke bawah *thumb pad* dan panel aplikasi tombol.

Linux *Embedix* mengacu pada suatu distribusi komersil. Sedang kebanyakan distribusi Linux mempunyai kegunaan yang sama, *libraries* (perpustakaan), *drivers* (pengarah), dan *windowing frameworks*, perbedaan terjadi didalam *patches*, *modul*, dan kegunaan yang dimasukkan, dan bagaimana instalasi, *configuration*, dan *upgrade* dilakukan. Suatu system Linux *embedded* minimal memerlukan tiga unsur rumit : *boot utility*, *Linux micro-kernel*, dan suatu proses inialisasi. Aplikasi pemakai berdasar pada penggunaan pribadi dapat ditambahkan untuk *self-customisasi* menyangkut *device* tersebut.

Distribusi Linux juga tersedia untuk HP iPAQ, Dell's Axim, dan PDA lain tetapi memerlukan pemakai untuk menginstal OS yang ada. Sebagai contoh, iPAQ *device* datang dengan instalasi Windows Microsoft's untuk Pocket PC. Linux dapat menggantikan Microsoft OS didalam unit *flash ROM*. Suatu distribusi Linux populer untuk iPAQ adalah Distribusi yang umum dikenal. Yang umum dikenal meliputi suatu sistem pengemasan dipanggil *ipkg* (paket Itsy) yang menginstal, membaharui, memindahkan, dan mengatur paket dengan cara yang sama seperti pada **Redhat** atau fasilitas paket **Debian** untuk desktop Linux. Karena informasi yang sekarang tentang *handheld devices* berbasis Linux, Lokasi Web sites harus dimonitor secara regular.

Gambar 2.4 memberi suatu arsitektur konseptual untuk sistem operasi Linux. Sistem operasi Linux bertanggung jawab untuk *memory management* (manajemen memori), *process* (proses) dan *thread creation*, *interprocess communication mechanisms*, *interrupt handling* (penganganan kesalahan), *execute-in-place* (XIP) ROM *filesystems*, RAM *filesystems*, *flash management*, dan TCP/IP *networking*.



Gambar 2.4 Arsitektur Linux

Kernel Linux terdiri atas subsistem dan komponen modular yang meliputi *device drivers*, protokol, dan komponen jenis lainnya. Kernel juga terdiri dari *scheduler*, manajer memori, *filesystem* yang sebetulnya, dan *resource allocator*. Penghubung pemrograman *device* menyediakan suatu metoda standard dimana kernel Linux dapat diperluas. Pengolahan berasal dari panggilan sistem penghubung ke peminta layanan, sebagai contoh, dari proses pengawasan subsistem atau file, yang mana pada gilirannya meminta jasa dari perangkat keras. Perangkat keras kemudian menyediakan jasa kepada kernel, mengembalikan hasil melalui kernel ke sistem penghubung panggilan.

Linux menawarkan dukungan menyeluruh untuk keamanan yang telah menjadi bagian dari sistem operasi dari serangan. Cirinya meliputi *user identification* dan *authentication* (pengesahan), akses kontrol dalam file dan direktori berdasarkan pada pemilik (*user/group/all*), pembukuan aktivitas *security-relevant*, dan berbagai tingkatan *network encryption* (Point-To-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC), Secure Shell (SSH), dan lain-lain). Proses mengalir dibawah Linux pada mesin yang sama juga dilindungi dari pertentangan satu orang dengan yang lain. Sistem operasi Linux diadakan untuk PDA berakibat pada kesempatan ditemukannya sifat mudah diserang keamanannya didalam implementasi dan disain yang mempengaruhi sistem keamanan. Sebagai contoh,

screen-locking passcode pada Zaurus menyediakan *user authentication*, menciptakan nilai acak yang sama (yaitu, *salt value*) setiap kali *passcode* diset. Kekeliruan ini memperlemah keamanan dengan membiarkan suatu penyerang menghasilkan suatu tabel *passcode* dan menemukan nilai-nilai konsisten untuk membongkar *password device*, dan memerlukan koreksi. Di samping ciri *built-in* keamanannya, solusi pihak ketiga keamanan juga ada untuk Linux, menyediakan ukuran keamanan tambahan untuk *device* dan file akses.

Bootloader adalah *firmware* yang bertanggung jawab untuk *initializing* perangkat keras dan *physical memory* (memori fisik), dan memindahkan dan memuat kendali ke kernel. *Bootloaders* berbasis Linux pada *device* yang ditempelkan pada umumnya dapat menerima gambaran kernel yang ditransfer diatas satu atau lebih *device* penghubung berbeda, termasuk *serial connections*, *Ethernet connections*, dan *memory cards*. Mereka juga dapat menyediakan suatu perintah yang kaya. Sebagai contoh, *flash bootloader* untuk Linux pada iPAQ *device* adalah suatu *full-featured program* yang ditonjolkan meliputi perintah untuk membaca dan menulis lokasi *arbitrary* RAM dan tulis lokasi *arbitrary flash* ROM.

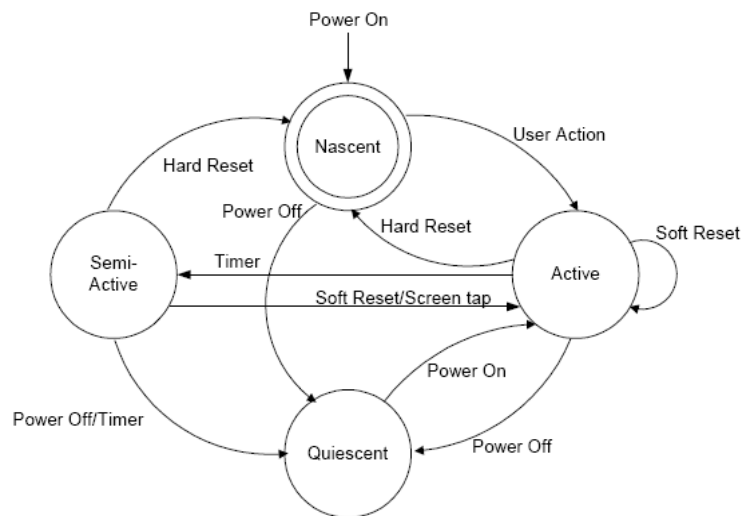
2.5 Status General atau umum

Pandangan yang paling sederhana dari suatu komputasi *device*, seperti suatu komputer *desktop*, adalah bahwa sama-sama terdapat status "**on**" atau "**off**". Bagaimanapun, pembesaran lebih lanjut diperlukan, terutama sekali untuk PDA, perilaku siapa yang menjadi lebih kompleks. Gambar 2.5 memberi suatu diagram tingkat tinggi yang menggambarkan berbagai status dimana suatu PDA dapat pada setiap waktu, bersama dengan transisi yang dapat terjadi yang dapat menyebabkan suatu perubahan status. Ketika sesuatu yang lebih terperinci dinyatakan dalam diagram yang mungkin, berikut empat status yang menyediakan suatu model sederhana yang umum yang paling berlaku bagi PDA:

1. **Nascent State** (Status Mulai) - *Device* ada didalam status ini saat diterima dari pabrik - *Device* tidak berisi data pemakai dan masih dalam bentuk wujud pabrik. PDA harus diganti untuk suatu level voltase minimum untuk dapat dipakai dan untuk memperoleh masukan awal kepada status mulai, yang mana dicapai ketika *device* pertama kali menekan tombol power. Tindakan transisi pemakai manapun dalam *device* keluar dari status ini. Status ini dapat dicapai lagi dengan melakukan *hard reset* atau membiarkan

baterei kosong, yang mana membersihkan *filesystem* keduanya dan memori dinamis aktif dan mengembalikan ke bentuk dari pabrik.

2. **Active State** (Status aktif) – *Device* yang dalam keadaan aktif adalah yang sedang menyala, melakukan tugas, dan mampu di ubah - ubah oleh pemakai dan mempunyai *filesystem* yang berisi data mereka. Jika *soft reset* dilakukan, *device* kembali ke keadaan aktif setelah membersihkan memori yang bekerja. Jika mekanisme *user authentication* dimungkinkan, mereka dinyatakan pada saat menyala atau pada transisi *soft reset* pada status ini .
3. **Quiescent State** (Status Diam) - status diam adalah suatu mode tidak aktif yang memelihara hidup baterai selagi pemeliharaan data pemakai dan melakukan fungsi lainnya. Konteks Informasi untuk *device* dipelihara didalam memori untuk mengijinkan suatu penerusan pengolahan yang cepat manakala kembali ke keadaan aktif. Menekan tombol power apabila dalam status aktif atau status semi-aktif (yaitu, untuk mematikan *device*), atau mempunyai suatu ketidakaktifan pengatur waktu apabila didalam semi-aktif, menyebabkan suatu transisi ke status diam.
4. **Semi-Active State** (Status Semi-Aktif) - status Semi-Aktif adalah suatu status penengah antara yang diam dan aktif. Status dicapai oleh suatu pengatur waktu, yang mana dilakukan setelah masa ketidakaktifan yang membiarkan hidup baterai dipelihara dengan sedikit pertimbangan pengambilan dan pengambilan tindakan lain yang sesuai. Status Semi-Aktif kembali ke keadaan aktif manakala suatu *screen-tap*, mekanan tombol, atau saat *soft reset* terjadi. *Device* yang tidak mendukung status Semi-Aktif memerlukan pengatur ketidakaktifan waktu tunggal ke transisi yang secara langsung dari yang status aktif ke status diam.



Gambar 2.5 Diagram Bagian secara umum

Sederhananya dinyatakan suatu PDA *device* dengan kekuatan baterai yang tidak pernah benar-benar mati, karena proses aktif bahkan ketika tidak aktif akan terlihat.

Untuk kesederhanaan, suatu *device* disebut "**off**" atau "**powered off**" jika ada di status yang diam, dan "**on**" atau "**powered on**" jika ada di status peringatan apapun. Dengan cara yang sama, suatu *device* disebut "**cleared**" dan *devoid of data* (tanpa data) apabila berada didalam status *nascent* (status mulai). Catatan: bagaimanapun, penyimpangan dapat terjadi pada *device* yang menggunakan *flash memory* untuk tujuan selain dari penggunaan sistem operasi yang eksklusif tersebut. Sebagai contoh, ada aplikasi untuk Palm OS yang memungkinkan data untuk disimpan pada *flash memory* didalam ruang yang tak terpakai oleh sistem operasi itu. Dengan cara yang sama, beberapa Pocket PC terbaru PDA mulai untuk meliputi suatu ciri untuk mem-*backup* data penting PIM pada *flash memory*, dimana data dapat ditahan dan diperbaiki jika dilakukan *hard reset* pada *device* tersebut. Akhirnya, *handheld* distribusi Linux, seperti distribusi yang umum dikenal dari handhelds.org, sering menggunakan *flash memory* sebagai pengganti RAM untuk data pemakai untuk menghindari kerugian apabila terjadi *hard reset*. Di dalam situasi ini, *nascent state* harus ditafsirkan secara tepat.

3. Forensic Tools

Tidak sama dengan kondisi pada komputer pribadi, variasi dan jumlah nomor *toolkits* untuk PDA dan *handheld devices* lain sangatlah terbatas. Tidak hanya ada lebih sedikit khusus *tools* disana dan *toolkits*, tetapi juga cakupan *device* dimana mereka beroperasi secara khas dibatasi ke hanya keluarga PDA *device* yang populer. Hal itu didasarkan pada Pocket PC dan Palm OS. *Device* berbasis Linux ini dapat di gambarkan dengan kegunaan dd, sedikit banyaknya sejalan untuk suatu *desktop* Linux, dan dianalisa dengan penggunaan dari suatu *device* yang dapat dipertukarkan (seperti, EnCase). Karena Palm OS *device* menjadi yang terbesar, banyak *forensic tools* tersedia untuk dibanding dengan keluarga *device* lain. Pada tabel 3.1 terdapat daftar *open-source* dan *tools* yang dikenal pengarang secara komersial tersedia dan fasilitas yang mereka sediakan: *acquisition* (perolehan), *examination* (pengujian), atau *reporting* (pelaporan). Singkatan NA berarti bahwa *tool* yang ditinggalkan untuk baris tidak dapat digunakan untuk *tool* pada puncak dari kolom. Dengan satu perkecualian (yaitu, versi Palm OS sebelum 4.0), *tools* ini memerlukan pemeriksa yang mempunyai akses tanpa halangan untuk memperoleh isi (yaitu, tidak ada kebutuhan teknik pengesahan yang dicukupi untuk memperoleh akses).

	Palm OS	Pocket PC	Linux PDA
pdd	Acquisition	NA	NA
Pilot-Link	Acquisition	NA	NA
POSE	Examination, Reporting	NA	NA
PDA Seizure	Acquisition, Examination, Reporting	Acquisition, Examination, Reporting	NA
EnCase	Acquisition, Examination, Reporting	NA	Examination, Reporting
dd	NA	NA	Acquisition

Tabel 3.1 PDA Forensic Tools

Forensic tools memperoleh data dari suatu *device* dengan satu atau dua jalan: secara fisik atau logis. Perolehan secara fisik melibatkan suatu salinan *bit-by-bit* keseluruhan

penyimpanan fisik (seperti, suatu *disk drive* atau RAM chip), ketika *forensic tools* didapat secara logis mellihatkan suatu salinan *bit-by-bit* objek penyimpanan logis (seperti, direktori dan file) yang berada pada suatu penyimpanan logis (seperti, suatu partisi *filesystem*). Perbedaan berada didalam pembedaan antara memori ketika dilihat oleh suatu proses melalui fasilitas sistem operasi (yaitu, suatu pandangan logis), melawan memori ketika dilihat di format mentah oleh pengolah dan komponen perangkat keras lain yang berhubungan (yaitu, suatu pandangan fisik).

Perolehan secara fisik mempunyai keuntungan daripada secara logis, karena itu *forensic tools* mengijinkan file dihapus dan sisa data ditampilkan (seperti, RAM yang tidak teralokasi atau ruang *filesystem* yang tak terpakai) untuk diuji, yang mana jika tidak pergi tidak akan dibukukan. Gambaran fisik *device* biasanya dengan mudah diimport kedalam *device* lain untuk pengujian dan pelaporan. Bagaimanapun, suatu struktur logis mempunyai keuntungan bahwa suatu organisasi yang lebih alami untuk dipahami dan digunakan selama pengujian. Hal seperti itu, jika mungkin, membuat kedua jenis yang didapat PDA lebih baik. *Tools* yang tidak dirancang khusus untuk tujuan forensik adalah diragukan dan harus secara menyeluruh dievaluasi sebelum penggunaan. Dalam beberapa situasi, mereka dapat jadi satu-satunya *device* untuk mendapat kembali informasi yang dapat relevan sebagai bukti.

3.1 Palm dd (pdd)

Palm dd (pdd) adalah suatu *command line tool* berbasis Windows yang melaksanakan pengadaan informasi fisik dari Palm OS *device*. pdd dirancang untuk bekerja sama dengan banyak PDA yang menjalankan Palm OS didalam *console mode*. Sepanjang status *acquisition*, suatu gambar *bit-for-bit* dapat diperoleh memori *device*. Data yang didapat kembali oleh pdd meliputi semua database dan aplikasi pemakai. pdd adalah suatu *command line driven application* seperti *graphics libraries* (perpustakaan grafik), *report generation* (generasi laporan), *search facilities* (fasilitas pencarian), dan *bookmarking capabilities* (kemampuan petunjuk halaman buku). Ketika informasi telah diperoleh, dua file akan dihasilkan : satu yang berisi informasi *device-specific* (seperti, versi OS , jenis prosesor, ukuran RAM dan ROM), dan yang lain berisi suatu gambar *bit-by-bit* menyangkut *device* tersebut. Pemeriksa menghadapi tantangan untuk berhati-hati dalam menguji keluaran, yang berada dalam format biner, dan sebagian menjadi karakter ASCII. File yang diciptakan dari pdd dapat diimport ke dalam suatu *forensic tool*, seperti EnCase, untuk menanmpung analisa. Cara lainnya, *tool* yang

salah disebut *hex editor*. pdd tidak melakukan *hash* nilai-nilai untuk informasi yang diperoleh. Bagaimanapun, suatu prosedur terpisah dapat digunakan untuk memperoleh nilai-nilai *hash* yang diperlukan. Mulai dari Januari 2003, pdd tidak lagi didukung, bagaimanapun, source program versi 1.11 tersedia dan tersedia untuk penggunaan, seperti dirumuskan dalam lisensi yang dimasukkan. *Paraben* telah mengintegrasikan unsur-unsur menyangkut mesin pdd ke dalam PDA *Seizure*.

3.2 Pilot-Link

Pilot-Link adalah suatu perangkat lunak yang *open source* dikembangkan untuk masyarakat Linux untuk memungkinkan informasi untuk ditransfer antara penghuni Linux dan Palm OS *device*. Pilot-Link berjalan pada sistem operasi *desktop* lain disamping Linux, mencakup Windows dan Mac OS. Sekitar tiga puluh *command line programs* menjadi deretan anggota perangkat lunak. Tidak sama dengan pdd, yang menggunakan protokol Palm *debugger* untuk *acquisition*, pilot-link menggunakan protokol *Hotsync*. Dua program yang berminat ke spesialis forensik adalah *pi-getram* dan *pi-getrom*, yang mana berturut-turut mendapat kembali muatan RAM dan ROM dari suatu *device*, sama seperti *acquisition* fisik yang dilakukan oleh pdd. Program bermanfaat yang lain adalah *pilot-xfer*, yang mana memungkinkan instalasi program dan *backup* serta *restoration* (pemugaran) database. *Pilot-xfer* menyediakan arti untuk memperoleh muatan dari suatu *device* secara logika. Muatan yang didapat kembali dengan kegunaan ini dapat dengan diuji manual dengan POSE, suatu *forensic tool* yang kompetibel seperti EnCase, atau *hex editor*. Pilot-Link tidak menghasilkan nilai *hash* menyangkut informasi yang diperoleh. Suatu langkah terpisah harus dilaksanakan untuk memperoleh nilai *hash* yang diperlukan.

3.3 POSE

POSE (Palm OS Emulator) adalah suatu program perangkat lunak yang berjalan pada suatu komputer *desktop* dibawah berbagai sistem operasi, dan bertindak sama sebagai perangkat keras Palm OS *device*, ketika suatu ROM terisi ke dalam POSE. Emulator program yang cuma-cuma ini meniru perangkat keras dari suatu pengolah Dragonball. Aplikasi *built-in* PIM (seperti, Datebook, Address Book, To Do, dan lain-lain) yang berjalan dengan baik dan tombol perangkat keras yang menampilkan reaksi secara akurat. Gambaran ROM dapat diperoleh dari *Palmsource Web site* atau dengan pengcopian muatan ROM dari suatu *device*

nyata, menggunakan pdd, Pilot-Link, atau suatu *tools* yang dilengkapi dengan emulator itu. POSE dibatasi pada Palm OS versi 4.x dan di bawahnya.

Pemuatan database nyata berbasis RAM kedalam emulator, yang disadap menggunakan *pilot-link* atau *tool* yang lain, memungkinkan pemeriksa untuk melihat dan mengoperasikan emulator *device* yang memiliki kesamaan bentuk seperti yang dipunya aslinya. Meskipun demikian, mula-mula dikembangkan untuk dijalankan, diuji, dan didebug aplikasi Palm OS tanpa harus mendownload alatnya, POSE juga bertindak sebagai suatu *tool* yang bermanfaat untuk membuat presentasi atau menangkap *screen shots* dari bukti yang ditemukan emulator *device* dari dalam database yang dimuat dari suatu *device* yang diserang. POSE dapat diatur untuk memetakan serial port Pam OS bagi salah satu dari serial port yang tersedia pada komputer desktop atau untuk mengalihkan jurusan TCP/IP manapun kepada TCP/IP *stack* pada desktop itu. Dengan beberapa percobaan, protokol *Hotsync* dapat berjalan antara *device* yang beremulasi dan komputer desktop, diatas dari suatu pengulanga serial koneksi atau koneksi TCP/IP yang dialihkan.

3.4 PDA Seizure

PDA *Paraben Seizure* adalah suatu perangkat lunak forensik yang tersedia *toolkit* yang memungkinkan pemeriksa forensik untuk memperoleh dan menguji informasi pada PDA untuk kedua platforms Pocket PC (PPC) dan Palm OS. Produk Paraben yang sekarang ini mendukung Palm OS sampai kepada versi 5, Pocket PC 2000-2003 (sampai kepada Windows CE 4.2), Activesync 3.7, dan Hotsync. PDA Seizure meliputi kemampuan untuk memperoleh suatu gambar forensic dari Palm OS dan Pocket PC *device*, untuk melakukan pencarian *examiner-defined* pada data yang dimasukkan didalam file yang diperoleh, menghasilkan *hash* file nilai-nilai individu dan untuk menghasilkan suatu laporan menyangkut penemuan. PDA Seizure juga menyediakan kemampuan *bookmarking* untuk mengorganisir informasi, bersama dengan suatu perpustakaan grafik yang secara otomatis memasang gambaran yang ditemukan dibawah fasilitas tunggal, berdasar pada file grafik perluasan dari file yang diperoleh.

Sepanjang *acquisition* suatu PPC *device*, diperlukan *connectivas* dari *device* melalui *ActiveSync*. Suatu account tamu harus digunakan untuk menciptakan suatu koneksi. Sebelum *acquisition* dimulai, PDA Seizure menempatkan suatu program kecil pada *device* didalam blok memori yang tersedia yang pertama untuk mengakses daerah memori yang tidak teralokasi. Untuk mengakses informasi yang sisanya, PDA Seizure menggunakan protokol Remote API

(RAPI), yang menyediakan satu set fungsi untuk aplikasi *desktop* untuk berkomunikasi dengan suatu *device* dan secara logika mengakses informasi. Karena Palm OS *device*, PDA pertama harus memasuki suatu model *debug*, yang biasanya dikenal sebagai *console mode*, dan semua aplikasi *Hotsync* aktif harus tertutup. Sekali ketika gambaran memori dari suatu Palm OS *device* diperoleh, pemakai dibisikkan untuk memilih tombol *Hotsync* pada atas *device* untuk memperoleh data logis yang secara terpisah. Data yang logis diwakili dalam gambaran file RAM itu yang diperoleh sampai *acquisition* fisik.

3.5 EnCase

EnCase adalah suatu perangkat lunak forensik *toolkit* yang menyediakan *acquisition* dari media yang dicurigai, pencarian dan analisa *tool*, *hash* generasi file individu, *data capture* dan tampilan dokumentasi. Walaupun lebih luas digunakan untuk pengujian PC, EnCase juga mendukung Palm OS *device*. Sekarang ini, dukungan terhadap Pocket PC tidak tersedia, tetapi kemampuan untuk mengimport suatu *data dump* dari PDA berbasis Linux tersedia. EnCase mengizinkan ciptaan dari suatu gambaran fisik lengkap *bit-stream* dari suatu Palm OS *device*. Sepanjang proses, integritas dari gambaran *bit-stream* secara terus menerus dibuktikan oleh nilai-nilai CRC (Cyclical Redundancy Check), yang mana dihitung berbarengan ke *acquisition*. Hasil gambaran *bit-stream*, dipanggil file bukti EnCase, dikenal sebagai read-only file atau "virtual drive" dari yang mana EnCase mulai merekonstruksi struktur file menggunakan data yang logis didalam gambaran *bit-stream*. Proses ini mengizinkan pemeriksa untuk mencari dan menguji muatan dari *device* yang digunakan baik logis maupun *physical perspective*.

EnCase mempertimbangkan file, folder, atau bagian dari suatu file untuk digarisbawahi dan diselamatkan untuk acuan kemudiannya. Tanda ini disebut *bookmarks*. Semua *bookmarks* disimpan didalam file kasus, dengan masing-masing kasus yang mengerti petunjuk file *bookmarks* sendiri. *Bookmarks* dapat dilihat kapanpun dan dapat dibuat dari data atau folder manapun yang ada. Pelaporan mengizinkan pemeriksa untuk memandang informasi dari sejumlah perspektif : semua file diperoleh, satu berkas, hasil dari suatu pencarian string, suatu laporan, atau keseluruhan file kasus yang diciptakan.

3.6 Duplicate Disk (dd)

Kegunaan Duplicate Disk (dd) adalah sama seperti pdd yang sepanjang akan memungkinkan pemeriksa untuk menciptakan suatu gambaran *bit-by-bit* yang menyangkut *device* itu. Seperti salah satu dari kegunaan Unix yang asli, dd telah menjadi satu format yang lain untuk dekade. Tidak sama dengan *tools* lain yang diuraikan diatas, dd melakukannya secara langsung pada PDA itu. Suatu gambaran menyangkut *device* dapat diperoleh dengan menghubungkan PDA, mengeluarkan perintah dd, dan membuang muatan ke tempat lain, sebagai contoh, sebuah alat bantu media seperti suatu kartu memori atau yang melintasi sesi *network* ke forensik *workstation*. Perhatian hal ini harus dicoba, karena dd dapat menghancurkan bagian-bagian dari *filesystem* (seperti, *overwriting data*) jika digunakan salah. Seperti dengan pdd, dd menghasilkan keluaran berupa data biner, sebagiannya berisi informasi karakter ASCII. dd menciptakan gambaran yang mungkin diimport untuk pengujian kedalam suatu *forensic tool*, seperti EnCase, jika didukung *filesystem*. Suatu dd dapat juga menciptakan gambaran mengulang didalam model *loopbacknya* pada suatu mesin Linux *Filesystem-Compatible* untuk dianalisa. Versi standard dd tidak menghasilkan nilai-nilai *hash* untuk memperoleh informasi. Bagaimanapun, suatu prosedur terpisah dapat digunakan untuk memperoleh nilai-nilai *hash* yang diperlukan. Versi modifikasi dd ada dengan menyertakan *hash* yang menghargai perhitungan, tetapi akan memerlukan instalasi dan kompilasi silang untuk menggunakannya.

3.7 Miscellaneous Tools

Tool lain tersedia dari suatu perusahaan perangkat keras atau perangkat lunak untuk mem-backup data atau mengembangkan perangkat lunak untuk suatu keluarga *device* yang dapat menopang suatu penyelidikan. Sebagai contoh, Microsoft telah mengembangkan suatu *tool* yang dipanggil ActiveSync Remote Display (ASRDISP) yang memungkinkan ActiveSync untuk dihubungkan kepada suatu Pocket PC dan kemampuan sepenuhnya ditampilkan didalam suatu *device window* sebenarnya pada *desktop*, seolah-olah sedang melakukan tindakan atas *device* fisik dirinya sendiri. Setelah data diperoleh dari target *device*, suatu *backup* penuh melalui ActiveSync dapat dilakukan untuk mengembalikan data yang di *backup* pada suatu *device* serupa, yang digunakan di ASRDISP untuk tujuan presentasi. Kegunaan ASRDISP menjadi bagian dari *Windows Mobile Developer Power Toys suite*.

Pengertian lain dalam merepresentasikan data adalah menggunakan Pocket PC emulator dan tersedianya kemampuan membagi folder. Selanjutnya, setelah *acquisition device*

telah berlangsung, pemeriksa dapat mengekspor file ke luar individu dari *device* bagi suatu folder spesifik yang disajikan pada *forensik workstation*. Folder yang disebarkan mengijinkan informasi untuk diimport dan dipertunjukkan melalui emulator, memberi pemeriksa kemampuan untuk menyajikan informasi yang relevan. Emulators untuk semua versi sistem operasi Pocket PC tersedia untuk didownload di situs Microsoft .

3.8 Custom Tools

Jika mungkin, prosedur perlu dibentuk pemandu pengolahan *acquisition* secara teknis, seperti halnya pengujian bukti. Bagaimanapun, beberapa situasi menuntut metode dan prosedur yang khusus diterapkan. Prosedur harus diuji untuk memastikan bahwa hasil diperoleh dengan bebas dapat direproduksi dan sah. Pengesahan dan Pengembangan dari prosedur harus didokumentasikan dan meliputi yang meliputi langkah-langkah :

1. Mengidentifikasi masalah atau tugas
2. Pengusulan kemungkinan pemecahan masalah
3. Pengujian masing-masing solusi pada suatu alat test serupa dan dibawah kondisi kendali yang dikenal
4. Mengevaluasi hasil dari test
5. Membereskan prosedur

4. Aturan dan Prosedur

Peristiwa dan Penyelidikan ditangani dalam berbagai jalan tergantung keadaan dari peristiwa, gravitas dari peristiwa, dan persiapan dan pengalaman dari regu penyelidikan. Penyelidikan digital dapat diperbandingkan ke peristiwa kejahatan dimana teknik investigasi yang digunakan penyelenggaraan peraturan daerah telah diterapkan sebagai pondasi untuk menciptakan prosedur yang digunakan apabila berhadapan dengan bukti digital. Bagian ini menyediakan suatu ikhtisar sebagai prinsip dan model mengenai cara yang telah diusulkan.

4.1 Aturan – aturan dan tanggung jawab

Apapun jenis dari peristiwa, berbagai jenis peran dilibatkan serupa. Perencanaan untuk peristiwa perlu menunjuk bagaimana personil memenuhi peran ini apabila menjawab dan melaksanakan suatu penyelidikan. Suatu peran yang umum dan berhubungan dengan tanggung jawab dapat dikenali. Mereka meliputi *First Responders* (responder pertama), *Investigators* (Penyelidik), *Technicians* (Teknisi), *Forensic Examiners* (Pemeriksa Forensik), dan *Forensic Analysts* (Analisis Forensik). Didalam situasi ditentukan, individu tunggal boleh melaksanakan lebih dari satu peran. Meskipun demikian, peran pembeda dan tanggung-jawab yang dihubungkan adalah bermanfaat.

First Responders (Responders Pertama) dilatih untuk tiba yang pertama pada tempat dari suatu peristiwa, menyediakan suatu penilaian awal, dan mulai memberi tanggapan yang sesuai. Tanggung-Jawab dari Responders Pertama adalah mengamankan tempat insiden, meminta pendukungan yang perlu, dan membantu dengan koleksi bukti.

Investigators (Penyelidik) merencanakan dan mengatur *preservation* (pemeliharaan), *acquisition* (perolehan), *examination* (pengujian), *analysis* (analisa), dan *reporting* (pelaporan) dari bukti elektronik. Petunjuk Penyelidik bertanggung-jawab meyakinkan aktivitas di tempat peristiwa dari suatu peristiwa dieksekusi didalam keadaan dan waktu yang benar. Petunjuk Penyelidik mungkin bertanggung jawab untuk mengembangkan bukti, menyiapkan suatu laporan kasus, dan pengarahan singkat manapun penentuan dan penemuan ke pejabat senior.

Technicians (Teknisi) menyelesaikan tindakan dibawah arahan Petunjuk Penyelidik. Teknisi bertanggung jawab untuk mengidentifikasi dan mengumpulkan bukti dan dokumen dari tempat peristiwa. Mereka secara khusus dilatih untuk menangkap peralatan elektronik dan memperoleh gambaran penduduk digital didalam memori. Lebih dari satu teknisi secara khas dilibatkan didalam suatu peristiwa, sebab pengetahuan dan ketrampilan berbeda diperlukan. Keahlian cukup harus tersedia di tempat peristiwa untuk menunjuk semua piranti digital yang berbeda yang dilibatkan didalam peristiwa itu.

Evidence Custodians (Penjaga Bukti) melindungi semua bukti yang dikumpulkan dan disimpan didalam suatu lokasi pusat. Mereka menerima bukti yang dikumpulkan oleh Teknisi, memastikannya dengan baik berlabel, memeriksanya kedalam dan keluar dari pengawasan protektif, dan memelihara suatu rantai penjagaan dengan tegas.

Forensic Examiners (Pemeriksa Forensik) secara khusus dilatih untuk menghasilkan gambaran yang diperoleh dari pengambilan peralatan dan pemulihan data digital. Pemeriksa membuat informasi pada *device* yang kelihatan. Pemeriksa boleh juga memperoleh data yang lebih terabaikan yang menggunakan peralatan yang sangat khusus, rancang-bangun kebalikan intensive, atau alat-alat sesuai lain yang tak tersedia ke Teknisi Forensik.

Forensic Analysts (Analisis Forensik) mengevaluasi produk dari Pemeriksa Forensik untuk artinya dan probative menghargai kepada kasus.

4.2 Prinsip – prinsip dalam pembuktian

Sebagai latar belakang bagi basis dasar penyelidikan utama manapun yang telah diusulkan dalam hubungannya dengan bukti digital. Bukti digital mempunyai keduanya aspek fisik dan logis. Sisi fisik tentangnya melibatkan komponen perangkat keras, *peripherals*, dan media, yang dapat berisi data atau bagaimana untuk mengaksesnya, selagi sisi yang logis berhadapan dengan data mentah yang diambil dari suatu sumber informasi yang pantas. Panduan Praktek Kebajikan untuk Komputer yang baik berdasarkan pada Bukti Elektronik menyarankan empat prinsip apabila berhadapan dengan bukti digital.

- 1) Tidak ada aksi yang dilakukan oleh penyelidik yang perlu merubah data yang diisi pada alat digital atau media penyimpanan.
- 2) Individu yang mengakses data asli harus berkompeten untuk melakukannya dan mempunyai kemampuan untuk menjelaskan tindakan mereka.

- 3) Suatu jejak audit atau record yang lain tentang proses diterapkan, yang pantas untuk pihak ketiga sebagai tinjauan ulang mandiri, harus diciptakan dan dipelihara, dengan meteliti dokumen masing-masing langkah investigasi.
- 4) Orang yang bertanggung-jawab atas penyelidikan mempunyai keseluruhan tanggung jawab untuk memastikan prosedur yang tersebut diatas diikuti dan sesuai dengan peraturan hukum.

Standard yang diusulkan untuk Pertukaran Bukti Digital [IOCE], menyarankan suatu yang berupa satuan utama untuk kesembuhan yang distandardisasi dari bukti berbasis komputer:

- 1) Ketika perampasan bukti digital, tindakan yang diambil mestinya tidak merubah bukti itu.
- 2) Manakala ada seseorang yang penting untuk mengakses bukti digital asli, orang itu harus berkompeten secara forensik.
- 3) Semua aktivitas berkenaan dengan *seizure* (perampasan), akses, penyimpanan, atau perpindahan bukti digital harus secara penuh didokumentasikan, dipelihara, dan tersedia untuk tinjauan ulang.
- 4) Seorang yang bertanggung jawab untuk semua tindakan rasa hormat ke bukti digital selagi bukti yang digital berada didalam pemilikan mereka.
- 5) Agen manapun yang bertanggung jawab untuk *seizing* (merampas), *accessing* (mengakses), *storing* (menyimpan), atau memindahkan bukti digital adalah bertanggung jawab untuk pemenuhan dengan prinsip ini.

Satuan tujuan prinsip diatas untuk memastikan tanggung-jawab dan integritas dari bukti digital sampai kejalan kehidupan keseluruhannya. Penanganan bukti yang sesuai selalu penting untuk dapat diterima didalam cara bekerja pengadilan. Bagaimanapun, standard berbeda dapat berlaku bagi jenis penyelidikan yang berbeda. Derajat tingkat keahlian dan pelatihan diperlukan untuk melaksanakan suatu tugas forensik yang sebagian besar tergantung bukti jujur yang diperlukan didalam kasus.

Metode Daubert, satu set standard yang bertindak sebagai suatu pemandu apabila berhadapan dengan bukti didalam suatu pengadilan, mengusulkan beberapa faktor keandalan,

yang mana harus diingat apabila menerapkan dan memberitakan suatu teknik ilmiah yang sedang digunakan didalam suatu pengujian forensik:

1. **Testability** (Testabilas) - Mempunyai teknik atau teori yang ilmiah dengan pengalaman yang diuji? Menurut K.Popper (1989) didalam *The Growth of Scientific Knowledge*, "ukuran pada status yang ilmiah dari suatu teori *falsifiability, refutability, and testability*."
2. **Acceptance** (Penerimaan) - Mempunyai teknik atau teori yang ilmiah yang diperlakukan untuk mengamati tinjauan ulang dan penerbitan? Memastikan kekurangan didalam metodologi sedang dideteksi dan bahwa teknik sedang menemukan caranya kedalam penggunaan melalui literatur itu.
3. **Credibility** (Kredibilitas) - Apa yang merupakan *qualifications* dan kecakapan tenaga ahli didalam masyarakat yang ilmiah? Mengerjakan teknik kepercayaan atas peralatan dan ketrampilan satu orang tenaga ahli yang khusus, atau dapat diduplikat oleh tenaga ahli lain di tempat lain?
4. **Clarity** (Kejelasan) - Dapatkah teknik dan hasilnya diterangkan dengan kesederhanaan dan kejelasan cukup sehingga lapangan dan dewan juri dapat memahami maksud datarannya? Ukuran ini diasumsikan untuk menjadi disatukan didalam Daubert yang secara implisit.

Secara umum, bahkan diluar pelaksanaan hukum penyelidikan, bukti harus dikumpulkan didalam suatu cara yang membuat bukti mungkin dapat diterima didalam lapangan. Mungkin tidak jelas nyata apabila suatu penyelidikan diaktifkan, sebagai contoh, apabila suatu peristiwa keamanan komputer dideteksi yang pertama, yang suatu tindakan lapangan akan terjadi. Bukti penting boleh jadi dilewatkan, dengan tidak sesuai ditangani, atau secara kebetulan dibinasakan sebelum kesungguhan hati dari peristiwa direalisasikan.

4.3 Model – model Prosedur

The Electronic Crime Scene Investigation - Suatu Pemandu untuk yang Responder Pertama, yang diproduksi oleh Departemen Keadilan U.S., menawarkan usul berikut apabila mendekati suatu pemandangan peristiwa kejahatan digital.

1. ***Securing and Evaluating the Scene*** (Mengamankan dan Mengevaluasi Peristiwa) – Langkah yang harus diambil untuk memastikan keselamatan individu dan untuk mengidentifikasi dan melindungi integritas bukti potensi.
2. ***Documenting the Scene*** (Dokumentasi suatu Peristiwa) - Menciptakan suatu catatan yang permanen menyangkut pemandangan peristiwa yang dengan teliti merekam kedua bukti konvensional dan terkait dengan digital.
3. ***Evidence Collection*** (Koleksi Bukti) - Mengumpulkan bukti digital dan tradisional didalam cara yang memelihara nilai bukti mereka.
4. ***Packaging, Transportation, and Storage*** (Pengemasan, Transportasi, dan Penyimpanan) - Mengambil tindakan pencegahan cukup ketika melakukan pengemasan, mengangkut, dan menyimpan bukti, serta memelihara rantai penjagaan.

Tanggapan Peristiwa, sebuah “Metodologi penanganan suatu peristiwa” mengusulkan tahapan berikut apabila menemui suatu peristiwa atau melakukan suatu penyelidikan digital.

1. ***Pre-incident preparation*** (persiapan Pre-Incident) - Melalui pendidikan dan pelatihan, memperoleh suatu pemahaman pada bagaimana cara bereaksi terhadap suatu peristiwa.
2. ***Detection of incidents*** (Pendeteksian peristiwa) - Mengembangkan teknik pada bagaimana cara mendeteksi orang yang dicurigai aktivitasnya.
3. ***Initial Response*** (Tanggapan Awal) - Mengkonfirmasi bahwa suatu peristiwa telah terjadi dan memperoleh bukti yang *volatile*.
4. ***Response strategy formulation*** (strategi Perumusan tanggapan) - Bereaksi terhadap peristiwa berdasar pada pengetahuan dari semua fakta yang dikenal dikumpulkan dari tahap Awal penanganan.
5. ***Duplikasi*** (forensik *backup*) - yang didasarkan atas skenario, yang manapun menciptakan suatu gambaran forensik fisik atau lakukan suatu perolehan kembali tempat bukti.
6. ***Investigation*** (Penyelidikan) - Menentukan apa yang terjadi , siapa yang melakukan dan bagaimana peristiwa dapat dicegah di masa datang.
7. ***Security measure implementation*** (mengukur implementasi Keamanan) - Menerapkan ukuran keamanan untuk mengisolasi dan berisi sistem yang terkena infeksi.
8. ***Network monitoring*** (monitoring Jaringan) - Memonitor lalu lintas jaringan untuk serangan tambahan atau berkelanjutan.

9. **Recovery** (Kesembuhan) - Mengembalikan sistem yang dipengaruhi kepada suatu jaminan, status operasional.
10. **Reporting** (Pelaporan) - detail semua Dokumen dan langkah-langkah investigasi yang diambil sepanjang insiden.
11. **Follow-Up** - Belajar dari peristiwa dengan meninjau ulang bagaimana dan mengapa hal tersebut terjadi dan membuat penyesuaian yang perlu.

Riset yang diselenggarakan di Angkatan udara U.S. mengusulkan langkah-langkah berikut apabila berhadapan dengan suatu penyelidikan forensik.

1. **Identification** (Identifikasi) - Mengenali dan menentukan jenis suatu peristiwa.
2. **Preparation** (Persiapan) - Menyiapkan *tools*, teknik, *search warrants* (surat kuasa untuk menggeledah), otorisasi, dan persetujuan manajemen.
3. **Approach Strategy** (Strategi Pendekatan) - Memaksimalkan bukti koleksi yang bersih selagi memperkecil dampak atas korban itu.
4. **Preservation** (Pemeliharaan) - Mengisolasi, menjamin/mengamankan, dan memelihara status fisik dan bukti digital.
5. **Collection** (Koleksi) – Record pemandangan fisik dan salinan bukti digital.
6. **Examination** (Pengujian) - Mencari bukti berkenaan dengan kejahatan yang dicurigai itu.
7. **Analysis** (Analisa) - Menentukan arti, fragmen rekonstruksi data, dan menarik kesimpulan berdasar pada bukti yang ditemukan. Tahap analisa boleh menghasilkan banyak perkataan berulang - ulang sampai suatu teori telah didukung.
8. **Presentation** (Presentasi) - Meringkas dan menjelaskan hal kesimpulan.
9. **Return Evidence** (Kembalian Bukti) - Memastikan fisik dan hak milik digital dikembalikan ke pemilik yang sesuai.

Masing-Masing model yang menyangkut diatas mengenai cara dan prinsip utama bukti yang berisi titik kunci yang harus dipertimbangkan ketika berhadapan dengan bukti digital. Karena tiap penyelidikan peristiwa berbeda dengan kepunyaannya yang unik dalam satuan keadaan, pendekatan tunggal mengenai cara pasti sukar untuk ditentukan. Meskipun demikian, kebanyakan sentuhan model pada kondisi pokok yang sama, meskipun demikian menekankan pada aspek berbeda. Bagian yang sisanya mengikuti suatu kerangka yang

sederhana dari empat area mengenai pokok-pokok : perolehan suatu barang yang dipamerkan, membuat suatu salinan muatan forensiknya, memperoleh bukti dari copy forensik, dan memberitakan perolehan bukti dan proses menggunakannya. Mereka berturut-turut disebut didalam dokumen ini sebagai *preservation* (pemeliharaan), *acquisition* (perolehan), *examination* (pengujian) dan *analysis* (analisa), dan *reporting* (pelaporan).

5. Pemeliharaan

Pemeliharaan bukti adalah proses mencurigai *seizure* hak milik tanpa merubah atau mengubah muatan data yang berada pada *device* dan media yang dapat dipindahkan. Hal ini merupakan langkah pertama untuk memperbaiki bukti digital. Bagian mulai dengan pengenalan umum ke pemeliharaan kemudian menyediakan lebih mendalam pada panduan PDA yang spesifik.

Pemeliharaan melibatkan pencarian, pengenalan, dokumentasi, dan koleksi dari bukti elektronik yang didasarkan. Dalam rangka menggunakan bukti dengan sukses, apakah didalam suatu pengadilan atau lebih sedikit kelanjutan formal, bukti harus dipelihara. Kegagalan dalam memelihara bukti dalam status aslinya dapat membahayakan keseluruhan penyelidikan, yang berpotensi gagal atau kehilangan informasi berharga tentang suatu peristiwa untuk selamanya.

Laporan penyelidikan Peristiwa Kejahatan Elektronik DOJ's meliputi pokok ini secara detail. Pemandu menawarkan prinsip, kebijakan, dan prosedur untuk mengikuti apabila bertemu suatu peristiwa bukti digital. Pembaca diarahkan pada laporan itu untuk informasi tambahan. Berikut adalah suatu ringkasan menyangkut titik kunci untuk mengamatinya.

1. Pengamanan dan Mengevaluasi Peristiwa

- a. Memastikan keselamatan dari semua individu di peristiwa itu.
- b. Melindungi integritas dari bukti elektronik dan tradisional.
- c. Mengevaluasi peristiwa dan merumuskan suatu rencana pencarian.
- d. Mengidentifikasi bukti potensi.
- e. Semua bukti potensi harus dijamin aman, didokumentasikan, dan dipotret.
- f. Melakukan wawancara.

2. Dokumentasi Peristiwa

- a. Menciptakan suatu catatan historis yang permanen menyangkut

peristiwa itu.

- b. Dengan teliti merekam kondisi dan penempatan komputer, media penyimpanan, alat digital lain, dan bukti konvensional.
- c. Penempatan dokumen dan kondisi dari sistem komputer, termasuk menggerakkan status menyangkut komputer (mode *on*, *off*, atau *in sleep*).
- d. Mengidentifikasi dan dokumen berhubungan komponen elektronik yang tidak akan dikumpulkan.
- e. Memotret keseluruhan peristiwa untuk menciptakan suatu record atau catatan secara visual seperti dicatat oleh responder pertama itu.

3. Pengumpulan Bukti

- a. Memegang Bukti komputer, apakah fisik atau digital, didalam suatu cara yang memelihara nilai buktinyanya.
- b. Memulihkan bukti tidak elektronik (seperti, *password* yang tertulis, catatan tangan, catatan yang kosong dengan penulisan, perangkat keras dan perangkat lunak manual, penanggalan, literatur, teks atau hasil print komputer komputer grafis, dan foto).

4. Pengemasan, Mengangkut, dan menyimpan Bukti

- a. Tidak membuat aksi untuk menambahkan, memodifikasi, atau menghancurkan data yang disimpan pada suatu komputer atau media lain.
- b. Menghindari kelembaban dan temperatur tinggi, guncangan fisik, keelektrikan statik, dan sumber magnetis.
- c. Memelihara rantai penjagaan dari bukti elektronik, dokumen pengemasannya, penyimpanan dan transportasi.

1) Prosedur Pengemasan

- a. Didokumentasi dengan baik, label, dan menginventarisir bukti sebelum dibungkus.
- b. Mengemasi media magnetis didalam pengemasan antistatic (kertas atau plastic antiseptik).
- c. Menghindari *folding* (lipatan), *bending* (kelenturan), atau penggarukan media komputer seperti disket, CD-ROMS, *removable*

media, dan lain lain

- d. Memberi bukti sebuah label dengan baik.

2) prosedur Memeriksa Transportasi

- a. Menghindari sumber magnetis (seperti, pemancar radio, *speaker magnets*).
- b. Menghindari kondisi-kondisi dari panas berlebihan, dingin, atau kelembaban selagi dalam pemindahan.
- c. Menghindari guncangan dan getaran berlebihan.

3) prosedur Memeriksa Penyimpanan

- a. Memastikan bukti disimpan menurut kebijakan yang berwenang.
- b. Penyimpanan bukti Material didalam suatu kawasan pengamanan jauh dari kelembaban dan temperatur yang ekstrim.
- c. Melindungi bukti material dari sumber magnetis, embun, debu, dan partikel unsur atau zat-pencemar berbahaya lain.

Subseksi yang sisanya menyediakan informasi bersifat tambahan berhubungan dengan PDA, mengikuti paradigma *search* (pencarian), *recognition* (pengenalan), *documentation* (dokumentasi), dan *collection* (koleksi).

5.1 Pencarian

Apabila suatu regu investigasi tiba di tempat peristiwa dengan otorisasi yang sesuai untuk menguji suatu lingkungan yang dicurigai (seperti, suatu surat kuasa untuk menggeledah, telah disetujui oleh pemilik), mereka perlu memproses dengan hati-hati dan mengikuti langkah-langkah yang perlu untuk memastikan bahwa *device* tiba di laboratorium forensik tanpa penghabisan data. Prosedur salah sepanjang *seizure* (perampasan) dapat menyebabkan hilangnya informasi kritis. Kesadaran isu spesifik *device* dan suatu pemahaman berbagai keluarga *device* dan aksesoris dan karakteristik mereka (seperti, pemakaian power, tipe baterai, *cradles* (mengayun), dan *power supplies* (pengadaan persediaan)) adalah penting.

Untuk PDA, sumber bukti meliputi *device*, *device cradle*, *power supply*, dan *associated*

peripherals, media, dan aksesoris. Media dapat dipindahkan bervariasi dari ukuran suatu perangkat ke suatu tongkat, yang mana dapat bersembunyi dan sangat sukar untuk ditemukan. Paling sering media yang dapat dipindahkan dapat dikenali lewat penempatan dan nomor pin atau seperti penampung pin yang ditempatkan pada media yang menetapkan suatu *device* penghubung dengan *device* pada PDA. Lingkupan area dan ruang selain dari mana *device* yang ditemukan harus dicari untuk memastikan bukti terkait tidak dilewatkan. Peralatan dihubungkan dengan PDA, seperti komputer pribadi atau kartu memori yang sama dengan PDA, mungkin yang lebih berharga dibanding PDA sendiri.

Secara kebetulan atau tindakan sengaja, peralatan elektronik mungkin ditemukan dalam keadaan dirusakkan. Media atau *device* dengan kerusakan eksternal kelihatan tidak perlu mencegah data yang sedang disadap dari mereka. Peralatan yang dirusakkan harus ditarik kembali ke laboratorium untuk penyelidikan lebih lanjut. Perbaikan komponen yang dirusakkan pada suatu perbaikan dan *device* itu bekerja untuk analisa dan pengujian adalah mungkin. Komponen memori boleh juga diperbaiki di tempat itu, atau dipindahkan dan yang diuji oleh suatu pemeriksa yang terlatih.

Penasehat hukum harus dihubungi untuk bantuan, jika diperlukan, dengan dua pertimbangan berikut mengenai undang-undang kritis :

1. Menentukan tingkat penguasa untuk mencari dan memproses apa yang sah mengenai undang-undang tambahan mungkin perlu untuk melanjutkan pencarian itu (seperti, menjamin keabsahan, persetujuan yang berkembang terbentuk), jika bukti yang ditempatkan tidak diberi hak didalam otoritas pencarian yang asli.
2. Mengidentifikasi perhatian mungkin berhubungan dengan hukum dan kebijakan lokal dapat diterapkan, dan Internasional, Pemerintah pusat, atau status bagian, seperti *Electronic Communications Privacy Act* tahun 1986 (ECPA) dan *the Cable Communications Policy Act* (CCPA).

5.2 Pengenalan

Untuk diproses secara efektif, jenis *device* yang tepat harus dikenali. Individu dapat mencoba untuk merintangi spesialis dengan mengubah *device* untuk merahasiakan identitas sebenarnya. Perubahan *device* dapat terbentang dari memindahkan label pabrikan untuk pergi berbaris menjadi satu logo. Sebagai tambahan, sistem operasi mungkin dimodifikasi dengan sepenuhnya digantikan dan nampak dengan cara yang berbeda, seperti halnya bertindak

dengan cara yang berbeda dibanding sebelumnya.

Jika alat digital seperti PDA dalam keadaan "**on**" menyatakan jenis *device* yang dapat dikenali oleh sistem operasi, yang lebih konsisten dalam identitas *device* dibanding suatu logo. Meskipun demikian dua sistem operasi dominan adalah Pocket PC dan Palm OS, PDA dihasilkan untuk berjalan pada satu sistem operasi yang dapat menjalankan sistem operasi alternatif. Sebagai contoh, distribusi Linux yang tersedia dari handhelds.org dapat terisi dan dimajukan berbagai Pocket PC *device*. dengan cara yang sama, versi Linux, seperti Linux DA, ada untuk Palm OS *device*.

Masing-Masing sistem operasi mempunyai aplikasi tertentu yang terjaln didalam *device* penghubung pemakai grafis yang utama (yaitu, *icon* seperti *Word*, *Explorer*, *Memo Pad*, *Terminal*, dan lain-lain). Kunci rahasia lain yang mengijinkan identifikasi dari suatu *device* berikut adalah : *the cradle interface*, *manufacturer serial number*, *the cradle type*, *power supply*, dan lain lain. Sinkronisasi perangkat lunak menemukan suatu PC dihubungkan juga untuk membantu membedakan antar keluarga sistem operasi.

5.3 Dokumentasi

Bukti harus dengan teliti dibukukan dan dikenali. Proses label perlu mendokumentasikan nomor kasus, suatu uraian ringkas, tandatangan, waktu dan tanggal bukti dikumpulkan. Apalagi, peristiwa kejahatan harus dipotret di samping status laporan dokumen dari tiap *device* personal komputer digital (komputer pribadi boleh berisi data bermanfaat yang belum disamakan dengan PDA pemilik). Ini sangat menolong jika ditanyakan tentang lingkungan kemudian.

Suatu record atau catatan dari semua data harus diciptakan. Semua alat digital (PDA) itu mungkin dapat menyimpan data dan harus dipotret dengan semua *peripherals cables*, *cradles*, *power connectors*, *removable media*, and *connections*. Jika alat berada dalam suatu status aktif atau semi-active, muatan layar harus dipotret dan, jika perlu, direkam dengan tangan. Karakteristik lain seperti aktifitas LED (seperti, *blinking*) atau konektifitas fisik perlu juga dicatat. Setelah perorangan yang berwenang melaksanakan tugas penjaga bukti di tempat peristiwa, di samping suatu mitra yang bertanggung jawab untuk dokumentasi bukti, adalah diinginkan sepanjang tahap koleksi.

Tindakan yang diterima sistem untuk melihat dan merekam data *volatile* tidak dipertunjukkan ketika mempengaruhi bukti sisanya. Sebagai contoh, menjalankan suatu

aplikasi untuk melihat alokasi memori atau proses akan menjalankan overwrite bagian dari memori. Lebih dari itu, resiko yang akan mengaktifkan kode tersembunyi *Trojan horse* didalam aplikasi itu.

Rantai prosedur penjagaan adalah prosedur sederhana sekalipun belum begitu efektif proses dari dokumentasi perjalanan bukti yang lengkap sampai kepada *lifecycle* dari kasus tersebut. Secara hati-hati memelihara rantai penjagaan yang tidak hanya melindungi integritas bukti, tetapi juga membuat yang sulit untuk seseorang yang membantah bahwa bukti dirusakkan. Dokumentasi perlu menjawab pertanyaan berikut :

1. Siapa yang mengumpulkan itu? (yaitu, alat, media, berhubungan sekeliling)
2. Bagaimana dan di mana? (yaitu., bagaimana bukti dikumpulkan dan di mana bukti terletak)
3. Siapa yang mengambil pemilikan tentangnya? (yaitu., individu yang bertanggung-jawab pada saat pengambilan bukti)
4. Bagaimana bukti itu disimpan dan dilindungi didalam penyimpanan? (yaitu., prosedur *evidence-custodian*)
5. Siapa yang mengeluarkan bukti dari tempat penyimpanan dan mengapa? (yaitu., nama individu yang bertanggung jawab mendokumentasikan dokumentasi dan tujuan untuk *check-out* bukti)

Dokumentasi bagi semua pertanyaan diatas harus dirawat dan disimpan didalam suatu jaminan penempatan untuk acuan sekarang dan yang akan datang.

5.4 Koleksi

Dimana PDA terkait, proses koleksi secara normal melibatkan informasi yang *volatile* dan dinamis yang mungkin hilang kecuali jika tindakan pencegahan diambil di tempat peristiwa kejahatan atau kejahatan. "Panduan Praktek Kebaikan untuk Komputer Mendasarkan Bukti Elektronik" menyarankan prosedur berikut manakala berhadapan dengan PDA:

- 1) Pada saat *seizure* (perampasan), PDA harus tidak dinyalakan, jika telah off.
- 2) PDA harus ditempatkan didalam suatu amplop kemudian disegel sebelummen jadi dimasukkan kedalam suatu kantong bukti, untuk membatasi akses fisik walaupun masih disegel didalam kantong bukti.

- 3) Jika PDA dicoba dengan hanya baterai setruman tunggal, kekuatan adaptor yang sesuai harus dihubungkan ke alat dengan kabel yang melintasi kantong bukti sedemikian sehingga bukti dapat disimpan untuk tugas.
- 4) Jika PDA dinyalakan manakala ditemukan, alat harus ditahan dalam keadaan aktif (seperti, dengan *tapping on a blank section of the screen*) dan disediakan power sampai suatu tenaga ahli dapat mengujinya, untuk menghindari konsekuensi dalam mengaktifkan mekanisme keamanan seperti isi dan pengesahan pemakai *encryption*. Jika power cukup tidak bisa disediakan, pertimbangan harus diberikan dengan mematikan PDA untuk memelihara hidup baterai, dokumen alat yang sekarang menyatakan dan mencatat waktu dan tanggal dari *shutdown*.
- 5) Suatu pencarian harus dilaksanakan untuk dihubungkan pada memori *device*, seperti SD, MMC, atau CF kartu semikonduktor, *microdrives*, dan USB.
- 6) Power manapun, kabel, atau *cradles* berkenaan dengan PDA perlu juga ditangkap, seperti halnya manual.
- 7) Seseorang yang menangani PDA sebelum pengujian perlu diperlakukan sedemikian rupa sehingga mengakui memberikan kesempatan yang baik dalam *me-recover* data sebagai bukti didalam proses selanjutnya.

Memelihara data pemakai pada PDA didalam suatu status *volatile* yang bertenaga mesin baik oleh suatu baterai yang bersifat alkali maupun sumber baterai ion litium. Disain *device* menentukan jenis sumber baterai yang disajikan baterai mungkin dapat diganti atau bisa disetrum kembali. Jika *device* kehilangan power terlalu lama, kesempatan untuk penyembuhan semua data dari *device* yang ditangkap tidak mungkin terjadi. Sebelum suatu teknisi dapat mengantongi suatu PDA, bagian power sekarang sangat dipertimbangkan. Sebagai contoh, *device* mungkin menerima power dari suatu ayunan diisi kedalam suatu saluran dengan penuh, baterai mungkin telah baru-baru ini dipindahkan dari *device* ke memori yang bersih, atau *device* mungkin dalam keadaan lemah power baterainya.

Dalam keadaan dimana *device* diberi power baterai bersifat alkali, baterai baru harus dimasukkan secepat mungkin untuk mengurangi kerugian data sebelum bukti diperoleh. Penerapan baterai baru adalah suatu aktivitas normal untuk PDA, terutama yang berjalan pada *device* berbasis alkaline. Bagaimanapun, menarik baterai keluar dan menerapkan baterai penggantian berubah status dari *device*. oleh karena itu, teknisi perlu memperhatikan status

sekarang dari *device* dahulu, bersama dengan foto yang diperlukan.

Device yang bertenaga sumber baterai lithium-ion yang manapun perlu diisi kedalam *cradle* yang dipertukarkan dengan suatu sumber power, atau mempunyai baterai pengganti penuh untuk menggantikan baterai yang didalam. Jika suatu ayunan ditemukan di tempat peristiwa yang sedang sibuk dengan *device*, ayunan pertama perlu diputus dari computer manapun dimana komputer dipasang. Selama penggantian baterai, PDA menyimpan suatu kapasitansi kecil ke *device* untuk memelihara data *volatile* dalam waktu singkat. Begitu, baterai harus digantikan dengan cepat untuk mencegah hilangnya data.

Untuk memelihara power, PDA secara normal diatur untuk *off* setelah suatu ketidakaktifan jangka pendek. Oleh karena itu, mereka kebanyakan seperti diberi *power off* ketika ditemukan. Jika suatu PDA *power on* pada saat ditemukan, pemeliharaan suatu *device* didalam suatu mode aktif menyebabkannya pengkonsumsian power lebih dibanding jika diberi *power off* dan non-aktif, membuat penggantian baterai dan pertimbangan *charging* lebih penting lagi. Bukti *anekdot* menyatakan bahwa pengesahan pemakai *built-in* dan kemampuan mengisi *encryption* tidak dipekerjakan untuk mayoritas luas PDA yang ditangkap. Oleh karena itu, jika power tidak bisa disediakan untuk suatu *device*, dan PDA dipadamkan untuk memelihara power dan perlindungan isi memori, resiko dalam mengaktifkan mekanisme keamanan seperti itu manakala *device* dipasang lagi haruslah rendah. Menjaga agar sebuah *device* dalam keadaan aktif dapat membuat masalah juga. Bagaimanapun Mekanisme Pemeliharaan, seperti *passwords*, biasanya tidak dapat di *turned off* tanpa memuaskan mekanisme tersebut (seperti, menyediakan *password* yang benar). Karena pertimbangan ini, prosedur untuk beberapa organisasi boleh merekomendasikan pemadaman kelas PDA tertentu atau membiarkan mereka memadamkannya secara otomatis, jika power ditemukan terpasang on.

5.4.1 Exacerbating Conditions / kondisi yang buruk

Di samping tingkatan baterai, faktor lain yang dapat mempengaruhi tindakan seorang teknisi dalam menerima situasi yang ditentukan untuk memelihara bukti apabila *device* ditemukan didalam suatu status. Sebagai contoh, beberapa *device* dapat menerima data *wireless networks* yang mungkin mendukung bukti baru, tetapi dapat membuat *overwrite* data yang ada. Oleh karena itu, penghitungan suatu keputusan harus dibuat apakah untuk mencegah atau mengijinkan komunikasi *wireless* lebih lanjut. Faktor lain meliputi apakah

device diayun, sedang disamakan dengan komunikasi melalui suatu *host* komputer, atau mempunyai suatu kartu memori yang dimasukkan. Tabel 5.1 menyediakan daftar kondisi-kondisi umum dan tindakan yang dihubungkan untuk teknisi forensik untuk dipertimbangkan dalam menemui maksud yang dikenali itu.

No.	Kondisi atau Tujuan	Aksi
1.	Device ON	<ul style="list-style-type: none"> • Tinggalkan device dalam keadaan “on” dan tetap aktif. • Jika level baterai sudah rendah, segera ganti dengan yang baru atau disarankan untuk men-charge baterai dengan power adaptor device. • Memelihara level baterai dengan power adaptor device atau penggantian baterai secara berkala. • Ciptakan gambaran pada device ketika keadaan diizinkan.
	<ul style="list-style-type: none"> • Memelihara device dalam keadaan aktif dengan mengukur level power yang cukup. • Memperoleh gambar pada kesempatan paling awal. 	
2.	Device OFF	<ul style="list-style-type: none"> • Tinggalkan device dalam keadaan “off”. • Secepatnya ganti baterai dengan yang baru, atau secara berkala diganti dengan yang baru, atau disarankan untuk di charge dengan power adaptor device. • Ciptakan gambaran pada device ketika keadaan diizinkan.
	<ul style="list-style-type: none"> • Memelihara ukuran level power pada device. • Memperoleh gambar pada kesempatan paling awal. 	
3.	Device dalam cradle	<ul style="list-style-type: none"> • Tarik USB sebagai alat penghubung koneksi dari computer • Jika kondisi device “on” lihat kondisi 1 • Jika kondisi device “off” lihat kondisi 2 • Tarik cradle-nya
	<ul style="list-style-type: none"> • Hapus kemungkinan aktifitas komunikasi lebih lanjut. 	
4.	Device diluar cradle	<ul style="list-style-type: none"> • Jika kondisi device “on” lihat kondisi 1 • Jika kondisi device “off” lihat kondisi 2 • Tarik cradle-nya
	<ul style="list-style-type: none"> • Kumpulkan material bukti-bukti yang saling berhubungan. 	
5.	Wireless (Wi-Fi, Bluetooth, dan lain-lain) ON	<ul style="list-style-type: none"> • Lihat kondisi 1 • segera bungkus alat dalam suatu amplop, kantong anti-static, dan suatu kotak pengasingan dengan perbandingan frekwensi, hapus kemungkinan koneksi dari alat atau mesin yang lain.
	<ul style="list-style-type: none"> • Hapus kemungkinan aktifitas komunikasi lebih lanjut. 	
6.	Wireless (Wi-Fi, Bluetooth, dan lain-lain) OFF	<ul style="list-style-type: none"> • Lihat kondisi 1. • Segera bungkus alat untuk mengurangi aktifitas wireless yang sedang terjadi.
	<ul style="list-style-type: none"> • Kumpulkan material bukti-bukti yang saling berhubungan. 	
7.	Kartu dalam kartu expansion	<ul style="list-style-type: none"> • Hindari pemindahan peripheral atau kartu media apapun, seperti (CF, SD, MMC)
	<ul style="list-style-type: none"> • Menghindari aktifitas didalam alat lebih lanjut lagi. 	
8.	Kartu tidak dalam kartu expansion	<ul style="list-style-type: none"> • Tarik hubungan peripheral atau kartu media apapun, seperti (CF, SD, MMC)

No.	Kondisi atau Tujuan	aksi
	<ul style="list-style-type: none"> Kumpulkan material bukti-bukti yang saling berhubungan. 	
9.	Expansion Sleeve Attached	<ul style="list-style-type: none"> Hindari pemindahan expansion sleeve Hindari pemindahan peripheral atau kartu media (contoh CF, SD, MMC) dari sleeve Jika wireless dan network terjadi koneksi, lihat kondisi 5
	<ul style="list-style-type: none"> Menghindari aktifitas didalam alat lebih lanjut lagi. 	
10.	Expansion Sleeve Removed	<ul style="list-style-type: none"> Ukur expansion sleeve Ukur peripheral dan kartu media (contoh CF, SD, MMC) yang saling terhubung.
	<ul style="list-style-type: none"> Kumpulkan material bukti-bukti yang saling berhubungan. 	

Tabel 5.1 Action Matrix

5.4.2 Modifikasi Device

Sejumlah pertimbangan perlu dibuat apabila sedang menangani suatu *device*. Sebagai contoh, menekan tombol power, tombol sinkronisasi, atau kontak *PIM-related*, penanggalan, *to-do list*, dan tombol tugas pada *device* bisa berpotensi meneruskan suatu perubahan status. Yang lebih menarik, bagaimanapun, adalah modifikasi aplikasi perangkat lunak dan sistem operasi yang mungkin telah dibuat oleh devices, yang mana bisa dipicu dari tindakan ini. Berikut adalah daftar kelas modifikasi yang umum yang dapat terjadi:

- 1) **Key Remapping** – Key remapping ini secara relatif langsung untuk memetakan kembali suatu kunci perangkat keras untuk melihat suatu fungsi berbeda dibanding kegagalan itu. Keseluruhan, *key press* atau kombinasi dari *key press* dapat dibuat untuk meluncurkan suatu program yang sewenang-wenang.
- 2) **Malicious Programs** - fungsi atau kegunaan umum dapat digantikan dengan versi yang berisi *Trojan horse* yang dirancang untuk mengubah atau merusakkan data yang disajikan pada *device* itu. Sebagai contoh, *tools* yang ada mengijinkan para pemakai untuk menangkap, membaharui, dan menggantikan gambaran ROM dengan aplikasi yang lebih disukai, seperti ditingkatkan dari *Web browsers*. Program *Trojan-Bearing* kondisinya dapat diaktifkan didasarkan pada kondisi-kondisi seperti kunci *interrupt* perangkat keras atau parameter masukan. Aplikasi *Watchdog* dapat juga ditulis untuk mendengarkan untuk peristiwa tali kunci yang spesifik dan menyelesaikan tindakan seperti membersihkan *device*.

- 3) **Security Enhancements** (Peningkatan Keamanan) - Banyak individu dan organisasi meningkatkan *handheld devices* mereka dengan tambahan mekanisme keamanan. Berbagai login visual, biometric, dan mekanisme pengesahan *token-based* tersedia untuk penggunaan sebagai tenaga pengganti atau lampiran ke mekanisme *password*. Interaksi yang tidak pantas dengan suatu mekanisme dapat menyebabkan *device* mengunci dan bahkan menghancurkan muatannya. Ini terutama sekali merupakan suatu perhatian sebagai tanda keamanan atas kehadiran siapa yang konstan dimonitor dan kepindahan siapa dari kartu slot atau *device* penghubung *device* lain dengan seketika dilaksanakan.

5.4.3 Transportasi dan media penyimpanan

Ketika *device* siap untuk ditangkap, spesialis forensik perlu menyegel *device* dalam suatu label dan kantong bukti statis. Individu yang menangkap *device* harus menandai dan menanggali dengan label untuk memulai suatu rantai penjagaan. Suatu kasus yang sulit, dimana lapisan yang internal dapat menyesuaikan diri dengan berbagai bentuk *device*, akan bersifat lebih baik dengan menggunakan suatu pembungkus didalam kantong bukti untuk mencegah kunci dari yang sedang ditekan secara kebetulan. Frekwensi radio kantong pengasingan yang ada untuk memotong siaran radio dan penerimaan *device* harus digunakan sesuai dengan PDA yang mempunyai kemampuan *wireless*. Suatu eksternal *charger* yang mandiri akan dihubungkan dan ditempatkan didalam kantong dengan *device* untuk menyimpan ukuran power penuh selama pemindahan. *Device* dapat juga dibungkus untuk mengijinkan suatu adaptor yang dihubungkan kepada *device* melalui suatu lubang dalam kantong, sebagai alat-alat untuk memelihara power berukuran tinggi. Lithium-Ion *device* pada umumnya bertenaga mesin suatu dapat dipertukarkan kabel *cigarette-lighter* untuk menyimpan beban ke *device* selagi dalam pemindahan. Jika suatu kabel digunakan disuatu kantong frekwensi radio pengasingan, kabel harus dengan baik dilindungi untuk mencegahnya dari bertindak sebagai suatu penghapusan dan efek antena dari kantong pengasingan.

Alat digital mudah pecah dan mudah dirusakkan. Apabila suatu alat diangkut, haruslah ditangani secara hati-hati dan cukup dilindungi dari goncangan, kerusakan, dan temperatur ekstrim. Dalam kaitan dengan status PDA yang *volatile*, mereka perlu dicek ke dalam suatu laboratorium forensik untuk diproses dan penjaga bukti dibuat sadar akan situasi mengenai kebutuhan power. *Device* bertenaga baterai menyimpan dalam penyimpanan untuk lebih dari

beberapa hari mengambil resiko kerugian data dan penghabisan kuasa, kecuali jika suatu proses pada tempatnya untuk menghindari hasil ini.

Fasilitas penyimpanan yang memegang bukti perlu menyediakan suatu lingkungan yang dingin, lingkungan yang kering sesuai dengan peralatan elektronik berharga. Semua bukti harus dalam kontainer yang disegel, didalam suatu kawasan pengamanan dengan akses yang dikendalikan.

6. Akuisisi

Acquisition adalah proses dalam menggambarkan atau memperoleh informasi dari suatu alat digital dan media dan peralatan sekelilingnya. *Acquisition* terjadi pada suatu laboratorium forensik ketika informasi yang ditangkap telah dengan aman didaftar. Keuntungan dalam melakukan *Acquisition* di tempat peristiwa adalah bahwa hilangnya informasi dalam kaitan dengan penghabisan baterai, kerusakan, dan lainnya dapat dihindarkan. Bagaimanapun, menemukan suatu pengaturan yang dikendalikan digunakan untuk bekerja, mempunyai peralatan yang sesuai, dan memuaskan prasyarat lain yang tidak boleh terjadi di peristiwa, tetapi sebagai gantinya tersedia didalam suatu laboratorium yang telah diatur. Untuk kepentingan diskusi, didalam bagian ini suatu lingkungan laboratorium yang diasumsikan.

Sekali ketika *device* telah tiba di laboratorium forensik, pemeriksa forensik memulai *Acquisition* dengan mengidentifikasi *device*. Tipe dari alat dan Jenis sistem operasi dapat menentukan rute untuk melihat ciptaan dari suatu bunyi gambaran *bit-for-bit* atau jika tidak memperoleh muatan dari *device*. Hanya sedikit perangkat lunak *forensic tools* yang berbeda dengan gambaran PDA sekarang ini ada dan tak seorangpun aplikasi yang segera menangani cakupan *device* yang penuh pada pasar. Jenis PDA dan sistem operasi, oleh karena itu, biasanya mendikte aplikasi mana yang digunakan dalam suatu penyelidikan.

Secara normal, *forensik toolkit* menggunakan *acquisition* juga untuk analisa dan pengujian. Di mana ada suatu pilihan diantara beberapa *tools*, seperti Palm OS *device*, *interoperability* antar fasilitas pengujian dan *acquisition* mungkin hadir, seperti ditunjukkan dalam Tabel 6.1. Masukan ditempat itu menunjukkan hasil data diperoleh dengan satu *device*, yang ditandai oleh *row header*, yang dianalisa oleh yang lain, yang ditandai oleh *column header*. *Interoperability* suatu aspek penting untuk pertimbangan, karena beberapa *tools* mungkin terbatas pada sistem operasi versi spesifik atau tidak boleh mendukung model *device* tertentu. Lebih dari itu, adakalanya satu *tool forensik* dapat gagal untuk memperoleh informasi dari suatu spesifik *device*, selagi *device* yang lain bekerja tanpa permasalahan.

	POSE	PDA Seizure	EnCase
Pdd	Menerima gambar ROM, tapi pdd tidak memberikan output database sendiri	Menerima gambar ROM dan RAM yang diproduksi, hanya dengan fungsi parsial	Menerima gambar ROM dan RAM yang diproduksi
Pilot-Link	Menerima gambar ROM dan database sendiri yang diciptakan berturut-turut dengan pi-getrom dan pilotx-fer	Menerima gambar ROM dan database sendiri yang diciptakan berturut-turut dengan pi-getrom, pi-getram dan pilotx-fer	Menerima gambar ROM dan database sendiri yang diciptakan berturut-turut dengan pi-getrom, pi-getram dan pilotx-fer
PDA Seizure	Membangun versi POSE yang menerima output yang diperoleh secara implicit	Bekerja secara implisit	Menerima gambar ROM dan RAM yang diproduksi
EnCase	Menerima database yang diproduksi sendiri	Menerima gambar ROM dan RAM yang diproduksi, dengan hanya fungsi parsial.	Bekerja secara implisit

Tabel 6.1 Interoperability Among Palm OS Tools

Pemeriksa forensik diberi petunjuk untuk mengadakan percobaan dengan berbagai *toolkits* pada *test device* untuk menemukan *tools* yang dapat bekerja secara efisien dengan jenis *device* tertentu, dan untuk menentukan derajat tingkat *interoperability* antar *tools* pengujian dan *acquisition* berbeda untuk suatu keluarga *device*. Di samping memperoleh keakraban dengan kemampuan dari *device*, percobaan mengijinkan wujud kebiasaan dan campuran konfigurasi khusus untuk disediakan sebelum penggunaan dalam suatu kasus nyata. Sebagai tambahan, perangkat lunak yang diperbaharui dari pabrik dapat diinstall.

Bukan masalah apakah *device* adalah Pocket PC, Palm OS, atau berbasis Linux, untuk memperoleh data dari itu, suatu koneksi harus dibentuk dari *workstation* spesialis forensik kepada *device* tersebut. Sebelum melakukan suatu *acquisition*, versi dari *device* yang sedang digunakan harus didokumentasikan, bersama dengan kesalahan tulis manapun atau tambalan bisa diterapkan dari pabrik dan berlaku untuk *device* tersebut. Sekali ketika koneksi telah dibentuk, deretan perangkat lunak forensik dapat mulai memperoleh data dari *device* dengan baik.

Tidak sama dengan *network server* atau mesin *desktop* terbaru kini PDA tidak punya perangkat keras dan mempercayakan memori semikonduktor sebagai ganti dengan sepenuhnya. Perangkat lunak yang khusus ada untuk memproduksi suatu gambaran *device*, seperti halnya melakukan suatu pengadaan logis data PIM. Bagaimanapun, muatan dari suatu PDA adalah dinamis dan secara terus menerus berubah, bahkan ketika dimatikan (yaitu,

dalam status diam). Dua pengadaan suatu *device back-to-back* menggunakan *device* yang sama menghasilkan hasil berbeda secara keseluruhan, meskipun mayoritas informasi, seperti data PIM, tinggal tanpa perubahan. Untuk gambaran suatu PDA memori *device*, *device* harus dinyalakan, yang mana merupakan suatu perbedaan utama dari komputer pribadi. Ini secara efektif berarti prinsip *evidentiary* yang pertama tersebut dibagi dalam 4 bagian – *actions taken should not modify data contained on the device* - tidak bisa mentaati, pada hakekatnya. Oleh karena itu, tujuan PDA *acquisition* akan mempengaruhi muatan memori sedikit sama seperti mungkin dan kemudian hanya didalam pengetahuan dari apa yang sedang terjadi secara internal, menempatkan lebih penting pada kesetiaan yang memastikan kepada yang kedua dan prinsip ketiga *evidentiary*, yang mana menekan kemampuan dari spesialis dan pembuatan suatu jejak audit terperinci.

Setelah suatu *acquisition* selesai, spesialis forensik perlu selalu mengkonfirmasi bahwa keseluruhan muatan dari suatu *devices* ditangkap dengan tepat (yaitu, memverifikasi ukuran RAM/ROM yang memastikan konsistensi dengan *device*). Pada kesempatan, suatu *device* boleh gagal dari tugasnya tanpa pemberitahuan kesalahan dan memerlukan spesialis untuk mencobanya kembali dengan baik *device* yang sama maupun *device* yang lain. Dengan cara yang sama, beberapa *tools* tidak bekerja baik dengan *device* tertentu sebagai yang orang lain lakukan, dan boleh gagal dengan suatu pemberitahuan kesalahan. Begitu, manakala mungkin, adalah sebaiknya untuk mempunyai berbagai *tools* tersedia.

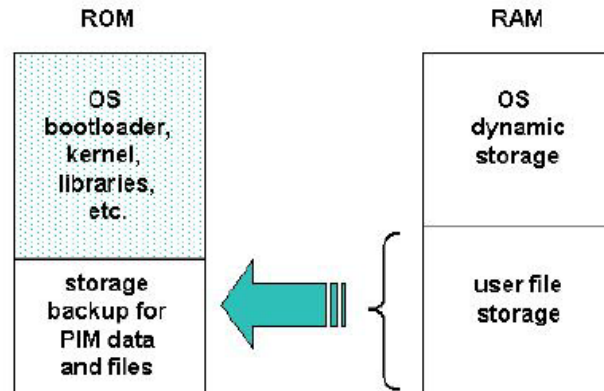
6.1 Unobstructed Device (Device yang tidak dihalangi)

Suatu *device* yang tanpa halangan adalah suatu *device* yang tidak memerlukan suatu *password* atau teknik pengesahan lain untuk dicukupi untuk diwarisi akses kepada *device* itu. Dari informasi *anekdot*, kebanyakan *device* ditangkap didalam penyelidikan terlihat masuk ke kategori ini. Seperti disebut lebih awal, apabila perampasan suatu "Unobstructed Device " perhatian harus digunakan untuk menghindari, sebagai contoh, mengubah status dari *device* dengan menekan urutan tali kunci yang mempunyai potensi untuk merusak atau menghapus bukti berharga.

Secara umum, sebuah PDA mempunyai empat kategori penyimpanan yang utama untuk mempertimbangkan kode sistem operasi, mencakup *kernel* (inti), *device drivers*, dan *system libraries* dengan dinamis dialokasikan untuk pelaksanaan aplikasi sistem operasi dan menyimpan dan melaksanakan aplikasi pemakai tambahan memuat ke alat, penyimpanan

pemakai untuk berbagai jenis data file, mencakup teks, gambaran, dan bunyi dan data kritis backup ttg aplikasi informasi PIM dan data file. Karakteristik empat kategori ini terbentang dari yang sangat stabil ke yang *volatile*. Perbedaan ini dikombinasikan dengan karakteristik dari suatu sistem operasi spesifik, menentukan bagaimana ROM dan RAM digunakan untuk mendukung masing-masing kategori penyimpanan.

Gambar 6.1 menggambarkan pengaturan yang paling khas. *Flash* ROM yang digunakan sebagian besar untuk memegang kode sistem operasi dan secara bebas memilih data PIM manapun atau file yang di-*backup* oleh pemakai kedalam ruang yang sisanya itu. *Flash memory* mempunyai suatu waktu yang terbatas kira-kira 100,000 siklus untuk menghapus. RAM digunakan untuk penyimpanan yang dinamis dan penyimpanan file pemakai. Suatu *soft reset* (yaitu, *warm boot*) yang secara khas me-*reinitializes* penyimpanan yang dinamis didalam RAM, tetapi daun-daun file penyimpanan pemakai tidak disentuh, sedang suatu *hard reset* (yaitu, *cold boot*) me-*reinitializes* keduanya. Dengan sepenuhnya mengalirkan power dari PDA mempunyai efek yang sama sebagai efek yang keras. ROM tidak dibuat baik oleh suatu reset lembut maupun yang keras.

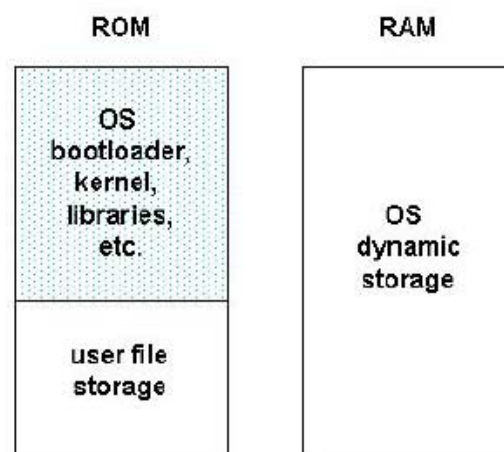


Gambar 6.1 ROM/RAM Storage Assignments

Suatu pengaturan memori alternatif umum ditunjukkan dalam Gambar 6.2. Di sini pemakai file penyimpanan yang berada dalam *Flash* ROM dengan kode sistem operasi, yang mana menghindari kebutuhan akan kegunaan *backup*, karena penyimpanan tidak dibuat terus-menerus dan tidak dipengaruhi oleh reset dan aliran power. Ukuran ROM dan RAM secara normal normalnya berukuran berbeda (yaitu, ROM lebih RAM dan lebih sedikit) apabila dibandingkan dengan pengaturan yang lebih awal untuk menyediakan kapasitas setaraf. Untuk

menyimpan file penyimpanan pemakai didalam ROM melawan RAM, suatu *filesystem* khusus diperlukan untuk menghindari percepatan hidup media tersebut. File sistem seperti JFFS2 (The Journaling Flash File System, version 2) dirancang secara rinci untuk mengatur pemakaian *flash memory* yang secara hati-hati. Sebagai contoh, JFFS2 mencegah menulis kembali dari suatu keseluruhan sektor untuk menghapus *byte* tunggal dan memastikan bahwa lingkup memori yang berbeda digunakan bergiliran untuk mengatur pemakaian.

Karena terbatasnya jumlah *tools forensik* yang ada untuk pengadaan muatan ROM dan ROM dari suatu PDA, pilihan sederhana sering jadi. Satu pertimbangan utama akan memelihara kecocokan dengan *toolkit* yang secepatnya yang digunakan didalam analisa dan pengujian, karena interoperabilitas antar PDA *tools* berbeda, terutama kasus komersil file format, adalah tidak dijamin.



Gambar 6.2 Alternative ROM/RAM Assignments

Dalam rangka memelihara integritas data, pemeriksa perlu menangani bukti yang asli mungkin lebih sedikit sama. Biasanya, direkomendasikan untuk menciptakan sebuah "master" *forensik* salinan *device* dulu, yang mana dijaga dengan murni sepenuhnya. Copy master kemudian digunakan untuk menciptakan gambaran cermin tambahan untuk pengujian dan analisa bukti. Suatu jalan kuat searah *cryptographic hash* (seperti: SHA1) harus dilakukan untuk memastikan bahwa gambaran tambahan yang diciptakan copy dari master adalah serupa.

6.2 Obstructed Devices (Device yang dihalangi)

Device yang dihalangi mengacu pada *device* yang ditutup (yaitu, dalam status diam) dan memerlukan *authentication* yang sukses menggunakan *password* atau beberapa alat-alat lain untuk memperoleh akses. *Password* melindungi *device* yang secara normal memerlukan keahlian dari suatu spesialis forensik secara khusus dilatih untuk memperoleh akses ke muatan *device*, selagi pemeliharaan integritas menyangkut informasi dan menghindari kerusakan pada *device* tersebut. Sejumlah jalan ada untuk menyadap data dari *device* yang dihalangi. Mereka masuk kedalam tiga kelas: *investigative*, *metoda hardware-based* dan *software-based*.

Perangkat lunak dan metoda *hardware-based* sering dikembangkan terutama untuk *device* tertentu atau membatasi kelas *device*. Didalam mengembangkan suatu metoda, tindakan berikut harus dipertimbangkan untuk menentukan pendekatan yang mungkin:

- a) Menghubungi *device* pabrik untuk informasi yang dikenal *backdoors* dan sifat mudah diserang yang boleh jadi dimanfaatkan.
- b) Meninjau ulang spesifikasi pabrik dan dokumentasi lain apabila perumusan eksploitasi masuk akal.
- c) Menghubungi para profesional *me-recover* bukti omersil yang mengkhususkan dalam *handheld devices*.
- d) Menghubungi pemelihara *devices* dan perusahaan perbaikan, seperti halnya organisasi komersil yang menyediakan informasi arsitektur pada *handheld devices products*.

6.2.1 Metode Investigasi

Metoda Investigasi adalah prosedur regu isvestigasi yang dapat diterapkan, yang mana tidak memerlukan perangkat lunak atau perangkat keras *tools forensik*. metoda yang paling jelas nyata adalah sebagai berikut:

- 1) *Ask the suspect* (menanyai orang yang dicurigai) - Jika suatu *device* dilindungi dengan kata sandi, pin, tanda, atau mekanisme pengesahan lain yang menyertakan pengesahan berbasis pengetahuan, orang yang dicurigai dapat disangsikan untuk informasi ini sepanjang wawancara awal.
- 2) *Review seized material* (meninjau ulang material penangkapan) - *password* sering

dituliskan pada suatu catatan dan yang dijaga dengan atau dekat *device*, pada suatu komputer desktop yang digunakan untuk mencocokkannya dengan *device*, atau pada orang-orang yang dicurigai, seperti didalam suatu dompet, dan mungkin diperbaiki melalui inspeksi visual.

- 3) *Manually supply commonly used input* (Mengirimkan masukkan yang digunakan secara manual) - Para pemakai boleh memperlemah suatu mekanisme yang digunakan. Sebagai contoh, jika suatu *device* memerlukan suatu 4-digit pin, suatu pemeriksa boleh ingin mencoba kombinasi 1-2-3-4, seperti ketika salah satu dari ke tiga terkaan yang diijinkan sebelum *device* dengan sepenuhnya dikunci bawah.

6.2.2 Metode Software-based

Metoda *Software-based* melibatkan teknik perangkat lunak untuk dipecahkan atau mem-bypass mekanisme pengesahan. Sedang beberapa *general-purpose* teknik perangkat lunak dan *tools* dapat meminta suatu kelas PDA devices, kebanyakan dari teknik khusus untuk suatu model yang spesifik didalam suatu kelas. Apabila suatu teknik khusus dikembangkan, hal itu secara normal diprogramkan dan diuji pada suatu devices test serupa. Metoda *Software-based* meliputi yang berikut:

- a. *Exploit known weaknesses in authentication* (Mengeksploitasi kelemahan yang diketahui dalam pengesahan) - Jika suatu mekanisme pengesahan lemah, memanfaatkan kelemahan untuk mengalahkan mungkin saja bisa. Sebagai contoh, awal perlindungan *password* pada PDA Palm OS di-*obfuscate password* yang menggunakan suatu algoritma yang dapat dibalik, membiarkan di-*recover* dengan mudah dari *device* yang menjalankan versi 4.0 atau lebih awal, menggunakan suatu kegunaan. Dengan cara yang sama, awal versi protokol Pocket PC Sync Aktif mengijinkan pengesahan tak terbatas untuk dicoba tanpa hukuman, membiarkan suatu serangan kamus dari *password* yang biasanya digunakan untuk dicoba. Sebagai tambahan, beberapa sistem mungkin punya suatu *password* cadangan atau menguasai *password* yang dibangun kedalam mekanisme pengesahan, yang mana mengijinkan akses tak terkekang apabila dimasukkan.
- b. *Gain access through a backdoor* (Keuntungan mengakses melalui suatu backdoor) - Pabrik sering membangun didalam fasilitas test atau *backdoors* lain bahwa suatu

pemeriksa dapat memanfaatkannya untuk memperoleh informasi. Sebagai contoh, *bootloaders* pada beberapa PDA *device* pendukung berfungsi diantaranya memungkinkan memori *device* untuk dibaca dan dicopy atau dipancarkan. Sebagai contoh, iPAQ 3900 dan model lain didalam rangkaian produk itu mendukung *bootloader*, suatu kegunaan tidak diiklankan yang dinamai oleh karena burung yang nampak pada tampilan itu. Apabila dicetuskan oleh suatu kombinasi spesifik *key chord* dan menyajikan perintah sesuai serial melalui *port*, *bootloader* mengembalikan muatan memori atau salinan kepada suatu kartu memori. Dengan cara yang sama, penguin *bootloader* untuk Linux *handheld devices* memungkinkan memori untuk dicopy untuk suatu kartu memori.

- c. *Exploit known system vulnerabilities* (Sistem Eksploitasi dikenal penyerang) - Sistem mobile dapat memiliki sifat mudah diserang didalam suatu standar interface protokol yang dapat pemeriksa memanfaatkan untuk mem-*bypass* pengesahan dan keuntungan mengakses informasi. Sebagai contoh, mengakses devices adalah mungkin melalui suatu *network service misconfigured*, suatu kekurangan didalam suatu protokol *networking* standar yang didukung oleh *device*, atau suatu kesalahan didalam implementasi protokol yang membuatnya peka kepada suatu metoda serangan seperti *buffer overflow*. Komunikasi mungkin menghubungkan untuk penghisapan meliputi yang serial, USB, *Irda*, *Bluetooth*, *Wifi*, dan fasilitas GSM/GPRS.

6.2.3 Metode Hardware-based

Metoda *Hardware-based* melibatkan suatu kombinasi perangkat lunak dan perangkat keras yang mematahkan atau mem-*bypass* mekanisme pengesahan. Sedikit alasan umum, metoda *hardware-based* berlaku bagi suatu kelas PDA *device* umum. Kebanyakan menyangkut teknik khusus untuk suatu model yang spesifik dalam suatu kelas. Seperti dengan metoda *software-based*, apabila suatu teknik khusus dikembangkan, secara normal dikembangkan penggunaan suatu alat test yang serupa kepada satu orang di bawah pengujian. *Device* Pabrik boleh juga menyediakan informasi bermanfaat dan *tools* untuk penyulingan data. metoda *Hardware-based* yang didasarkan meliputi yang berikut:

- a. *Gain access through a hardware backdoor* (Keuntungan mengakses melalui suatu perangkat keras backdoor) - Perangkat keras *backdoors*, seperti *device* penghubung

untuk *debugging*, pengujian produksi, atau pemeliharaan, mungkin digunakan untuk memperoleh akses ke memori. Sebagai contoh, beberapa *device* mempunyai perangkat keras test aktif menunjuk pada sirkuit menumpang bahwa dapat digunakan untuk memeriksa *device* itu. Banyak pabrik sekarang yang mendukung JTAG (Joint Test Action Group) standar, yang mana menggambarkan suatu test umum untuk prosesor, memori, dan chip semikonduktor lain, pada *device* mereka. Pemeriksa forensik dapat berkomunikasi dengan suatu komponen JTAG-Compliant dengan pemanfaatan perangkat lunak dan suatu pengontrol perangkat keras siap pasang dalam suatu kartu slot komputer pribadi atau suatu tujuan khusus *device* programmer yang berdiri sendiri untuk memeriksa poin-poin test yang digambarkan. JTAG yang menguji unit dapat mengirimkan data dan perintah kepada komponen JTAG-Compliant dan mengembalikan hasil kepada unit untuk terjemahan dan penyimpanan. JTAG memberi spesialis jalan lebar yang lain untuk imaging *device* yang dikunci atau *device* yang mungkin punya pelajaran pelengkap kerusakan dan tidak bisa dihubungkan cara lainnya dengan baik.

- b. *Examine memory independently of the device* (Menguji memori bebas dari *device*) - Suatu pemeriksa berpengalaman mungkin mampu menguji memori chips secara langsung pada *device* dan informasi penting dari mereka. Sebagai contoh, Institut Forensik Netherlands telah mengembangkan suatu maksud umum *device* untuk pengujian suatu cakupan luas chip memori. Sekali ketika secara fisik menghubungkan melalui suatu klip memori, alat tidak hanya dapat untuk dibaca dan menyimpan muatan memori, tetapi juga ke *overwrite* merekanya.
- c. *Reverse engineer the device to find and exploit a vulnerability* (Merekayasa balik *device* untuk menemukan dan memanfaatkan suatu sifat mudah diserang) - kebalikan Rancang-Bangun mendapat kembali kode sistem operasi dari ROM dari suatu PDA yang serupa kepada seseorang di bawah pengujian dan meneliti kode untuk memahami penggunaannya menyangkut *device* perangkat keras. Dengan pemahaman yang diperoleh, sifat mudah terserang manapun masuk akal dicatat dapat secara sistematis diuji untuk menentukan suatu teknik eksploitasi yang bermanfaat. Sebagai contoh, karena suatu mekanisme pengesahan *password*, mungkin saja menggunakan memori suntikan untuk *overwrite password* dengan nilai yang dikenal atau menggantikan program pengesahan dengan suatu versi yang selalu membuktikan keaslian dengan

sukses. Dengan cara yang sama, melemparkan dua bit kedalam suatu struktur data, yang mana menentukan apakah memulai *password* diatur dan aktif, boleh memadamkan mekanisme yang dengan sepenuhnya, seperti dilaporkan untuk XDA PDA/PHONE *hybrid device*-nya.

- d. Menyimpulkan informasi dengan monitoring karakteristik alat fisik teknik yang memonitor penggunaan power atau karakteristik device lain menjadi efektif secara sistematis menentukan *password* atau pin. Sebagai contoh, spesialis forensik melaporkan bahwa *password* beberapa organisator elektronik telah terbongkar dengan menentukan area alamat dari *password* dan ketika karakter dimasukkan, secara sistematis data monitoring dan menunjukkan ke bus. Semua penempatan memori mengungkapkan nilai satu karakter serentak. Diferensial penggerakkan analisa, yang mana telah ditunjukkan untuk bisa efektif didalam perolehan informasi dari *smart cards*, adalah teknik lain yang bisa diterapkan.
- e. Penggunaan mengotomatiskan kekuatan fisik Jika suatu mekanisme *password* tidak punya pembatasan pada banyaknya usaha manual yang dibuat dan pemeriksa mempunyai waktu terluang, suatu kekuatan fisik kamus serangan dapat dicoba. Secara normal, pendekatan ini akan menjadi hal yang tidak mungkin. Bagaimanapun, dengan tombol masukan diotomatiskan, akan menjadi masuk akal. Sebagai contoh, Institut Forensik Netherlands mengembangkan, suatu password masukan untuk sistem yang diotomatiskan untuk device dengan suatu *keyboard* dan layar. dilengkapi dengan Suatu tangan robot dan video kamera unit yang secara sistematis memasukkan kata sandi sampai masukan dideteksi atau, didalam kasus yang terburuk, kunci menjadi rusak.

6.3. Tangential Equipment

Peralatan menurut garis singgung meliputi *device* yang berisi memori dan dihubungkan dengan suatu PDA. Dua kategori utama adalah host komputer dan kartu memori untuk suatu PDA yang mana telah disamakan muatannya. Yang anehnya, USB *memory drives*, yang mana biasa untuk host komputer, biasanya tak satu faktor pun untuk PDA oleh karena isu device penghubung.

PDA, khususnya model yang terakhir, secara khas mendukung *Compact Flash* (CF), *Secure Digital* (SD), *Multi-Media Cards* (MMC), dan jenis media lain yang dapat dipindahkan dirancang terutama untuk *handheld devices*, yang mana dapat berisi sejumlah data penting.

Seperti RAM dan ROM, kartu memori adalah memori semikonduktor. Mereka secara normal digunakan sebagai alat bantu pemakai file penyimpanan, *backup* dari isi PDA penting, atau bermakna untuk menyampaikan file ke dan dari *device* itu. Ukuran fisik kartu memori yang didukung oleh *handheld devices* adalah penting sepanjang mereka adalah yang sungguh kecil, seukuran koin, dan mudah untuk dilewatkan. Oleh karena itu, penyelidik memerlukan banyak waktu dan secara menyeluruh mencari pendapat, apabila perampasan material. Data dapat diperoleh dari media dapat dipindahkan dengan penggunaan dari suatu pembaca media dan suatu aplikasi forensik untuk menggambarkan hard driver.

Data diisi pada suatu PDA sering disajikan pada suatu komputer pribadi, dalam kaitan dengan kemampuan dari suatu PDA untuk mensinkronkan atau jika tidak berbagi informasi antar satu atau lebih *host* komputer. Komputer pribadi atau stasiun-kerja seperti itu dikenal sebagai *synced devices*. Oleh karena sinkronisasi, sejumlah bukti yang penting pada suatu PDA, jika tidak semua, dapat juga hadir pada laptop orang yang dicurigai atau komputer pribadi, dan pengembalian kondisi ke suatu komputer *forensik tools* konvensional untuk pengujian dan *acquisition* hard drive.

USB drives, kadang-kadang dikenal sebagai *thumb drives*, adalah ukuran komponen perangkat keras *chewing-gum-pack* dengan konektor USB pada akhirnya, dan membangun sebagai sirkuit yang dicetak didalam suatu plastik yang memondokkan yang membungkus suatu memori dan prosesor. USB memori drive dapat diperlakukan dengan cara yang sama bagi suatu disk drive yang dapat dipindahkan, dan difoto dan dianalisa menggunakan forensic tools konvensional.

6.3.1 Synced Devices

Sinkronisasi mengacu pada proses perbedaan pemecahan didalam kelas informasi tertentu, seperti e-mail, bertempat tinggal pada dua *device* (yaitu, suatu PDA dan PC), seperti yang kedua-duanya kebanyakan mempertahankan versi sekarang, yang mana mencerminkan tindakan manapun yang diambil oleh pemakai (seperti, penghapusan) pada satu *device* atau *device* lainnya. Tergantung pada bagaimana *device* yang dicurigai diatur, sejumlah data informatif penting dapat berada ditempat komputer pribadi itu. Apabila suatu koneksi dibentuk antara *device* dan PC, pemakai boleh berkomunikasi sampai jenis account berikut:

1. Account Tamu - Tidak ada data secara otomatis disamakan antara alat dan PC, kecuali jika diaktifkan oleh pemakai.

2. Account Pemakai- Ketika koneksi, data disamakan secara otomatis antara PC dan *device*. Pemakai *predefines* apa yang data synched dan *device* yang mana yang mengambil hak yang lebih tinggi. Kebanyakan *handheld device* diatur untuk mensinkronkan data baru, seperti pesan, masukkan buku alamat, dan agenda informasi.

Sinkronisasi informasi dapat terjadi baik pada level record maupun level file. Apabila dilaksanakan ditingkatan file manapun bertentangan dari waktu dan tanggal sinkronisasi terakhir yang mengakibatkan versi yang terakhir secara otomatis menggantikan versi yang lebih lama tersebut. Intervensi manual adakalanya diperlukan jika kedua versi dimodifikasi dengan bebas karena sinkronisasi yang terakhir terjadi. Record tingkatan Sinkronisasi dilaksanakan dengan cara yang sama, tetapi dengan lebih *granularas* dengan yang hanya bagian dari suatu file yang dipecahkan dan digantikan.

Dengan Palm OS *device*, tingkatan sinkronisasi record adalah norma itu. Inti database PIM yang dapat disamakan meliputi yang berikut: *Address Book*, *Date Book*, *Memo Pad*, *Note Pad*, dan *To Do List*. Dengan Pocket PC *device*, tingkatan sinkronisasi file adalah norma itu. Inti aplikasi file PIM bahwa dapat disamakan meliputi yang berikut: *Calendar*, *Contacts*, *Inbox*, *Pocket Access*, *Tasks*, and *Favorites*. Perangkat lunak sinkronisasi selain yang dibangun kedalam sistem operasi juga ada dan dapat menyediakan suatu yang lebih luas atau kemampuan yang berbeda . Sebab muatan yang disamakan dari suatu PDA dan komputer pribadi cenderung berbeda dengan cepat dari waktu ke waktu, informasi tambahan mungkin ditemukan didalam satu *device* atau *device* lainnya.

Digital *device* didiami dengan data dari PC sepanjang proses sinkronisasi. Data dari PDA dapat juga disamakan kepada PC, melalui pilihan *user-defined* dalam perangkat lunak sinkronisasi. Perangkat lunak sinkronisasi dan jenis *device* menentukan dimana file PDA mungkin disimpan pada PC itu. Masing-Masing protokol sinkronisasi mempunyai suatu direktori instalasi, tetapi tempat terjadi peristiwa pemakai dapat ditetapkan. Hotsync manajer Palm menyimpan perpindahan data yang berisi: tanggal, lokasi dari data, dan informasi apa yang di-*synched*.

6.3.2 Memory Cards

Suatu array kartu memori yang luas ada pada pasar hari ini, berkisar antara ukuran dari suatu perangkat ke ukuran suatu *matchbook*. Kapasitas media penyimpanan dapat dipindahkan

dari 8MB sampai 2GB. Ketika kemajuan teknologi dibuat, media seperti itu menjadi lebih kecil dan menawarkan kepadatan penyimpanan lebih besar. Media dapat dipindahkan meluas kapasitas penyimpanan PDA, membiarkan individu untuk menyimpan file tambahan di luar *built-in* kapasitas *device*. Kartu memori menyediakan jalan lebar yang lain untuk berbagi data antar berbagai pemakai yang mempunyai perangkat keras yang dapat dipertukarkan.

Tidak sama dengan RAM, di dalam suatu *device*, media yang dapat dipindahkan adalah penyimpanan *non-volatile* dan tidak memerlukan baterai untuk mempertahankan data. Kebetulan, media seperti itu dapat diperlakukan dengan cara yang sama kepada suatu *disk drive* yang dapat dipindahkan, dan digambar dan dianalisa menggunakan *forensic tools* konvensional dengan penggunaan dari suatu pembaca media eksternal. Orang yang mengadaptasikan pendukung kartu memori pendukung itu adalah suatu penghubung Integrated Development Environment (IDE). Orang yang mengadaptasikan seperti itu memungkinkan media dipindahkan untuk diperlakukan sebagai suatu *hard-disk* dan digunakan perangkat lunak putih yang dihalangi, yang mana memastikan bahwa media yang dapat dipindahkan tidak diubah. Data berisi media dapat dicari dan digambar, dan file yang dihapus dikembalikan keadaannya. Di bawah ini adalah suatu ikhtisar yang meringkas beberapa media penyimpanan umum yang digunakan sekarang yang dapat berisi informasi penting yang berhubungan dengan suatu penyelidikan.

1. *Compact Flash Cards (CF)* - Compact Flash Cards adalah suatu kartu *solid-state* disk dengan suatu 50-pin konektor, terdiri dari dua baris yang paralel 25 pin pada satu tepi menyangkut kartu itu. Compact Flash Cards dirancang untuk kemampuan dan kecocokan PCMCIA-ATA, mempunyai 16-bit data bus, dan lebih digunakan sebagai *hard drive* dibanding sebagai RAM. Mereka menggunakan teknologi *flash memory*, suatu solusi penyimpanan *non-volatile* yang mempertahankan informasinya sekali ketika power dipindahkan dari kartu itu. Compact Flash Cards adalah tentang ukuran dari suatu matchbook (length-36.4 mm, width-42.8 mm, thickness-3.3 mm untuk tipe I dan 5mm untuk tipe II) dan mengkonsumsi sejumlah minimal power.
2. *Microdrives* - Hitachi Microdrive media digital adalah suatu *high-capacity*, memutar massa penyimpanan *device* yang terdapat suatu *Compact Flash* tipe II dibungkus dengan suatu 16-bit data bus. Suatu disk kecil bertindak sebagai media penyimpanan, yang mana lebih mudah pecah dibanding *solid-state* memori dan memerlukan energi untuk memutar.

Serupa dengan fungsinya kepada *solid-state* menyiarkan kartu memori, 4Gb Microdrive penyimpanan kartu yang di-preformatted dengan suatu file sistem FAT32. FAT32 diperlukan untuk memungkinkan penyimpanan diatas 2GB. Dengan bergerakkan ke FAT32, lebih banyak ruang penyimpanan yang dapat diakses, tetapi kamera dan devices lain harus mendukung sistem file yang lebih baru. Banyak kamera digital dan PDA paling mendukung FAT32.

3. *Multi-Media Cards (MMC)*- Suatu Multi-Media Cards (MMC) adalah suatu kartu *solid-state* disk dengan suatu 7-pin connector. Kartu MMC mempunyai suatu 1-bit data bus. Seperti dengan kartu CF, mereka dirancang dengan teknologi *flash*, suatu solusi penyimpanan *non-volatile* yang mempertahankan informasi sekali ketika power dipindahkan dari kartu itu. Kartu tidak berisi komponen yang bergerak dan menyediakan perlindungan data yang lebih besar dibanding *disk drive* magnetis konvensional. Multi-Media Cards berukuran dari suatu perangkat (length-32 mm, width-24 mm, dan thickness-1.4 mm). Ukuran Multi-Media Cards Yang dikurangi (RS-MMC) juga ada. Mereka kira-kira setengah ukuran dari kartu MMC standard (length-18mm, jarak- 24mm, dan thickness-1.4mm). Meskipun demikian mereka dirancang terutama untuk mobile phone, mereka dapat berpotensi digunakan di PDA. Suatu RS-MMC dapat digunakan didalam suatu slot MMC ukuran penuh dengan suatu orang yang mengadaptasikan mekanik. Suatu kartu MMC reguler dapat juga digunakan didalam kartu slot RS-MMC, meskipun demikian bagian itu akan dikeluarkan dari slot itu. MMCPLUS dan MMCMOBILE adalah yang jenis capaian yang lebih tinggi dari kartu MMC dan RS-MMC yang berturut-turut mempunyai 13-pin connector dan suatu 8-bit data bus.
4. *Secure Digital Card (SD)* - memori Secure Digital Card (SD) (length-32 mm, width-24 mm, dan thickness-2.1mm) dapat diperbandingkan dengan ukuran dan perancangan *solid-state* MMC kartu. Sesungguhnya, slot kartu SD sering mengakomodasi kartu MMC juga. Bagaimanapun, kartu SD mempunyai 9-pin connector dan suatu 4-bit data bus, yang mana mampu transmisi yang lebih cepat. SD memori kartu menonjolkan suatu tombol *erasure-prevention*. Menjaga tombol didalam posisi yang dikunci untuk melindungi data dari penghapusan yang kebetulan. Mereka juga menawarkan mengendalikan keamanan untuk perlindungan isi (yaitu, Content Protection Rights Management). kartu SD Mini adalah suatu perluasan yang dapat dipertukarkan (menyangkut) kartu SD standard yang ada di dalam suatu format yang lebih ringkas

(length-21.5 mm, width-20 mm, dan thickness-1.4 mm). Mereka berjalan pada bus perangkat keras yang sama dan menggunakan alat penghubung yang sama sebagai suatu kartu SD, dan juga termasuk melindungi keamanan isiyang menjadi cirinya, tetapi mempunyai suatu potensi kapasitas maksimum lebih kecil kaitan dengan pembatasan ukuran. Karena kecocokan mundur, orang yang mengadaptasikan memungkinkan suatu Kartu SD Mini bekerja sama dengan kartu SD slot yang ada.

5. *Tongkat Memori* - Tongkat memori menyediakan memori *solid-state* didalam ukuran yang serupa, tetapi lebih kecil dibanding, sebuah *stick of gum* (length-50mm, width-21.45mm, thickness-2.8mm). Mereka mempunyai 10-pin konektor dan 1-bit data bus. Seperti dengan kartu SD, Tongkat Memori juga mempunyai tombol *built-in erasure-prevention*, untuk melindungi muatan dari kartu. Kartu stik PRO menawarkan kapasitas yang lebih tinggi dan memindahkan jumlah transfer dengan memori stik standar, menggunakan 10-pin connector, tetapi dengan 4-bit data bus. *Memory Stick Duo* dan *Memory Stick PRO Duo*, versi yang lebih kecil dari *Memory Stick* dan *Memory Stick PRO*, adalah sekitar dua pertiga ukuran dari tongkat memori standard (length-31mm, width-20mm, thickness-1.6mm). Seorang yang beradaptasi diperlukan untuk *Memory Stick Duo* atau *Memory Stick PRO Duo* yang akan bekerja bersama Slot Memori Stick standard.
6. *Extended Memory Cards* (Kartu Memori Yang diperluas) - Kartu memori boleh mendukung perluasan untuk kemampuan tambahan. Sebagai contoh, Kartu X-Mobile dari Renesas adalah suatu kartu Multimedia yang keduanya berisi smart card dan suatu chip memori dan mampu berfungsi didalam mode yang manapun .

6.3.3 USB Memory Drives

Banyak pabrik yang memproduksi memori USB drive dalam beberapa kapasitas. Sekarang ini, sedikit sekali PDA *device* yang mendukung host USB port, yang diperlukan untuk dihubungkan dengan sekelilingnya. Lebih dari itu, sedikit bila ada pabrik USB drive menyediakan *drive* yang perlu untuk sistem operasi PDA. Situasi ini dapat dimengerti bahwa spesifikasi host USB berniat alat penghubung untuk untuk mampu mendukung berbagai *device* berbagi host, yang mana jika diijinkan akan menempatkan power yang penting yang mengalirkan baterai dari *device* tersebut. Faktor lain meliputi pembatasan didalam mobilitas yang dikenakan oleh suatu USB drive yang menyangkut sisi dari PDA dibandingkan kepada

keuntungan menyediakan satu atau lebih slot kartu memori yang dengan sepenuhnya berisi kartu apabila dimasukkan.

Seperti dengan perluasan kartu memori, USB *drive* dapat menawarkan kemampuan tambahan seperti suatu alat penghubung *wireless*. Mengakses kemuatan memori dapat juga dilindungi melalui suatu sidik jari pembaca yang *built-in* atau beberapa mekanisme lain seperti suatu *smart card*, yang mempersulit proses *acquisition*. Bagaimanapun, untuk pertimbangan tersebut di atas yang sekeliling ini adalah tidak secara normal dihubungkan dengan PDA *device*.

7. Pengujian dan Analisis

Proses pengujian memberi cahaya ke data probative. Hasilnya, diperoleh melalui penerapan metoda didasarkan secara ilmiah dibentuk, perlu menguraikan isi dan status dari data dengan sepenuhnya. Dokumentasi seperti itu memungkinkan semua pesta untuk menemukan apa yang dimasukkan, mencakup informasi yang mungkin tersembunyi atau digelapkan. Ketika semua informasi diarahkan, pengurangan data dapat dimulai, dengan demikian memisahkan dari informasi yang relevan ke informasi yang tidak relevan. Proses Analisa berbeda dengan pengujian didalam itu meneliti produk dari pengujian untuk artinya dan probative menghargai kepada kasus itu. Pengujian adalah pengolahan secara teknis adalah proses dari spesialis forensik. Bagaimanapun, analisa mungkin dilaksanakan oleh peranan lain dibanding analis yang forensik, seperti penyelidik atau pemeriksa yang forensik itu. Seseorang boleh melaksanakan semua peran yang dilibatkan.

Proses pengujian mulai setelah suatu forensik *workstation* telah disediakan dengan *tools* sesuai dan suatu copy dari bukti yang diperoleh dari alat itu. Jika tersedia, pemeriksa perlu belajar kasus dan menjadi terbiasa dengan parameter dari serangan, pesta yang terlibat, dan bukti potensial yang ditemukan. Melakukan pengujian didalam suatu persekutuan dengan analis forensik atau penyelidik memandu konstruksi kasus sebaiknya untuk pemeriksa itu. analis atau Penyelidik menyediakan pengertian yang mendalam ke dalam tipe hal yang dicari, sedang pemeriksa forensik menyediakan rata-rata untuk temukan informasi yang relevan yang dapat terjadi pada sistem itu.

Jika pemeriksa forensik melaksanakan analisa dengan bebas, tanpa berunding dengan penyelidik atau analis forensik, pengetahuan yang diperoleh dengan mempelajari kasus perlu menyediakan gagasan tentang *password* yang spesifik atau ungkapan untuk menggunakan manakala mencari gambaran yang diperoleh dari devcies itu. Kebetulan, bandingkan dengan pengujian *server network* atau *workstation* individu, jumlah data yang diperoleh, dalam kaitan dengan ukuran gambaran mentah, apakah lebih banyak kecil yaitu, Mbytes melawan Gbytes.

Tergantung pada jenis kasus, strateginya akan bervariasi. Suatu kasus tentang pornografi anak boleh mulai dengan *browsing* semua gambaran yang grafis pada sistem,

sedang suatu kasus tentang suatu serangan *Internet-Related* mungkin mulai dengan *browsing* Internet sejarah file. Pengujian sering mengungkapkan tidak hanya data berpotensi yang bersifat menuduh tetapi juga informasi bermanfaat seperti password, jaringan logon nama, dan aktivitas Internet. Sebagai tambahan terhadap bukti yang secara langsung berhubungan dengan suatu peristiwa, informasi dapat terbongkar tentang *lifestyle* dari orang yang dicurigai, rekaman mereka, dan jenis aktivitas di mana mereka dilibatkan.

7.1 Lokasi Bukti

Standard PDA secara khas menawarkan informasi serupa yang menangani kemampuan dan ciri, termasuk aplikasi Manajemen informasi Pribadi (PIM), dukungan untuk e-mail, dan *Web browsing*. *Hybrid device* yang menyertakan PDA keduanya dan kemampuan cell phone juga ada. Bukti potensial pada alat ini meliputi :

1. Buku Alamat
2. Kalender Janji/informasi
3. Dokumen
4. E-mail
5. Tulisan tangan
6. Password
7. Phone book
8. Pesan
9. Pesan suara

Biasanya, dua jenis penyelidikan komputer forensik berlangsung. Yang pertama adalah dimana beberapa peristiwa telah terjadi, tapi identitas pelanggar tak dikenal (seperti, *malicious code attack*, *hacking incident*, dan lain-lain). Yang kedua adalah dimana pelanggar dan peristiwa adalah kedua-duanya dikenal (seperti, penyelidikan kasus porno anak-anak). Dipersenjatai dengan pengetahuan dari keadaan menyangkut peristiwa, analis dan pemeriksa yang forensik dapat berproses ke arah yang memenuhi sasaran hasil berikut :

1. lipatan Informasi tentang individu yang dilibatkan { siapa }.
2. Menentukan kealamian dari suatu peristiwa yang terjadi { apa }.
3. Membangun suatu timeline peristiwa { kapan }.
4. Menemukan tool apa atau exploits yang digunakan { bagaimana }.

5. Membongkar informasi yang menjelaskan motivasi untuk keadaan serangan { mengapa }.

Tabel 7.1 di bawah menyediakan suatu referensi silang dari sumber bukti umum yang ditemukan pada PDA dan kontribusi mereka kearah pemuasan dari penilaian objektif diatas. Kebanyakan dari sumber informasi datang dari data PIM, dan Internet dihubungkan informasi. Aplikasi pendukung lain yang berjalan pada devices yang berpotensi menyediakan sumber bukti lain. File pemakai ditempatkan pada alat untuk terjemahan, mengamati, atau editing adalah juga sumber bukti penting yang lain. Di samping file grafis, isi file relevan lain meliputi *spreadsheet*, *presentation slides*, dan materi serupa. Karena hybrid devices, seperti telepon PDA atau GPS PDA, sumber bukti tambahan ada, sebagai contoh, nomor jumlah diputar terakhir atau mengkoordinir kepada beberapa tujuan.

	Who	What	Where	When	Why	How
Owner Info	X					
Contacts	X				X	X
Calendar	X	X	X	X	X	X
To Do List	X	X	X	X		X
E-mail Contact	X	X	X	X	X	X
Web URLs/Content		X	X	X		X
Graphic Files	X	X				
Other File Content		X	X	X	X	X

Tabel 7.1 Cross Reference of Sources and Objectiv

Pengetahuan dan pengalaman dengan berbagai *tools* untuk memperoleh dan menguji muatan PDA sangat berharga. Sebagai contoh, satu *device* dapat melaksanakan lebih baik daripada area inspecific yang lain seperti identifikasi file atau fasilitas pencarian, *tools* dapat melaporkan, memperoleh, dan menguji muatan dari data yang diperoleh dengan cara yang berbeda dan beberapa tools mungkin adalah platform spesifik. Oleh karena itu, menggunakan toolkit yang menawarkan yang ciri yang terbaik untuk menyembuhkan dan meneliti bukti dari suatu devices spesifik yang menguntungkan.

7.2 Penerapan Tools

Ketika gambaran yang diperoleh telah dicopy, langkah yang berikutnya akan mulai mencari data, menciptakan *bookmarks*, dan mengembangkan muatan dari suatu laporan akhir.

Tool pengujian forensik adalah komponen rumit didalam proses ini ketika mereka menterjemahkan data dari gambaran bit mentah kepada suatu struktur dan format yang dapat dimengerti oleh pemeriksa dan dapat secara efektif digunakan untuk mengidentifikasi dan memulihkan bukti. Adalah penting untuk mencatat bahwa *tools* mempunyai kemungkinan untuk berisi beberapa derajat tingkat kesalahan. Sebagai contoh, implementasi dari *device* mungkin punya suatu kesalahan programming; spesifikasi dari suatu struktur file yang digunakan oleh *device* untuk menterjemahkan data dirusak sehingga dapat dimengerti oleh pemeriksa yang mungkin ketinggalan zaman atau tidak akurat, atau struktur file yang dihasilkan oleh program yang lain sebagai masukan mungkin adalah salah, menyebabkan *device* berfungsi dengan tidak sesuai. Oleh karena itu, mempunyai suatu derajat tinggi pemahaman dan kepercayaan menyangkut kemampuan *device* untuk melaksanakan fungsi pentingnya dengan baik. Sebagai tambahan, suatu orang yang dicurigai banyak mengetahui boleh merusakkan informasi *device*, seperti penuh arti salah memanggil nama suatu perluasan file untuk menggagalkan aktif dari suatu *device* atau menerapkan suatu *device* yang menyeka untuk memindahkan atau menghapuskan data. Dari waktu ke waktu, percobaan dengan suatu *device* menyediakan suatu pemahaman tentang pembatasannya, membiarkan pemeriksa untuk meratakan mereka dan menghindari kesalahan.

Pengujian Forensik dari Bukti Digital - Suatu Panduan untuk Pelaksanaan hukum, yang diproduksi oleh itu Departemen Keadilan U.S., menawarkan usul berikut untuk analisa ttg data yang disadap:

1. **analisa Timeframe** - Menentukan apabila peristiwa terjadi pada sistem yang berhubungan dengan pemakaian secara perorangan dengan meninjau ulang log manapun yang ada sekarang dan date/time mencap didalam filesystem, seperti waktu dimodifikasi terakhir.
2. **Data hiding analysis** (Data yang menyembunyikan analisa) - Mendeteksi dan pemulihan menyembunyikan data yang boleh menandai adanya pengetahuan, kepemilikan, atau tujuan dengan menghubungkan keterhubungan file untuk perluasan file untuk menunjukkan *obfuscation* disengaja; perolehan akses ke *password-protected*, *encrypted*, dan memampatkan file; perolehan akses ke informasi *steganographic* dideteksi didalam gambaran; dan memperoleh akses untuk memesan area penyimpanan data diluar *filesystem* normal itu .

3. **Application and file analysis** (Aplikasi dan analisa file) - Mengidentifikasi informasi relevan kepada penyelidikan dengan pengujian isi file, menghubungkan file untuk menginstall aplikasi, mengidentifikasi hubungan antar file (seperti, file e-mail ke pemasangan e-mail), menentukan arti dari file yang tak dikenal tipenya, menguji bentuk wujud sistem yang ditentukan, dan menguji file metadata (seperti, dokumen yang berisi identifikasi kebebasan).
4. **Ownership and possession** (pemilikan dan Kepemilikan) - Mengidentifikasi individu yang menciptakan, memodifikasi, atau mengakses suatu file, dan pemilikan dan kepemilikan dari data ditanyakan dengan penempatan pokok materi dengan devices pada situasi tertentu dan menanggalnya, menempatkan minat file bukan melalui penempatan, menyembuhkan kata sandi yang menandai adanya kepemilikan atau pemilikan, dan muatan file yang mengidentifikasi yang dikhususkan untuk seorang pemakai.

Kemampuan dari *tool*, kesempurnaan ciri, dan sistem operasi itu (seperti, Windows CE, Palm OS, Linux) dan jenis *device* di bawah pengujian menentukan informasi apa yang dapat temukan, disembuhkan, dan dilaporkan, dan jumlah usaha yang diperlukan. Area variabilitas meliputi kesembuhan dan pencarian ttg informasi yang dihapus, informasi pada *device* dipasang lagi, atau informasi didalam arsip file bersejarah dimampatkan atau file dengan perluasan salah dipanggil namanya. Sebagai contoh, beberapa *tools* yang digunakan untuk mencari-cari bukti boleh mengidentifikasi file dengan perluasan file di mana orang lain menggunakan suatu database tandatangan file. Ciri selanjutnya adalah lebih baik karena menghapuskan kemungkinan data penutup berdasar pada suatu perluasan file yang tidak tetap. Ini terutama benar untuk berbagai jenis file grafik, oleh karena seluruh yang mereka alami biasanya adalah *shrouded* dari pencarian textual.

Mesin pencarian bermain dalam suatu peran penting didalam penemuan informasi yang digunakan untuk menciptakan suatu *bookmarks* dan laporan akhir. Pencarian data untuk hal positif menghasilkan bukti bersifat menuduh mengambil kesabaran dan dapat menjadi waktu pemakaian. Beberapa *tools* mempunyai suatu mesin pencarian sederhana yang persisnya menandingi suatu teks masukan string, membiarkan hanya untuk dilakukan pencarian dasar. *Tools* rumah lain yang lebih cerdas dan memperlihatkan mesin pencarian yang kaya, mempertimbangkan jenis mencari *grep* (pola teladan ungkapan reguler yang disamaratakan), mencakup *wildcard*; penyaringan file dengan perluasan, direktori, dan lain -

lain dan catatan batch yang mencari-cari jenis isi spesifik (yaitu, e-mail alamat, URLS, dan lain - lain). Dengan cara yang sama, kemampuan untuk menemukan dan mengumpulkan gambaran yang secara otomatis ke dalam suatu fasilitas perpustakaan grafik umum dapat berbeda antar perkakas. Semakin besar kemampuan alat, semakin pengalaman dengan dan pengetahuan dari devices menjadi berharga untuk pemeriksa forensik itu.

Untuk membongkar bukti, spesialis pertama harus melawan latar belakang menyangkut orang yang dicurigai dan keadaan serangan dan menentukan satu set terminologi untuk pengujian itu. Ungkapan pencarian harus dikembangkan didalam suatu pertunjukan sistematis, seperti penggunaan nama kontak yang mungkin adalah relevan. Dengan membuat ini, spesialis menciptakan suatu profil untuk potensi penemuan yang berharga yang tidak akan menyelimuti penemuan. Untuk menghapuskan semua kemungkinan penghilangan bukti berharga, data harus secara menyeluruh diperiksa dari permulaan untuk berakhir dengan suatu jendela memori yang disajikan oleh tool yang baik maupun seorang hex editor. apalagi, spesialis perlu mempunyai suatu tandatangan file database untuk menempatkan header dan footers file spesifik yang boleh mendorong kearah bukti lebih lanjut seperti: file grafik, avi file, dan lain lain.

Sekali ketika data telah secara menyeluruh dicari dan materi relevan di *bookmark*, adalah waktunya untuk menciptakan suatu laporan. Banyak aplikasi forensik datang dengan suatu *built-in* yang melaporkan fasilitas yang mengimport data yang di*bookmark*, membiarkan spesialis untuk mengorganisir laporan, memilih modenya, dan aspek customize yang lain menyangkut laporan itu. Laporan dapat meliputi hal yang berikut: Nama Spesialis, Nomor Jumlah Kasus, Tanggal, Judul, Nama Orang yang dicurigai, Kategori bukti, dan relevansi bukti yang ditemukan. laporan *software-generated* hanya suatu bagian kecil dari keseluruhan laporan akhir. laporan Yang akhir berisi laporan yang *software-generated* sepanjang dokumentasi yang dikumpulkan sepanjang keseluruhan siklus, yang mana meringkas tindakan dari pengujian forensik dan banyak hadiah dari hasil analisa, mencakup membongkar bukti manapun.

Ukuran-Ukuran berikut telah diusulkan sebagai pokok satuan kebutuhan untuk forensik tool, dan harus dipertimbangkan manakala suatu pilihan perkakas tersedia:

1. **Usability** (Usabilas) - kemampuan untuk menyajikan data didalam suatu format yang adalah berguna bagi suatu penyelidik.

2. **Comprehensive** (Menyeluruh) - kemampuan untuk menyajikan semua data kepada suatu penyelidik sedemikian sehingga bukti kedua - duanya *inculpatory* dan *exculpatory* dapat dikenali.
3. **Deterministic** - kemampuan tool untuk menghasilkan keluaran yang sama manakala diberi satuan instruksi dan data masukan yang sama.
4. **Verifiable** - kemampuan untuk memastikan ketelitian menyangkut keluaran dengan mempunyai akses ke hasil presentasi dan terjemahan intermediate.

Faktor lain didalam memilih perangkat lunak antar tool meliputi pertimbangan Daubert yang disebutkan lebih awal didalam bagian 4.2 (terutama sekali Penerimaan) dan materi berikut :

1. **Quality** (Mutu) - pendukung teknis, keandalan, dan meningkatkan mutu alur versi.
2. **Capability** (Kemampuan) – didukung ciri set, performance, dan kesempurnaan mengenai cirri fleksibilitas dan customisasi.
3. **Affordability** (Affordabilas) - manfaat berharga melawan produktivitas didalam.

8. Pelaporan

Pelaporan adalah proses dalam menyiapkan suatu ringkasan terperinci dari semua langkah-langkah yang diambil dan kesimpulan dicapai didalam penyelidikan dari suatu kasus. Pelaporan tergantung pada semua peserta yang secara hati-hati memelihara suatu record / catatan dari pengamatan dan tindakan mereka, melaporkan hasil test, dan menjelaskan kesimpulan menarik dari bukti itu. Basis dari suatu laporan yang baik adalah dokumentasi padat, catatan, sket, foto, dan laporan *tool-generated*.

Pelaporan hasil dari suatu pengujian forensik cenderung untuk mengikuti templates yang sudah dikenal, *customized* diperlukan oleh keadaan yang spesifik dari tiap penyelidikan. Laporan dari hasil pengujian forensik meliputi semua informasi diperlukan untuk mengidentifikasi kasus dan sumbernya, menguraikan secara singkat hasil percobaan dan penemuan, dan membawa tandatangan dari individu yang bertanggung jawab untuk muatannya. Secara umum, laporan dapat meliputi informasi yang berikut:

1. Identitas menyangkut pelaporan agen
2. identifier Kasus atau nomor submission
3. Penyelidik kasus
4. Identitas menyangkut submitter
5. Tanggal tanda terima
6. Tanggal laporan
7. Daftar deskriptif materi yang disampaikan untuk pengujian, mencakup nomor urut, buatan, dan model
8. Tandatangan dan Identitas menyangkut pemeriksa
9. Peralatan dan yang disediakan digunakan didalam pengujian
10. Meringkas uraian langkah-langkah diambil selama pengujian, seperti pencarian string, pencarian gambaran grafik, dan file penyembuhan dihapus.
11. Pendukung material seperti hasil print computer ttg materi bukti tertentu, salinan bukti digital, dan rantai penjagaan dokumentasi
12. Rincian penemuan:
 - a. File spesifik yang berhubungan dengan permintaan

- b. File lain, termasuk menghapus file, yang mendukung penemuan
- c. Pencarian string, kata kunci pencarian, dan teks mencari string
- d. Bukti *Internet-related*, seperti lalu lintas Analisa lokasi jaringan, chat logs, cache files, e-mail, dan news group activity
- e. Analisa gambaran grafis
- f. Indikator kepemilikan, yang mana bisa meliputi data pendaftaran program
- g. Data analysis
- h. Uraian relevan program pada materi yang diuji
- i. Teknik digunakan untuk besembunyi atau menyembunyikan data, seperti encryption, steganography, atribut yang tersembunyi, sekat yang tersembunyi, dan file menyebut keganjilan

13. Laporan Kesimpulan

Banyak perangkat lunak aplikasi forensik mempunyai fasilitas laporan built-in. Pemeriksa hanya perlu meliputi penemuan yang relevan didalam laporan untuk memperkecil kebingungan dan ukuran dari diantara mereka yang meninjau ulang itu. Laporan yang diotomatkan secara khas berisi komponen kunci berikut : Nomor Jumlah Kasus, Tanggal/Date, *Examiner Name*, Nama Orang yang dicurigai, dan *Files Acquired* (mempertunjukkan hash, data ASCII, penyajian data grafis, dan lain - lain.).

Bukti digital, seperti halnya *tools*, metodologi dan teknik yang digunakan didalam suatu pengujian, sebuah subjek yang sedang ditantang didalam suatu pengadilan atau procedure formal lain. kesesuaian Dokumentasi adalah penting didalam penyediaan kemampuan individu untuk menciptakan kembali proses dari permulaan untuk mengakhiri. Sebagai bagian dari proses pelaporan, membuat suatu salinan perangkat lunak yang digunakan dan mencakupnya dengan keluaran diproduksi yang sebaiknya. Hal Ini bersangkutan untuk kebiasaan tools, karena kebingungan tentang versi dari perangkat lunak yang digunakan untuk menciptakan keluaran dihapuskan, seharusnya hal itu dijadikan diperlukan untuk reproduksi pengolahan forensik yang menghasilkan pada suatu waktu kemudiannya. Praktek yang sama berlaku bagi perangkat lunak *tools* komersil, yang mana bisa diupgrade setelah suatu pengujian diselesaikan.

9. Contoh Penerapan

9.1 Bukti Elektroik

Bukti elektronik adalah informasi dan data dari sebuah nilai investigasi yang disimpan atau yang terpancar dari sebuah alat elektronik. Pada dasarnya, kita tidak bisa “melihat” isi dari sebuah objek fisik bukti yang dapat membuat bukti tersebut “kelihatan”

Bukti elektronik pada dasarnya sangatlah rapuh. Bukti tersebut dapat dirubah, dirusakkan, atau dihancurkan jika tidak ditangani dan diuji dengan benar. Karena alasan inilah diperlukan sebuah tindakan pencegahan khusus harus diambil untuk mengumpulkan, mendokumentasikan, memelihara, dan menguji bukti tersebut. Kegagalan dalam melihat dan melakukan suatu pemeriksaan akan membawa kita kearah yang salah dalam membuat sebuah kesimpulan nantinya.

Bukti elektronik biasanya :

- a. Sering tersembunyi (sama halnya seperti sidik jari atau bukti DNA).
- b. Dapat melewati perbatasan dengan mudah dan cepat.
- c. Mudah pecah dan dapat dengan mudah diubah, dirusak, atau dihancurkan.
- d. Kadang-kadang bersifat *time-sensitive*.

9.2 Proses Forensik

Sebuah bukti elektronik pada dasarnya mempunyai sifat dasar yang akan membuat seseorang dengan kemampuan khusus akan diakui selama proses investigasi. Oleh karena itu, dalam melewati proses tersebut haruslah mengikuti semua prosedur forensik yang sesuai. Adapun tahapan prosedur yang harus dilalui, antara lain : *collecting* (pengumpulan), *examination* (pengujian), *analysis* (analisa), dan *reporting* (pelaporan).

Pada tahap pengumpulan akan melibatkan pencarian dan dokumentasi dari bukti elektronik serta akan melibatkan *real-time* dan informasi yang tersimpan yang mungkin mudah hilang jika tidak diambil tindakan pencegahan pada saat terjadi peristiwa.

Proses pengujian akan membantu hingga membuat sebuah bukti dapat “kelihatan” dan dapat asal serta keaslian bukti tersebut. Proses ini harus memenuhi beberapa hal, antara lain :

proses ini harus mendokumentasikan isi serta keseluruhan status dari bukti tersebut. Pendokumentasian seperti ini akan memberikan petunjuk untuk menemukan isi dan informasi yang mungkin tersembunyi atau digelapkan. Ketika semua informasi yang dibutuhkan “kelihatan”, proses pengurangan data pun dapat dilakukan. Dengan jumlah data yang sebesar ini, informasi yang dapat disimpan pada suatu media penyimpanan computer menjadi bagian yang penting dalam suatu pengujian. Proses pengujian juga dapat dilakukan dengan meneliti produk yang akan diuji untuk mengetahui nilai keaslian kasus tersebut. Pengujian merupakan suatu tinjauan ulang teknik yang merupakan bagian dari forensik, sedangkan untuk proses analisa akan dilakukan oleh regu investigasi. Dalam beberapa organisasi, kedua peran ini dapat dikerjakan sekaligus oleh satu orang.

Dalam sebuah laporan menuliskan bahwa proses pengujian dan *recover* data dapat melengkapi suatu proses pengujian. Catatan pengujian harus dipelihara untuk sebuah kesaksian atau tujuan lainnya. Seorang pemeriksa dapat bersaksi tidak hanya menyangkut pengujian, tetapi juga kebenaran dari prosedur dan keahliannya untuk melakukan pengujian tersebut.

Adapun prinsip mengenai cara dan forensik umum yang harus diterapkan apabila berhadapan dengan bukti elektronik, antara lain:

1. Tindakan mengambil untuk mengamankan dan mengumpulkan bukti elektronik tidak akan merubah bukti tersebut.
2. Orang yang melaksanakan pengujian mengenai bukti elektronik harus orang yang terlatih untuk tujuan tersebut.
3. Aktivitas yang berkenaan dengan pengambilan, pengujian, penyimpanan, atau perpindahan bukti elektronik harus secara penuh didokumentasikan, dipelihara, dan tersedia untuk tinjauan ulang.

9.3 Penanganan bukti elektronik

Seperti yang dijelaskan diatas bahwa sebuah tindakan pencegahan harus diambil dalam setiap tahap pengumpulan, pemeliharaan, dan pengujian sebuah bukti elektronik.

Penanganan bukti elektronik pada suatu peristiwa kejahatan secara normal terdiri dari langkah-langkah berikut :

1. Pengenalan dan identifikasi bukti.
2. Dokumentasi menyangkut peristiwa kejahatan.

3. Pengumpulan dan pemeliharaan bukti.
4. Pengemasan dan transportasi bukti.

9.4 Prosedur dan Prinsip dalam penanganan bukti

Penyelidikan sebuah peristiwa kejahatan dapat ditangani dalam berbagai cara, tergantung dari keadaan dan persiapan serta pengalaman regu penyelidikan. Penyelidikan digital dapat dibandingkan dengan peristiwa kejahatan dengan melihat teknik investigasi yang digunakan yang telah diterapkan sebagai pondasi untuk menciptakan prosedur yang digunakan apabila berhadapan dengan sebuah bukti digital.

9.4.1 Aturan dan tanggung jawab

Dalam perencanaan sebuah peristiwa perlu menunjukkan bagaimana seorang personil memenuhi peran ini ketika menjawab dan melaksanakan suatu penyelidikan. Suatu peran yang umum dan berhubungan dengan tanggung jawab. Peran tersebut meliputi *First Responders* (responder pertama), *Investigators* (Penyelidik), *Technicians* (Teknisi), *Forensic Examiners* (Pemeriksa Forensik), dan *Forensic Analysts* (Analisis Forensik). Dalam situasi yang telah ditentukan dalam suatu peristiwa, seorang individu dapat melaksanakan lebih dari satu peran. Meskipun demikian, peran yang berbeda akan mempunyai tanggung jawab yang berbeda, namun tetap saling terhubung.

1. *First Responders* (Responder Pertama) Peran yang dilatih untuk tiba pertama ke tempat suatu peristiwa, membuat sebuah penilaian awal, dan memberikan tanggapan yang sesuai. Tanggung jawab dari responder pertama adalah mengamankan tempat insiden, meminta dukungan yang perlu, serta membantu dengan mengumpulkan bukti.
2. *Investigators* (Penyelidik) merencanakan dan mengatur *preservation* (pemeliharaan), *acquisition* (perolehan), *examination* (pengujian), *analysis* (analisa), dan *reporting* (pelaporan) dari bukti elektronik. Petunjuk penyelidik bertanggung jawab atas semua aktivitas di tempat peristiwa untuk tetap dalam keadaan dan waktu yang benar. Petunjuk Penyelidik mungkin bertanggung jawab dalam mengembangkan bukti, menyiapkan laporan kasus, dan pengarah singkat dan pertemuan dengan pejabat senior.
3. *Technicians* (Teknisi) melaksanakan semua tindakan dibawah arahan petunjuk penyelidik. Teknisi bertanggung jawab untuk mengidentifikasi dan mengumpulkan bukti serta dokumen dari tempat peristiwa. Mereka secara khusus dilatih untuk mengambil peralatan

elektronik dan memperoleh gambaran data digital didalam memori. Biasanya ada lebih dari satu yang teknisi yang dilibatkan dalam suatu peristiwa, karena pengetahuan dan ketrampilan berbeda dari tiap teknisi sangatlah diperlukan. Keahlian cukup harus tersedia di tempat peristiwa untuk dapat menunjuk ke semua piranti digital berbeda yang terlibat didalam peristiwa itu.

4. *Evidence Custodians* (Penjaga Bukti) melindungi semua bukti yang dikumpulkan dan disimpan didalam suatu lokasi pusat. Penjaga bukti menerima bukti yang dikumpulkan oleh teknisi, memastikannya berlabel baik, memeriksanya kedalam dan keluar dari pengawasan protektif, serta memastikan suatu penjagaan yang ketat.
5. *Forensic Examiners* (Pemeriksa Forensik) secara khusus dilatih untuk menghasilkan gambaran dari pengambilan peralatan dan pemulihan data digital. Pemeriksa membuat informasi pada *device* yang kelihatan. Pemeriksa dapat juga memperoleh data yang lebih terperinci dengan menggunakan peralatan yang sangat khusus, atau alat-alat sesuai lain yang tak tersedia ke Teknisi Forensik.
6. *Forensic Analysts* (Analisis Forensik) mengevaluasi produk dari Pemeriksa Forensik.

9.4.2 Prinsip – prinsip dalam bukti digital

Ada empat prinsip apabila berhadapan dengan bukti digital, antara lain [1]:

- 1) Tidak ada aksi yang dilakukan oleh penyelidik yang perlu merubah data yang diisi pada alat digital atau media penyimpanan.
- 2) Individu yang akan mengakses data asli harus berkompeten untuk melakukannya dan mempunyai kemampuan untuk menjelaskan tindakan mereka.
- 3) Suatu jejak atau record lain mengenai proses yang diterapkan, yang pantas untuk tinjauan ulang mandiri, harus diciptakan dan dipelihara, dengan meneliti dokumen masing-masing dari setiap langkah investigasi.
- 4) Orang yang bertanggung jawab atas penyelidikan bertanggung jawab penuh untuk memastikan bahwa prosedur diatas diikuti dan sesuai dengan peraturan hukum.

Dalam Pertukaran Bukti Digital, terdapat suatu aturan standard yang disarankan untuk *recover* sebuah bukti berbasis komputer, antara lain :

1. Ketika *seizure* (perampasan) bukti digital, tindakan yang diambil mestinya tidak akan merubah bukti tersebut.

2. Apabila ada seseorang yang penting yang mengakses bukti digital asli, orang itu haruslah berkompeten secara forensik.
3. Semua aktivitas berkenaan dengan *seizure* (perampasan), akses, penyimpanan, atau perpindahan bukti digital harus secara penuh didokumentasikan, dipelihara, dan tersedia untuk tinjauan ulang.
4. Seorang yang bertanggung jawab untuk semua tindakan ke bukti digital selagi bukti yang digital berada didalam pemilikan mereka.
5. Agen manapun yang bertanggung jawab untuk *seizing* (merampas), *accessing* (mengakses), *storing* (menyimpan), atau memindahkan bukti digital bertanggung jawab penuh dengan prinsip ini.

Penanganan bukti yang sesuai selalu penting untuk dapat diterima didalam cara bekerja suatu pengadilan. Bagaimanapun, standard berbeda dapat berlaku untuk jenis penyelidikan yang berbeda.

9.4.3 Model – model Prosedur

The Electronic Crime Scene Investigation - Suatu Pemandu untuk yang Responder Pertama, yang diproduksi oleh Departemen Keadilan U.S., menawarkan usulan apabila mendekati suatu peristiwa kejahatan digital, antara lain [4] :

- a. ***Securing and Evaluating the Scene*** (Mengamankan dan Mengevaluasi Peristiwa) – Langkah yang harus diambil untuk memastikan keselamatan individu untuk mengidentifikasi dan melindungi integritas bukti potensi.
- b. ***Documenting the Scene*** (Dokumentasi suatu Peristiwa) - Menciptakan suatu catatan permanen menyangkut pemandangan peristiwa yang dengan teliti merekam kedua bukti konvensional dan terkait dengan digital.
- c. ***Evidence Collection*** (Koleksi Bukti) - Mengumpulkan bukti digital dan yang memelihara nilai bukti mereka dalam cara tradisional.
- d. ***Packaging, Transportation, and Storage*** (Pengemasan, Transportasi, dan Penyimpanan) - Mengambil tindakan pencegahan cukup dalam pengemasan, pengangkutan, dan menyimpan bukti, serta memelihara rantai penjagaan.

Sebuah “Metologi penanganan suatu peristiwa” sebagai tanggapan dari suatu Peristiwa, mengusulkan beberapa tahapan apabila menemui suatu peristiwa atau ketika melakukan suatu penyelidikan digital [11].

- 1) ***Pre-incident preparation*** (persiapan Pre-Incident) - Melalui pendidikan dan pelatihan, memperoleh suatu pemahaman mengenai bagaimana cara bereaksi terhadap suatu peristiwa.
- 2) ***Detection of incidents*** (Pendeteksian peristiwa) - Mengembangkan teknik mengenai bagaimana cara mendeteksi orang yang dicurigai aktivitasnya.
- 3) ***Initial Response*** (Tanggapan Awal) - Mengkonfirmasi bahwa suatu peristiwa telah terjadi dan memperoleh bukti yang *volatile*.
- 4) ***Response strategy formulation*** (strategi Perumusan tanggapan) - Bereaksi terhadap peristiwa berdasar pada pengetahuan dari semua fakta yang dikenal dikumpulkan dari tahap Awal penanganan.
- 5) ***Duplikasi*** (forensik *backup*) - yang didasarkan atas skenario, yang menciptakan suatu gambaran forensik fisik atau melakukan suatu perolehan kembali tempat bukti.
- 6) ***Investigation*** (Penyelidikan) - Menentukan apa yang terjadi, siapa yang melakukan dan bagaimana peristiwa dapat dicegah di masa datang.
- 7) ***Security measure implementation*** (mengukur implementasi Keamanan) - Menerapkan ukuran keamanan untuk mengisolasi dan berisi sistem yang terkena infeksi.
- 8) ***Network monitoring*** (monitoring Jaringan) - Memonitor lalu lintas jaringan untuk serangan tambahan atau berkelanjutan.
- 9) ***Recovery*** (Kesembuhan) - Mengembalikan sistem yang dipengaruhi kepada suatu jaminan, status operasional.
- 10) ***Reporting*** (Pelaporan) - Detil semua dokumen dan langkah-langkah investigasi yang diambil sepanjang insiden.
- 11) ***Follow-Up*** - Belajar dari peristiwa dengan meninjau ulang bagaimana dan mengapa hal tersebut terjadi dan membuat penyesuaian yang perlu.

Dalam sebuah riset yang dilakukan di Angkatan udara Amerika Serikat mengusulkan langkah-langkah apabila berhadapan dengan suatu penyelidikan forensik [10]:

- 1) ***Identification*** (Identifikasi) - Mengenali dan menentukan jenis suatu peristiwa.
- 2) ***Preparation*** (Persiapan) - Menyiapkan *tools*, teknik, *search warrants* (surat kuasa untuk menggeledah), otorisasi, dan persetujuan manajemen.
- 3) ***Approach Strategy*** (Strategi Pendekatan) - Memaksimalkan bukti koleksi yang bersih selagi memperkecil dampak atas korban.

- 4) **Preservation** (Pemeliharaan) - Mengisolasikan, menjamin/mengamankan, dan memelihara status fisik serta bukti digital.
- 5) **Collection** (Koleksi) – *Record* pemandangan fisik dan salinan bukti digital.
- 6) **Examination** (Pengujian) - Mencari bukti berkenaan dengan kejahatan yang dicurigai itu.
- 7) **Analysis** (Analisa) - Menentukan arti, fragmen rekonstruksi data, dan menarik kesimpulan berdasar pada bukti yang ditemukan. Tahap analisa boleh menghasilkan banyak perkataan berulang sampai suatu teori didukung.
- 8) **Presentation** (Presentasi) - Meringkas dan menjelaskan hal kesimpulan.
- 9) **Return Evidence** (Kembalian Bukti) - Memastikan fisik dan hak milik digital dikembalikan ke pemilik yang sesuai.

Masing-masing model diatas menyangkut cara dan prinsip utama bukti yang berisi titik kunci yang harus dipertimbangkan apabila berhadapan dengan bukti digital. Karena setiap penyelidikan peristiwa pastilah berbeda dan mempunyai keadaan yang unik, pendekatan tunggal pastilah sangat sukar untuk ditentukan. Meskipun demikian, kebanyakan sentuhan model berada pada kondisi pokok yang sama, meskipun demikian tetap menekankan pada aspek yang berbeda. Bagian yang sisanya mengikuti suatu kerangka yang sederhana dari empat area mengenai pokok-pokok perolehan suatu barang yang dipamerkan, membuat suatu salinan muatan forensiknya, memperoleh bukti dari *copy* forensik, dan memberitakan perolehan bukti serta proses menggunakannya. Area ini disebut sebagai *preservation* (pemeliharaan), *acquisition* (perolehan), *examination* (pengujian) dan *analysis* (analisa), dan *reporting* (pelaporan).

Secara umum, bahkan diluar pelaksanaan hukum penyelidikan, bukti harus dikumpulkan dalam suatu cara yang dapat membuat bukti diterima didalam lapangan. Mungkin tidak terlihat nyata apabila suatu penyelidikan diaktifkan. Sebagai contoh, apabila suatu peristiwa keamanan komputer dideteksi pertama, tindakan lapangan akan terjadi. Kemungkinan bukti penting dapat dilewatkan, dengan tidak sesuai ditangani, atau secara kebetulan dibinasakan sebelum peristiwa direalisasikan akan tetap ada.

9.5 Preservation (Pemeliharaan)

Pemeliharaan bukti adalah proses pengambilan hak milik tanpa merubah isi data yang berada pada *device* dan media yang dapat dipindahkan. Pemeliharaan suatu bukti merupakan

langkah pertama dalam memperbaiki bukti digital. Mulai dengan pengenalan umum ke pemeliharaan, kemudian menyediakan lebih mendalam pada panduan PDA yang spesifik.

Pemeliharaan melibatkan pencarian, pengenalan, dokumentasi, dan pengumpulan dari bukti elektronik yang di temukan. Dalam rangka penggunaan bukti dengan baik, apakah didalam suatu pengadilan atau lebih sedikit kelanjutan formal, bukti tetap harus dipelihara. Kegagalan dalam memelihara bukti dalam status aslinya dapat membahayakan keseluruhan penyelidikan, yang berpotensi gagal atau hilangnya informasi berharga tentang suatu peristiwa untuk selamanya.

Berikut adalah suatu ringkasan menyangkut titik kunci dalam pengamatan suatu peristiwa [4]:

1. Mengamankan dan Mengevaluasi Peristiwa

- a. Memastikan keselamatan dari semua individu di peristiwa itu.
- b. Melindungi integritas dari bukti elektronik dan tradisional.
- c. Mengevaluasi peristiwa dan merumuskan suatu rencana pencarian.
- d. Mengidentifikasi bukti potensi.
- e. Semua bukti potensi harus dijamin aman, didokumentasikan, dan dipotret.
- f. Melakukan wawancara.

2. Dokumentasi Peristiwa

- a. Menciptakan suatu catatan historis yang permanen menyangkut peristiwa itu.
- b. Merekam kondisi dan penempatan komputer, media penyimpanan, alat digital lain, serta bukti konvensional dengan teliti.
- c. Penempatan dokumen dan kondisi dari sistem komputer, termasuk menggerakkan status menyangkut komputer (*mode on, off, atau in sleep*).
- d. Mengidentifikasi dan dokumentasi berhubungan dengan komponen elektronik yang tidak akan dikumpulkan.
- e. Memotret keseluruhan peristiwa untuk menciptakan suatu record atau catatan secara visual seperti dicatat oleh responder pertama.

3. Pengumpulan Bukti

- a. Memegang Bukti komputer, apakah fisik atau digital, dengan cara memelihara nilai buktinya.
- b. Memulihkan bukti tidak elektronik (seperti, *password* yang tertulis, catatan tangan, catatan kosong dengan penulisan, perangkat keras dan perangkat lunak manual,

penanggalan, literatur, teks atau hasil print komputer komputer grafis, dan foto).

4. Pengemasan, Mengangkut, dan Penyimpanan Bukti

- a. Tidak membuat aksi untuk menambahkan, memodifikasi, atau menghancurkan data yang disimpan pada suatu komputer atau media lain.
- b. Menghindari kelembaban dan temperatur tinggi, goncangan fisik, keelektrikan statik, dan sumber magnetis.
- c. Memelihara rantai penjagaan dari bukti elektronik, dokumen pengemasannya, penyimpanan dan transportasi.

A. Prosedur Pengemasan

- 1) Didokumentasi dengan baik, label, dan menginventarisir bukti sebelum dibungkus.
- 2) Mengemasi media magnetis didalam pengemasan antistatic (kertas atau plastic antiseptik).
- 3) Menghindari lipatan, *bending* (kelenturan), atau penggarukan media komputer seperti disket, CD-ROMS, *removable media*, dan lain lain.
- 4) Memberi bukti sebuah label dengan baik.

B. Prosedur Memeriksa Transportasi

- 4) Menghindari sumber magnetis (seperti, pemancar radio, *speaker magnets*).
- 5) Menghindari kondisi-kondisi dari panas berlebihan, dingin, atau kelembaban selagi dalam pemindahan.
- 6) Menghindari goncangan dan getaran berlebihan.

C. Prosedur Memeriksa Penyimpanan

- a. Memastikan bukti disimpan menurut kebijakan yang berwenang.
- b. Penyimpanan bukti material didalam suatu kawasan pengamanan yang jauh dari kelembaban dan temperatur yang ekstrim.
- c. Melindungi bukti material dari sumber magnetis, embun, debu, dan partikel unsur atau zat pencemar berbahaya lain.

Subseksi yang sisanya menyediakan informasi bersifat tambahan berhubungan dengan PDA, mengikuti paradigma *search* (pencarian), *recognition* (pengenalan), *documentation* (dokumentasi), dan *collection* (koleksi).

9.5.1 Pencarian

Apabila suatu regu investigasi tiba di tempat peristiwa dengan otorisasi yang sesuai untuk menguji suatu lingkungan yang dicurigai (seperti, surat kuasa untuk menggeledah yang telah disetujui oleh pemilik), mereka perlu memproses dengan hati-hati dan mengikuti langkah-langkah yang perlu untuk memastikan bahwa *device* tiba di laboratorium forensik tanpa kehilangan data. Kesalahan prosedur sepanjang *seizure* (perampasan) dapat menyebabkan hilangnya informasi kritis. Kesadaran akan spesifik *device* dan pemahaman akan berbagai keluarga *device* dan aksesoris serta karakteristik *device* (seperti, pemakaian power, tipe baterai, *cradles*, dan *power supplies*) adalah penting.

Untuk PDA, sumber bukti meliputi *device*, *device cradle*, *power supply*, dan *associated peripherals*, media, dan aksesoris. Media dapat dipindahkan bervariasi yang dapat bersembunyi dan sangat sukar untuk ditemukan. Sering kali media yang dapat dipindahkan dapat dikenali lewat penempatan dan nomor pin atau seperti penampung pin yang ditempatkan pada media yang menetapkan suatu *device* penghubung dengan *device* pada PDA. Lingkup area dan ruang selain dari mana *device* ditemukan harus dicari untuk memastikan bukti terkait tidak dilewatkan. Peralatan yang dihubungkan dengan PDA, seperti komputer pribadi atau kartu memori yang sama dengan PDA, mungkin menjadi lebih berharga dibanding PDA sendiri.

9.5.2 Pengenalan

Agar dapat diproses efektif, jenis *device* yang tepat haruslah dikenali. Seorang individu dapat mencoba melewati seorang spesialis dengan mengubah *device* untuk merahasiakan identitas sebenarnya. Sistem operasi mungkin dimodifikasi atau sepenuhnya digantikan dengan cara yang berbeda, seperti halnya bertindak dengan cara yang berbeda dibanding sebelumnya.

Jika alat digital seperti PDA dalam keadaan "**on**" berarti jenis *device* dapat dikenali oleh sistem operasi, yang lebih tepat dalam identitas *device* dibanding suatu logo. Meskipun demikian, dua sistem operasi yang dominan pada PDA adalah Pocket PC dan Palm OS. PDA berjalan pada satu sistem operasi yang dapat menjalankan sistem operasi alternatif. Sebagai contoh, distribusi Linux yang tersedia dari *handhelds.org* dapat terisi dan dimajukan berbagai Pocket PC *device*. Dengan cara yang sama, versi Linux, seperti Linux PDA, ada untuk Palm OS *device*.

Masing-Masing sistem operasi mempunyai aplikasi tertentu yang terjaln didalam

device penghubung pemakai grafis yang utama (yaitu, *icon* seperti *Word*, *Explorer*, *Memo Pad*, *Terminal*, dan lain-lain). Kunci rahasia lain yang mengizinkan identifikasi dari suatu *device* berikut adalah : *cradle interface*, *manufacturer serial number*, *cradle type*, *power supply*, dan lain-lain. Sinkronisasi perangkat lunak suatu PC yang dihubungkan dapat membantu dalam membedakan antar keluarga sistem operasi.

9.5.3 Dokumentasi

Bukti harus dengan teliti dibukukan dan dikenali. Proses label harus dilakukan untuk mendokumentasikan nomor kasus, membuat uraian ringkas, tandatangan serta waktu dan tanggal bukti ketika dikumpulkan. Sebuah peristiwa kejahatan harus selalu difoto di samping status laporan dokumen dari tiap *device* personal komputer digital (komputer pribadi dapat berisi data bermanfaat yang belum disamakan dengan pemilik PDA). Hal ini akan sangat menolong jika ditanyakan tentang lingkungannya kemudian [8].

Suatu record atau catatan dari semua data harus diciptakan. Semua alat digital (PDA) mungkin dapat menyimpan data dan harus difoto dengan semua kabel penghubung, *cradles*, *power connectors*, *removable media*, and *connections*. Jika alat berada dalam status aktif atau semi-aktif, muatan layar harus difoto dan, jika perlu, direkam dengan tangan. Karakteristik lain seperti aktifitas LED (seperti, *blinking*) atau konektifitas fisik perlu juga untuk dicatat. Setiap orang yang berwenang melaksanakan tugas penjaga bukti di tempat peristiwa, di samping orang yang bertanggung jawab untuk dokumentasi bukti sangatlah diharapkan sepanjang tahap koleksi [8].

Sistem tidak menerima tindakan untuk melihat dan merekam semua data *volatile* ketika menghubungkan bukti sisanya. Sebagai contoh, menjalankan suatu aplikasi untuk melihat alokasi memori atau proses akan menjalankan *overwrite* yang bagian dari memori. Lebih dari itu, mungkin resiko akan mengaktifkan kode tersembunyi *Trojan horse* didalam aplikasi itu.

Rantai prosedur penjagaan merupakan sebuah prosedur sederhana yang belum seefektif proses dokumentasi sebuah perjalanan bukti yang lengkap sampai kepada *lifecycle* dari kasus tersebut. Memelihara rantai penjagaan secara hati-hati tidak hanya akan melindungi integritas bukti, tetapi juga akan membuat sulit seseorang untuk membantah bahwa bukti telah dirusakkan. Bagian dokumentasi perlu menjawab beberapa pertanyaan berikut dalam pelaksanaan tugasnya [8]:

- 1) Siapa yang mengumpulkan itu? (yaitu, alat, media, berhubungan sekeliling, dan lain-

lain).

- 2) Bagaimana dan di mana? (yaitu, bagaimana bukti dikumpulkan dan di mana bukti terletak.
- 3) Siapa yang mengambil kepemilikan bukti? (yaitu, individu yang bertanggung-jawab pada saat pengambilan bukti).
- 4) Bagaimana bukti itu disimpan dan dilindungi didalam penyimpanan? (yaitu, prosedur *evidence-custodian*).
- 5) Siapa yang mengeluarkan bukti dari tempat penyimpanan dan mengapa? (yaitu, nama individu yang bertanggung jawab mendokumentasikan dokumentasi dan tujuan untuk *check-out* bukti)

Dokumentasi bagi semua pertanyaan diatas harus dijaga dan disimpan didalam suatu penyimpanan yang terjamin untuk acuan sekarang dan yang akan datang.

9.5.4 Pengumpulan

Dimana PDA terkait, proses pengumpulan secara normal melibatkan informasi yang *volatile* dan dinamis yang mungkin hilang kecuali jika tindakan pencegahan diambil di tempat peristiwa kejahatan atau terhadap kejahatan tersebut.

"Panduan Praktek Kebaikan untuk Komputer Berdasarkan Bukti Elektronik" menyarankan beberapa prosedur apabila berhadapan dengan PDA:

1. Pada saat *seizure* (perampasan), PDA harus tidak dinyalakan, jika telah off.
2. PDA harus ditempatkan didalam suatu amplop kemudian disegel sebelum dimasukkan kedalam kantong bukti, untuk membatasi akses fisik walaupun masih disegel didalam kantong bukti.
3. Jika PDA dicoba dengan hanya baterai setruman tunggal, kekuatan adaptor yang sesuai harus dihubungkan ke alat dengan kabel yang melintasi kantong bukti sedemikian sehingga bukti dapat disimpan untuk tugas.
4. Jika PDA dinyalakan apabila ditemukan, alat harus ditahan dalam keadaan aktif (seperti, dengan *tapping on a blank section of the screen*) dan disediakan power sampai seorang tenaga ahli dapat mengujinya, untuk menghindari kesalahan dalam mengaktifkan mekanisme keamanan seperti isi dan pengesahan pemakaian *encryption*. Jika power cukup tidak dapat disediakan, pertimbangan harus diberikan dengan mematikan PDA untuk memelihara hidup baterai, dokumentasi alat sekarang dicatat waktu dan tanggal dari

shutdown.

5. Pencarian harus dilaksanakan dengan selau dihubungkan pada memori *device*, seperti SD, MMC, atau CF kartu semikonduktor, *microdrives*, dan USB.
6. Power manapun, kabel, atau *cradles* berkenaan dengan PDA perlu juga ditangkap, seperti halnya manual.
7. Seseorang yang menangani PDA sebelum pengujian perlu diperlakukan sedemikian rupa sehingga mengakui memberikan kesempatan yang baik dalam *me-recover* data sebagai bukti didalam proses selanjutnya.

9.5.5 Berbagai Kondisi dalam koleksi

Di samping level baterai, faktor lain yang dapat mempengaruhi tindakan teknisi dalam menerima situasi yang ditentukan untuk memelihara bukti apabila alat ditemukan dalam suatu status. Sebagai contoh, beberapa alat dapat menerima data melalui jaringan *wireless* yang mungkin akan menimbulkan bukti baru, tetapi tetap akan ada kekuatan *overwrite* data. Oleh karena itu, suatu keputusan dibuat apakah untuk mencegah atau mengijinkan komunikasi *wireless* lebih lanjut [3]. Faktor lain meliputi apakah alat di *cradle*, sama dengan berkomunikasi melalui host komputer, atau mempunyai kartu memori yang dimasukkan. Tabel 9.1 menyediakan daftar kondisi-kondisi umum dan tindakan yang dihubungkan untuk teknisi forensik dalam mempertimbangkan untuk mengenali tujuan yang ingin dicapai.

No.	Kondisi atau Tujuan	Aksi
1.	Device ON	<ul style="list-style-type: none"> • Tinggalkan device dalam keadaan “on” dan tetap aktif. • Jika level baterai sudah rendah, segera ganti dengan yang baru atau disarankan untuk men-charge baterai dengan power adaptor device. • Memelihara level baterai dengan power adaptor device atau penggantian baterai secara berkala. • Ciptakan gambaran pada device ketika keadaan diizinkan.
	<ul style="list-style-type: none"> • Memelihara device dalam keadaan aktif dengan mengukur level power yang cukup. • Memperoleh gambar pada kesempatan paling awal. 	
2.	Device OFF	<ul style="list-style-type: none"> • Tinggalkan device dalam keadaan “off”. • Secepatnya ganti baterai dengan yang baru, atau secara berkala diganti dengan yang baru, atau disarankan untuk di charge dengan power adaptor device. • Ciptakan gambaran pada device ketika keadaan diizinkan.
	<ul style="list-style-type: none"> • Memelihara ukuran level power pada device. • Memperoleh gambar pada kesempatan paling awal. 	
3.	Device dalam cradle	<ul style="list-style-type: none"> • Tarik USB sebagai alat penghubung koneksi dari

	<ul style="list-style-type: none"> Hapus kemungkinan aktifitas komunikasi lebih lanjut. 	<ul style="list-style-type: none"> computer Jika kondisi device “on” lihat kondisi 1 Jika kondisi device “off” lihat kondisi 2 Tarik cradle-nya
4.	Device diluar cradle <ul style="list-style-type: none"> Kumpulkan material bukti-bukti yang saling berhubungan. 	<ul style="list-style-type: none"> Jika kondisi device “on” lihat kondisi 1 Jika kondisi device “off” lihat kondisi 2 Tarik cradle-nya
5.	Wireless (Wi-Fi, Bluetooth, dan lain-lain) ON <ul style="list-style-type: none"> Hapus kemungkinan aktifitas komunikasi lebih lanjut. 	<ul style="list-style-type: none"> Lihat kondisi 1 segera bungkus alat dalam suatu amplop, kantong anti-static, dan suatu kotak pengasingan dengan perbandingan frekwensi, hapus kemungkinan koneksi dari alat atau mesin yang lain.
6.	Wireless (Wi-Fi, Bluetooth, dan lain-lain) OFF <ul style="list-style-type: none"> Kumpulkan material bukti-bukti yang saling berhubungan. 	<ul style="list-style-type: none"> Lihat kondisi 1. Segera bungkus alat untuk mengurangi aktifitas wireless yang sedang terjadi.
7.	Kartu dalam kartu expansion <ul style="list-style-type: none"> Menghindari aktifitas didalam alat lebih lanjut lagi. 	<ul style="list-style-type: none"> Hindari pemindahan peripheral atau kartu media apapun, seperti (CF, SD, MMC)
8.	Kartu tidak dalam kartu expansion	<ul style="list-style-type: none"> Tarik hubungan peripheral atau kartu media apapun, seperti (CF, SD, MMC)
	<ul style="list-style-type: none"> Kumpulkan material bukti-bukti yang saling berhubungan. 	
9.	Expansion Sleeve Attached <ul style="list-style-type: none"> Menghindari aktifitas didalam alat lebih lanjut lagi. 	<ul style="list-style-type: none"> Hindari pemindahan expansion sleeve Hindari pemindahan peripheral atau kartu media (contoh CF, SD, MMC) dari sleeve Jika wireless dan network terjadi koneksi, lihat kondisi 5
10.	Expansion Sleeve Removed	<ul style="list-style-type: none"> Ukur expansion sleeve Ukur peripheral dan kartu media (contoh CF, SD, MMC) yang saling terhubung.

Tabel 9.1 daftar kondisi-kondisi umum beserta tindakan yang dipakai

9.6 Acquisition (perolehan)

Acquisition adalah proses dalam menggambarkan atau memperoleh informasi dari suatu alat digital dan media serta peralatan di sekelilingnya.

Acquisition dapat terjadi pada suatu laboratorium forensik ketika informasi yang didapat telah dengan aman didaftar. Keuntungan dalam melakukan *Acquisition* di tempat peristiwa adalah bahwa hilangnya informasi dalam kaitan dengan penghabisan baterai, kerusakan, dan lainnya dapat dihindarkan. Karena dalam tahapan ini kita menemukan suatu aturan yang dapat dikendalikan dan digunakan untuk bekerja, mempunyai peralatan yang

sesuai, dan memuaskan prasyarat lain yang tidak boleh terjadi di tempat peristiwa, tetapi sebagai gantinya persediaan dalam laboratorium yang telah diatur.

Ketika *device* telah tiba di laboratorium forensik, pemeriksa forensik memulai *Acquisition* dengan mengidentifikasi *device*. Tipe dari alat dan dan Jenis sistem operasi yang dapat menentukan rute untuk melihat ciptaan dari suatu gambaran *bit-for-bit* jika tidak memperoleh muatan dari *device*. Hanya ada sedikit perangkat lunak *forensic tools* yang berbeda dengan gambaran PDA sekarang ini dan tak seorangpun yang dapat segera menangani cakupan *device* yang penuh pada pasar. Oleh karena itu, jenis PDA dan sistem operasi biasanya melihat aplikasi mana yang digunakan dalam suatu penyelidikan [2].

Secara normal, *forensik toolkit* menggunakan *acquisition* untuk analisa dan pengujian. Di mana ada suatu pilihan diantara beberapa *tools*, seperti Palm OS *device*, *interoperability* antar fasilitas pengujian dan *acquisition* mungkin hadir, seperti ditunjukkan dalam Tabel 9.2 yang menunjukkan hasil data yang diperoleh oleh satu *device*, yang ditandai oleh *row header*, dan dianalisa oleh yang lain, yang ditandai oleh *column header*. *Interoperability* suatu aspek penting untuk pertimbangan, karena beberapa *tools* mungkin terbatas pada sistem operasi versi spesifik atau tidak boleh mendukung model *device* tertentu. Lebih dari itu, adakalanya satu *tool forensik* dapat gagal untuk memperoleh informasi dari suatu spesifik *device*, selagi *device* yang lain bekerja tanpa permasalahan.

	POSE	PDA Seizure	EnCase
Pdd	Menerima gambar ROM, tapi pdd tidak mengeluarkan database tersendiri.	Menerima gambar ROM dan RAM yang diproduksi, dengan hanya fungsi pasrial.	Menerima gambar ROM dan RAM yang diproduksi
Pilot-Link	Menerima gambar ROM dan database tersendiri yang diciptakan berturut-turut dengan pi-getrom dan pilot-xfer.	Menerima gambar ROM, RAM dan database tersendiri yang diciptakan berturut-turut dengan pi-getrom, pi-getram dan pilot-xfer.	Menerima gambar ROM, RAM dan database tersendiri yang diciptakan berturut-turut dengan pi-getrom, pi-getram dan pilot-xfer.
PDA Seizure	Berdiri dengan versi dari POSE yang menerima keluaran perolehan secara implisit.	Bekerja secara implicit	Menerima gambar ROM dan RAM yang diproduksi
EnCase	Menerima database tersendiri yang diproduksi	Menerima gambar ROM dan RAM yang diproduksi, dengan hanya fungsi parsial.	Bekerja secara implisit

Tabel 9.2 Interoperability diantara Palm OS Tools

Pemeriksa forensik disarankan mengadakan percobaan dengan berbagai *toolkits* pada *test device* untuk menemukan *tools* yang dapat bekerja secara efisien dengan jenis *device* tertentu, dan untuk menentukan tingkat derajat *interoperability* antar *tools* pengujian dan *acquisition* yang berbeda untuk suatu keluarga *device*. Di samping memperoleh keakraban dengan kemampuan dari *device*, percobaan mengijinkan sebuah kebiasaan dan campuran konfigurasi khusus untuk disediakan sebelum penggunaan dalam suatu kasus nyata. Perangkat lunak yang diperbaharui dari pabrik dapat diinstal.

Tidak masalah apakah *device* adalah Pocket PC, Palm OS, atau berbasis Linux, untuk memperoleh data tersebut, suatu koneksi harus dibentuk dari *workstation* spesialis forensik kepada *device* tersebut. Sebelum melakukan suatu *acquisition*, versi dari *device* yang sedang digunakan harus didokumentasikan bersama dengan kesalahan apapun atau tambalan yang dapat diterapkan dari pabrik dan berlaku untuk *device* tersebut. Sekali ketika koneksi telah dibentuk, deretan perangkat lunak forensik dapat mulai memperoleh data dari *device* dengan baik.

Tidak sama dengan *network server* atau mesin *desktop*, PDA terbaru kini tidak punya perangkat keras dan mempercayakan memori semikonduktor sebagai ganti dengan sepenuhnya. Perangkat lunak yang khusus ada untuk memproduksi suatu gambaran *device*, seperti halnya melakukan suatu pengadaan logis data PIM. Bagaimanapun, muatan dari suatu PDA adalah dinamis dan secara terus menerus berubah, bahkan ketika dimatikan (dalam status diam). Dua pengadaan suatu *device back-to-back* menggunakan *device* yang sama menghasilkan hasil berbeda secara keseluruhan, meskipun mayoritas informasi, seperti data PIM, tinggal tanpa perubahan. Untuk gambaran suatu PDA memori *device*, *device* harus dinyalakan, yang merupakan perbedaan utama dari komputer pribadi. Hal ini secara efektif berarti prinsip *evidentiary* yang pertama tersebut dibagi dalam 4 bagian – *actions taken should not modify data contained on the device* – (aksi yang diambil tidak akan memodifikasi data yang terkena pada *device*) pada hakekatnya tidak bisa ditaati. Oleh karena itu, tujuan perolehan PDA akan mempengaruhi muatan memori sedikit sama dan kemudian hanya dalam pengetahuan terjadi secara internal, lebih mementingkan pada kesetiaan pada prinsip kedua dan ketiga *evidentiary*, yang menekan kemampuan dari spesialis dan pembuatan suatu audit secara terperinci [1].

Setelah suatu *acquisition* selesai, spesialis forensik harus selalu mengkonfirmasi bahwa keseluruhan muatan dari suatu *device* ditangkap dengan tepat (yaitu, memverifikasi

ukuran RAM/ROM yang memastikan konsistensi dengan *device*). Pada suatu kesempatan, suatu *device* dapat gagal dari tugasnya tanpa pemberitahuan kesalahan dan memerlukan spesialis untuk mencobanya kembali baik dengan *device* yang sama maupun dengan *device* yang lain. Dengan cara yang sama, beberapa *tools* tidak bekerja baik dengan *device* tertentu seperti yang orang lain lakukan, dan dapat gagal karena suatu pemberitahuan kesalahan. Apabila mungkin, sebaiknya untuk mempunyai berbagai *tools* yang tersedia.

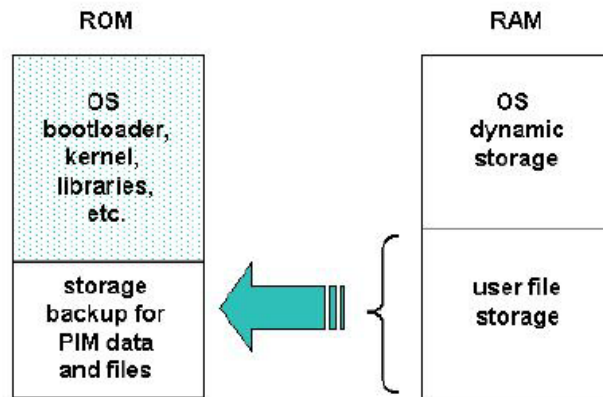
9.6.1 Device tanpa halangan

Suatu *device* yang tanpa halangan adalah suatu *device* yang tidak memerlukan suatu *password* atau teknik pengesahan lain untuk dicukupi untuk diwarisi akses kepada *device* itu. Dari informasi *anekdot*, kebanyakan *device* ditangkap didalam penyelidikan terlihat masuk ke kategori ini. Seperti disebut lebih awal, apabila perampasan suatu "*Unobstructed Device* (*device* tanpa halangan)" perhatian yang digunakan harus dihindari, sebagai contoh, mengubah status dari *device* dengan menekan urutan tali kunci yang mempunyai potensi untuk merusak atau menghapus bukti berharga.

Secara umum, sebuah PDA mempunyai empat kategori penyimpanan yang utama untuk mempertimbangkan kode sistem operasi, mencakup *kernel*, *device drivers*, dan *system libraries* dengan dinamis dialokasikan untuk pelaksanaan aplikasi sistem operasi dan menyimpan serta melaksanakan aplikasi pemakai tambahan ke alat, penyimpanan pemakai untuk berbagai jenis data file, mencakup teks, gambaran, dan bunyi serta *backup* data kritis mengenai aplikasi informasi PIM dan data file. Karakteristik empat kategori ini terbentang dari yang sangat stabil ke yang *volatile*. Perbedaan ini dikombinasikan dengan karakteristik dari suatu sistem operasi spesifik, yang menentukan bagaimana ROM dan RAM digunakan untuk mendukung masing-masing kategori penyimpanan.

Gambar 9.1 menggambarkan pengaturan yang paling khas. *Flash* ROM yang digunakan sebagian besar untuk memegang kode sistem operasi dan secara bebas dapat memilih data PIM manapun atau file yang di-*backup* oleh pemakai kedalam ruang yang sisanya. *Flash memory* mempunyai waktu terbatas, kira-kira 100,000 siklus untuk menghapus. RAM digunakan untuk penyimpanan dinamis dan penyimpanan file pemakai. Suatu *soft reset* (yaitu, *warm boot*) yang secara khas me-*reinitializes* penyimpanan yang dinamis didalam RAM, tetapi daun file penyimpanan pemakai tidak disentuh, sedang suatu *hard reset* (yaitu, *cold boot*) dapat me-*reinitializes* keduanya. Dengan sepenuhnya mengalirkan power dari PDA yang mempunyai efek yang sama sebagai efek yang keras. ROM tidak dibuat baik oleh suatu

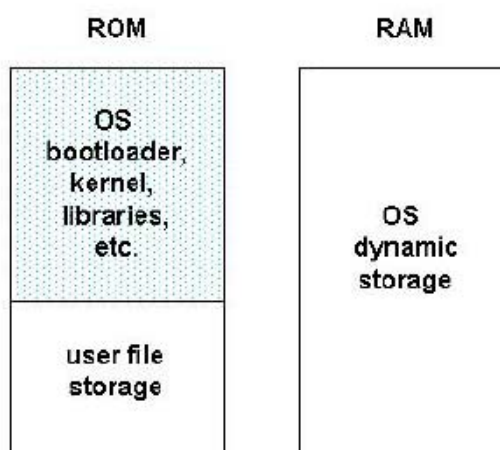
reset lembut maupun yang keras.



Gambar 9.1 Pengaturan storage pada ROM dan RAM

Suatu pengaturan memori alternatif umum ditunjukkan dalam Gambar 9.2. Di sini pemakai file penyimpanan berada dalam *Flash* ROM dengan kode sistem operasi, yang mana menghindari kebutuhan akan kegunaan *backup*, karena penyimpanan tidak dibuat terus-menerus dan tidak dipengaruhi oleh reset dan aliran power. Ukuran ROM dan RAM secara normal berbeda (yaitu, ROM lebih dan RAM lebih sedikit) apabila dibandingkan dengan pengaturan lebih awal untuk menyediakan kapasitas yang setaraf. Untuk menyimpan file penyimpanan pemakai didalam ROM dengan RAM, suatu *filesystem* khusus diperlukan untuk menghindari percepatan hidup media tersebut. File sistem seperti JFFS2 (*The Journaling Flash File System*, versi 2) dirancang secara rinci untuk mengatur pemakaian *flash memory* secara hati-hati. Sebagai contoh, JFFS2 mencegah menulis kembali suatu keseluruhan sektor untuk menghapus *byte* tunggal dan memastikan bahwa lingkup memori yang berbeda digunakan bergiliran untuk mengatur pemakaian.

Karena terbatasnya jumlah *tools forensik* yang ada untuk pengadaan muatan ROM dan ROM dari suatu PDA, pilihan sederhana sering jadi. Satu pertimbangan utama akan memelihara kecocokan dengan *toolkit* yang secepatnya digunakan didalam analisa dan pengujian, karena interoperabilas antar PDA *tools* berbeda, terutama kasus komersil file format tidak dijamin.



Gambar 9.2 Alternatif Pengaturan ROM dan RAM

Dalam rangka memelihara integritas data, pemeriksa perlu menangani bukti yang asli mungkin lebih sedikit sama. Biasanya, direkomendasikan untuk menciptakan sebuah salinan "master" forensik *device* dulu, yang dijaga dengan sepenuhnya. *Copy* master kemudian digunakan untuk menciptakan gambaran cermin tambahan untuk pengujian dan analisa bukti [12]. Suatu jalan searah *cryptographic hash* (misalnya, SHA1) harus dilakukan untuk memastikan bahwa gambaran tambahan yang diciptakan *copy* dari master adalah serupa.

9.6.2 Device yang dihalangi

Device yang dihalangi mengacu pada *device* yang ditutup (dalam status diam) dan memerlukan *authentication* dengan menggunakan *password* atau beberapa alat lain untuk memperoleh akses. *Password* melindungi *device* yang secara normal memerlukan keahlian dari suatu spesialis forensik secara khusus dilatih untuk memperoleh akses ke muatan *device*, selagi pemeliharaan integritas menyangkut informasi dan menghindarkan kerusakan pada *device* tersebut. Sejumlah jalan ada untuk menyadap data dari *device* yang dihalangi. Mereka masuk kedalam tiga kelas: *investigative*, *metoda hardware-based* dan *software-based*.

Perangkat lunak dan metoda *hardware-based* sering dikembangkan terutama untuk *device* tertentu atau untuk membatasi kelas *device*. Didalam mengembangkan suatu metoda, tindakan berikut harus dipertimbangkan untuk menentukan pendekatan lain yang mungkin :

- 1) Menghubungi *device* pabrik untuk informasi yang dikenal *backdoors* dan sifat mudah diserang yang dapat dimanfaatkan.
- 2) Meninjau ulang spesifikasi pabrik dan dokumentasi lain apabila perumusan eksploitasi

masuk akal.

- 3) Menghubungi para profesional untuk *me-recover* bukti komersil yang dikhususkan dalam *handheld devices*.
- 4) Menghubungi pemelihara *devices* dan perusahaan perbaikan, seperti halnya organisasi komersil yang menyediakan informasi arsitektur pada *handheld devices products*.

9.6.2.1 Metode Investigasi

Metoda Investigasi adalah prosedur regu isvestigasi yang dapat diterapkan, yang mana tidak memerlukan perangkat lunak atau perangkat keras *tools forensik*. metoda yang paling jelas adalah sebagai berikut:

1. *Ask the suspect* (menanyai orang yang dicurigai) - Jika suatu *device* dilindungi dengan kata sandi, pin, tanda, atau mekanisme pengesahan lain yang menyertakan pengesahan berbasis pengetahuan, orang yang dicurigai dapat disangsikan untuk informasi ini sepanjang wawancara awal.
2. *Review seized material* (meninjau ulang material penangkapan) - *password* sering dituliskan pada suatu catatan dan yang dijaga dengan atau dekat *device*, pada suatu komputer *desktop* yang digunakan untuk mencocokkannya dengan *device*, atau pada orang yang dicurigai, seperti didalam suatu dompet.
3. *Manually supply commonly used input* (Mengirimkan masukkan yang digunakan secara manual) - Para pemakai dapat memperlemah suatu mekanisme yang digunakan. Sebagai contoh, jika suatu *device* memerlukan suatu 4-digit pin, suatu pemeriksa ingin dapat mencoba kombinasi 1-2-3-4, seperti ketika salah satu dari ke tiga terkaan yang diijinkan sebelum *device* dengan sepenuhnya dikunci bawah.

9.6.2.2 Metode Software-based

Metoda *Software-based* melibatkan teknik perangkat lunak untuk dipecahkan atau *mem-bypass* mekanisme pengesahan. Sedang beberapa alasan umum untuk teknik perangkat lunak dan *tools* dapat dapat dilihat pada kelas PDA *device*. Apabila suatu teknik khusus dikembangkan, hal itu secara normal diprogramkan dan diuji pada suatu *device* test serupa. Metoda *Software-based* meliputi yang berikut:

1. *Exploit known weaknesses in authentication* (Mengeksploitasi kelemahan yang diketahui dalam pengesahan) - Jika suatu mekanisme pengesahan lemah, memanfaatkan kelemahan

untuk mengalahkan mungkin saja bisa. Sebagai contoh, awal perlindungan *password* pada PDA Palm OS di-*obfuscate password* yang menggunakan suatu algoritma yang dapat dibalik [6], membiarkan di-*recover* dengan mudah dari *device* yang menjalankan versi 4.0 atau lebih awal, menggunakan suatu kegunaan.

2. *Gain access through a backdoor* (Keuntungan mengakses melalui suatu backdoor) - Pabrik sering membangun didalam fasilitas test atau *backdoors* lain bahwa suatu pemeriksa dapat memanfaatkannya untuk memperoleh informasi. Sebagai contoh, *bootloaders* pada beberapa PDA *device* pendukung berfungsi mengijinkan memori *device* untuk dibaca dan dicopy atau dipancarkan.
3. *Exploit known system vulnerabilities* (Sistem Eksploitasi dikenal penyerang) - Sistem mobile dapat memiliki sifat mudah diserang didalam suatu standar *interface protokol* yang dapat pemeriksa manfaatkan untuk mem-*bypass* pengesahan dan keuntungan mengakses informasi. Sebagai contoh, mengakses *device* mungkin melalui suatu *network service misconfigured*, kekurangan didalam suatu protokol *networking* standar yang didukung oleh *device*, atau kesalahan didalam implementasi protokol yang membuatnya peka kepada suatu metoda serangan seperti *buffer overflow*. Komunikasi mungkin menghubungkan untuk penghisapan meliputi yang serial, USB, *Irda*, *Bluetooth*, *Wifi*, dan fasilitas GSM/GPRS.

9.6.2.3 Metode Hardware-based

Metoda *Hardware-based* melibatkan suatu kombinasi perangkat lunak dan perangkat keras yang mematahkan atau mem-*bypass* mekanisme pengesahan. Sebagai alasan umum, metoda *hardware-based* berlaku bagi suatu kelas PDA *device* umum. Kebanyakan menyangkut teknik khusus untuk suatu model yang spesifik dalam suatu kelas. Seperti dengan metoda *software-based*, apabila suatu teknik khusus dikembangkan, secara normal dikembangkan penggunaan suatu alat test yang serupa kepada satu orang di bawah pengujian. *Device* pabrik dapat juga menyediakan informasi bermanfaat dan *tools* untuk penyulingan data. metoda *Hardware-based* yang didasarkan meliputi yang berikut:

1. *Gain access through a hardware backdoor* (Keuntungan mengakses melalui suatu perangkat keras backdoor) - Perangkat keras *backdoors*, seperti *device* penghubung untuk *debugging*, pengujian produksi, atau pemeliharaan, mungkin digunakan untuk memperoleh akses ke memori. Sebagai contoh, beberapa *device* mempunyai perangkat

keras test aktif menunjuk pada sirkuit menumpang bahwa dapat digunakan untuk memeriksa *device* itu. Banyak pabrik sekarang yang mendukung JTAG (Joint Test Action Group) standar, yang mana menggambarkan suatu test umum untuk prosesor, memori, dan chip semikonduktor lain, pada alat mereka.

2. *Examine memory independently of the device* (Menguji memori bebas dari device) - Suatu pemeriksa berpengalaman mungkin mampu menguji memori chips secara langsung pada *device* dan informasi penting dari mereka. Sebagai contoh, Institut Forensik Netherlands telah mengembangkan suatu maksud umum *device* untuk pengujian suatu cakupan luas chip memori. Ketika secara fisik menghubungkan melalui suatu klip memori, alat tidak hanya dapat untuk dibaca dan menyimpan muatan memori, tetapi juga ke *overwrite* [7].
3. *Reverse engineer the device to find and exploit a vulnerability* (Merekayasa balik device untuk menemukan dan memanfaatkan suatu sifat mudah diserang) - Kebalikan Rancang-Bangun mendapat kembali kode sistem operasi dari ROM dari suatu PDA yang serupa kepada seseorang di bawah pengujian dan meneliti kode untuk memahami penggunaannya menyangkut *device* perangkat keras. Sebagai contoh, karena suatu mekanisme pengesahan *password*, mungkin saja menggunakan memori suntikan untuk *overwrite password* dengan nilai yang dikenal atau menggantikan program pengesahan dengan suatu versi yang selalu membuktikan keaslian dengan sukses, seperti dilaporkan untuk XDA PDA/PHONE *hybrid device*-nya.
4. Menyimpulkan informasi dengan monitoring karakteristik alat fisik teknik yang memonitor penggunaan power atau karakteristik alat lain menjadi efektif secara sistematis menentukan *password* atau pin. Sebagai contoh, spesialis forensik melaporkan bahwa *password* beberapa organisator elektronik telah terbongkar dengan menentukan area alamat dari *password* dan ketika karakter dimasukkan, secara sistematis data dimonitor dan menunjuk ke bus [7].
5. Penggunaan mengotomatiskan kekuatan fisik jika suatu mekanisme *password* tidak memiliki pembatasan pada banyaknya usaha manual yang dibuat dan pemeriksa mempunyai waktu luang, serangan kekuatan fisik kamus dapat dicoba. Secara normal, pendekatan ini akan menjadi hal yang tidak mungkin. Bagaimanapun, dengan tombol masukan diotomatiskan, akan menjadi masuk akal. Sebagai contoh, Institut Forensik Netherlands mengembangkan, suatu *password* masukan untuk sistem yang diotomatiskan untuk alat dengan suatu *keyboard* dan layar dilengkapi dengan suatu tangan robot dan

video kamera unit yang secara sistematis memasukkan kata sandi sampai masukan dideteksi atau didalam kasus yang terburuk, kunci menjadi rusak [7].

9.6.2.4 Peralatan Tangential

Peralatan tangensial meliputi *device* yang berisi memori dan dihubungkan dengan suatu PDA. Dua kategori utama dalam peralatan ini adalah host komputer dan kartu memori untuk PDA yang mana telah disamakan muatannya. Yang anehnya adalah USB *memory drives*, yang biasa untuk host komputer, biasanya tak satu faktor pun untuk PDA karena masalah pada *device* penghubung.

PDA, khususnya model yang terakhir, secara khas mendukung *Compact Flash* (CF), *Secure Digital* (SD), *Multi-Media Cards* (MMC), dan jenis media lain yang dapat dipindahkan dan dirancang terutama untuk *handheld devices*, yang mana berisi sejumlah data penting. Seperti halnya RAM dan ROM, kartu memori adalah memori semikonduktor. Mereka digunakan sebagai alat bantu pemakai file penyimpanan, *backup* dari isi data penting pada PDA, atau bermakna untuk menyampaikan file ke dan dari *device* tersebut. Ukuran fisik kartu memori yang didukung oleh *handheld devices* adalah penting sepanjang mereka berukuran kecil, seukuran koin, dan mudah untuk dilewatkan. Oleh karena itu, penyelidik memerlukan banyak waktu dalam penyelidikan. Data dapat diperoleh dari media dan dapat dipindahkan dengan penggunaan dari suatu pembaca media dan suatu aplikasi forensik untuk menggambarkan *hard driver*.

Data yang diisi pada suatu PDA sering disajikan pada suatu komputer pribadi karena berkaitan dengan kemampuan dari suatu PDA untuk mensinkronkan atau berbagi informasi antar satu atau lebih *host* komputer. Komputer pribadi atau *workstation* seperti itu dikenal sebagai *synched devices*. Karena sinkronisasi ini, sejumlah bukti yang penting pada suatu PDA, dapat juga hadir pada laptop orang yang dicurigai atau komputer pribadi, dan dalam pengembalian kondisi ke suatu komputer *forensik tools* konvensional untuk pengujian dan *acquisition* hard drive.

USB *drives*, kadang dikenal sebagai *thumb drives*, yang merupakan ukuran komponen perangkat keras *chewing-gum-pack* dengan konektor USB dan dibangun sebagai sirkuit yang dicetak didalam suatu plastik yang dibungkus oleh suatu memori dan prosesor. USB memori *drive* dapat diperlakukan dengan cara yang sama untuk suatu *disk drive* yang dapat dipindahkan, dan difoto serta dianalisa menggunakan *forensik tools konvensional*.

9.6.2.5 Synched Device

Sinkronisasi mengacu pada proses perbedaan pemecahan didalam kelas informasi tertentu, seperti e-mail, tempat tinggal pada dua device (yaitu, suatu PDA dan PC), seperti yang kedua-duanya kebanyakan mempertahankan versi sekarang, yang mana mencerminkan tindakan apapun yang diambil oleh pemakai (seperti, penghapusan) pada satu *device* atau *device* lainnya. Tergantung pada bagaimana *device* yang dicurigai diatur, sejumlah data informatif penting dapat berada di komputer pribadi itu. Apabila suatu koneksi dibentuk antara *device* dan PC, pemakai boleh berkomunikasi sampai jenis account berikut:

1. Account Tamu - Tidak ada data secara otomatis disamakan antara alat dan PC, kecuali jika diaktifkan oleh pemakai.
2. Account Pemakai- Ketika koneksi, data disamakan secara otomatis antara PC dan *device*. Pemakai *predefines* apa yang data synched dan *device* yang mana yang mengambil hak yang lebih tinggi. Kebanyakan *handheld device* diatur untuk mensinkronkan data baru, seperti pesan, masukkan buku alamat, dan agenda informasi.

Sinkronisasi informasi dapat terjadi baik pada level record maupun level file. Apabila dilaksanakan, ditingkatan file manapun bertentangan dari waktu dan tanggal sinkronisasi terakhir yang mengakibatkan versi yang terakhir secara otomatis menggantikan versi yang lebih lama tersebut. Intervensi manual adakalanya diperlukan jika kedua versi dimodifikasi dengan bebas karena sinkronisasi yang terakhir terjadi. *Record* tingkatan Sinkronisasi dilaksanakan dengan cara yang sama, tetapi dengan lebih *granularas* dengan yang hanya bagian dari file yang dipecahkan dan digantikan.

Dengan Palm OS *device*, tingkatan sinkronisasi *record* adalah norma itu. Inti database PIM yang dapat disamakan meliputi: *Address Book, Date Book, Memo Pad, Note Pad, dan To Do List*. Inti aplikasi file PIM bahwa dapat disamakan meliputi yang berikut: *Calendar, Contacts, Inbox, Pocket Access, Tasks, and Favorites*. Perangkat lunak sinkronisasi selain yang dibangun kedalam sistem operasi juga ada dan dapat menyediakan sesuatu yang lebih luas dengan kemampuan yang berbeda. Sebab muatan yang disamakan dari suatu PDA dan komputer pribadi cenderung berbeda dengan cepat dari waktu ke waktu, informasi tambahan mungkin ditemukan didalam satu *device* atau *device* lainnya.

Digital *device* didiami oleh data dari PC sepanjang proses sinkronisasi. Data dari PDA dapat juga disamakan kepada PC, melalui pilihan *user-defined* dalam perangkat lunak

sinkronisasi. Perangkat lunak sinkronisasi dan jenis *device* menentukan dimana file PDA mungkin disimpan pada PC tersebut. Masing-masing protokol sinkronisasi mempunyai suatu direktori instalasi, tetapi tempat terjadi peristiwa pemakai dapat ditetapkan. Hotsync manajer Palm menyimpan perpindahan data yang berisi: tanggal, lokasi dari data, dan informasi apa yang di-*synched*.

9.6.2.6 USB Memory Drives

Banyak pabrik yang memproduksi memori USB *drive* dalam beberapa kapasitas. Sekarang ini, sedikit sekali PDA *device* yang mendukung host USB port, yang diperlukan untuk menghubungkan dengan sekelilingnya. Lebih dari itu, ada sedikit pabrik USB drive yang menyediakan drive yang perlu untuk sistem operasi PDA. Situasi ini dapat dimengerti karena spesifikasi host USB membuat alat penghubung untuk mampu mendukung berbagai *device*, berbagai host, yang mana jika diijinkan akan menempatkan power yang penting yang akan mengalirkan baterai dari *device* tersebut. Faktor lain meliputi pembatasan didalam mobilitas yang dikenakan oleh suatu USB *drive* yang menyangkut sisi dari PDA dibandingkan keuntungan yang menyediakan satu atau lebih slot kartu memori yang dengan sepenuhnya berisi kartu apabila dimasukkan.

Seperti dengan perluasan kartu memori, USB *drive* dapat menawarkan kemampuan tambahan seperti suatu alat penghubung *wireless*. Mengakses kekuatan memori dapat juga dilindungi melalui suatu sidik jari pembaca yang *built-in* atau beberapa mekanisme lain seperti suatu smart card, yang mana mempersulit proses *acquisition*. Bagaimanapun, untuk pertimbangan tersebut di atas yang sekeliling ini adalah tidak secara normal dihubungkan dengan PDA *device*.

9.7 Pengujian dan Analisis

Proses pengujian memberi cahaya ke data *probative* dan hasilnya diperoleh melalui penerapan metoda didasarkan pada ilmiah yang dibentuk, perlu menguraikan isi dan status dari data dengan sepenuhnya. Dokumentasi seperti itu mengijinkan semua data untuk menemukan apa yang dimasukkan, seperti informasi yang mungkin tersembunyi atau digelapkan. Ketika semua informasi diarahkan, pengurangan data dapat dimulai, dengan demikian memisahkan dari informasi yang relevan ke informasi yang tidak relevan. Proses Analisa berbeda dengan proses pengujian didalam yang meneliti produk dari pengujian.

Pengujian adalah pengolahan secara teknis proses dari spesialis forensik. Analisa mungkin dilaksanakan oleh peranan lain dibanding analis yang forensik, seperti penyelidik atau pemeriksa forensik. Seseorang dapat melaksanakan semua peran yang dilibatkan [1].

Proses pengujian dimulai setelah forensik *workstation* telah disediakan dengan *tools* yang sesuai dan *copy* dari bukti yang diperoleh dari alat tersebut. Jika tersedia, pemeriksa dapat mempelajari kasus dan menjadi terbiasa dengan parameter dari serangan, dan bukti potensial yang ditemukan. Melakukan pengujian didalam suatu perkumpulan dengan analis forensik atau penyelidik memandu konstruksi kasus sebaiknya untuk pemeriksa itu. analis atau penyelidik menyediakan pengertian yang mendalam ke dalam tipe hal yang dicari, sedang pemeriksa forensik menyediakan rata-rata untuk informasi relevan yang ditemukan yang dapat terjadi pada sistem itu.

Jika pemeriksa forensik melakukan analisa dengan bebas, tanpa berunding dengan penyelidik atau analis forensik, pengetahuan yang diperoleh dengan mempelajari kasus perlu menyediakan gagasan tentang *password* yang spesifik atau ungkapan untuk menggunakan ketika mencari gambaran yang diperoleh dari alat tersebut. Bandingkan dengan pengujian *server network* atau *workstation* individu, jumlah data yang diperoleh, dalam kaitan dengan ukuran gambaran mentah, apakah lebih banyak kecil yaitu, Mbytes melawan Gbytes.

Tergantung pada jenis kasus, strateginyapun akan bervariasi. Suatu kasus tentang pornografi anak dapat mulai dengan *browsing* semua gambaran yang grafis pada sistem, sedang suatu kasus tentang suatu serangan *Internet-Related* mungkin dapat mulai dengan *browsing* internet mengenai sejarah file. Pengujian sering mengungkapkan tidak hanya data berpotensi yang bersifat menuduh tetapi juga informasi bermanfaat seperti *password*, jaringan logon nama, dan aktivitas Internet. Sebagai tambahan terhadap bukti yang secara langsung berhubungan dengan suatu peristiwa, informasi dapat terbongkar mengenai *lifestyle* dari orang yang dicurigai, rekanan mereka, dan jenis aktivitas di mana mereka dilibatkan.

9.7.1 Lokasi Bukti

Standard PDA secara khas menawarkan informasi serupa yang menangani kemampuan dan ciri, termasuk aplikasi Manajemen informasi Pribadi (PIM), dukungan untuk e-mail, dan *Web browsing*. *Hybrid device* yang menyertakan PDA keduanya dan kemampuan *cell phone* juga ada. Bukti potensial pada alat ini meliputi [4]:

1. Buku alamat
2. Kalender janji atau informasi

3. Dokumen
4. E-mail
5. Tulisan tangan
6. Password
7. Buku telepon
8. Pesan teks.
9. Pesan suara

Biasanya, dua jenis penyelidikan komputer forensik berlangsung. Yang pertama adalah dimana beberapa peristiwa telah terjadi, tapi identitas pelanggar tak dikenal (seperti, *malicious code attack*, *hacking incident*, dan lain-lain). Yang kedua adalah dimana pelanggar dan peristiwa keduanya dikenal (seperti, penyelidikan kasus porno anak-anak). Dilengkapi dengan pengetahuan dari keadaan yang menyangkut suatu peristiwa, analis dan pemeriksa yang forensik dapat berproses ke arah yang memenuhi sasaran hasil berikut :

1. Lipatan Informasi tentang individu yang dilibatkan { siapa }.
2. Menentukan kealamian dari suatu peristiwa yang terjadi { apa }.
3. Membangun suatu timeline peristiwa { kapan }.
4. Menemukan tool apa atau exploits yang digunakan { bagaimana }.
5. Membongkar informasi yang menjelaskan motivasi untuk keadaan serangan { mengapa }.

Tabel 9.3 di bawah menyediakan suatu referensi silang dari sumber bukti umum yang ditemukan pada PDA dan kontribusi mereka kearah pemuasan dari penilaian objektif diatas. Kebanyakan dari sumber informasi datang dari data PIM, dan Internet yang dihubungkan oleh informasi. Aplikasi pendukung lain yang berjalan pada *device* yang berpotensi menyediakan sumber bukti lain. File pemakai ditempatkan pada alat untuk terjemahan, pengamatan, atau editing adalah juga sumber bukti penting yang lain. Di samping file grafis, isi file relevan lain meliputi *spreadsheet*, *presentation slides*, dan materi serupa. Karena *hybrid device*, seperti telepon PDA atau GPS PDA, sumber bukti tambahan ada, sebagai contoh, nomor jumlah diputar terakhir atau mengkoordinir kepada beberapa tujuan.

	Who	What	Where	When	Why	How
Owner Info	X					
Contacts	X				X	X
Calendar	X	X	X	X	X	X
To Do List	X	X	X	X		X
E-mail Contact	X	X	X	X	X	X
Web URLs/Content		X	X	X		X
Graphic Files	X	X				
Other File Content		X	X	X	X	X

Tabel 9.3 referensi silang dari sumber bukti umum

Pengetahuan dan pengalaman dengan berbagai *tools* untuk memperoleh dan menguji isi PDA sangatlah berharga. Sebagai contoh, satu *device* dapat melaksanakan *area inspecific* lebih baik daripada yang lain seperti identifikasi file atau fasilitas pencarian, *tools* dapat melaporkan, memperoleh, dan menguji isi dari data yang diperoleh dengan cara yang berbeda dan beberapa *tools* mungkin adalah platform spesifik. Oleh karena itu, menggunakan *toolkit* menawarkan ciri yang terbaik untuk *recovering* dan meneliti bukti dari suatu *device* spesifik yang menguntungkan.

9.7.2 Penggunaan Tool

Ketika gambaran yang diperoleh telah dicopy, langkah yang berikutnya akan mulai fengan mencari data, menciptakan *bookmarks*, dan mengembangkan muatan dari suatu laporan akhir. *Tool* pengujian forensik adalah komponen rumit didalam proses ketika mereka menterjemahkan data dari gambaran bit mentah ke suatu struktur dan format yang dapat dimengerti oleh pemeriksa dan dapat secara efektif digunakan untuk mengidentifikasi dan memulihkan bukti. Penting untuk mencatat bahwa *tools* mempunyai kemungkinan untuk berisi beberapa derajat tingkat kesalahan. Sebagai contoh, implementasi dari *device* mungkin punya suatu kesalahan dalam programming. Spesifikasi dari suatu struktur file yang digunakan oleh *device* untuk menterjemahkan data dirusak sehingga dapat dimengerti oleh pemeriksa yang mungkin ketinggalan zaman atau tidak akurat, atau struktur file yang dihasilkan oleh program yang lain sebagai masukan mungkin salah, menyebabkan *device* berfungsi dengan tidak sesuai. Oleh karena itu, mempunyai suatu derajat tinggi pemahaman dan kepercayaan menyangkut kemampuan *device* untuk melaksanakan fungsi pentingnya dengan baik. Sebagai tambahan, orang yang dicurigai banyak mengetahui informasi dapat merusakkan informasi *device*, seperti penuh arti salah memanggil nama suatu perluasan file

untuk mengagalkan keaktifan dari suatu *device* atau menerapkan suatu *device* yang menyeka untuk memindahkan atau menghapuskan data. Dari waktu ke waktu, percobaan dengan suatu *device* menyediakan suatu pemahaman tentang pembatasannya, membiarkan pemeriksa untuk meratakan mereka dan menghindari kesalahan.

Pengujian Forensik dari Bukti Digital - Suatu Panduan untuk Pelaksanaan hukum, yang diproduksi oleh itu Departemen Keadilan U.S., menawarkan usul berikut untuk analisa ttg data yang disadap [5]:

1. **Analisa Timeframe** - Menentukan apabila terjadi peristiwa pada sistem yang berhubungan dengan pemakaian secara perorangan dengan meninjau ulang log manapun yang ada sekarang dan hari dan tanggal yang tercatat didalam *filesystem*, seperti waktu dimodifikasi terakhir.
2. **Data hiding analysis** (Data yang menyembunyikan analisa) - Mendeteksi dan pemulihan menyembunyikan data yang dapat menandai adanya pengetahuan, kepemilikan, atau tujuan dengan menghubungkan keterhubungan file untuk perluasan file untuk menunjukkan *obfuscation* yang disengaja, perolehan akses ke *password-protected*, *encrypted*, dan pemartisian file, perolehan akses ke informasi *steganographic* dideteksi didalam gambaran dan memperoleh akses untuk memesan area penyimpanan data diluar *filesystem* normal tersebut .
3. **Application and file analysis** (Aplikasi dan analisa file) - Mengidentifikasi informasi relevan kepada penyelidikan dengan pengujian isi file, menghubungkan file untuk menginstall aplikasi, mengidentifikasi hubungan antar file (seperti, file e-mail ke pemasangan e-mail), menentukan arti dari file yang tak dikenal tipenya, menguji bentuk wujud sistem yang ditentukan, dan menguji file metadata (seperti, dokumen yang berisi identifikasi kebebasan).
4. **Ownership and possession** (pemilikan dan Kepemilikan) - Mengidentifikasi individu yang menciptakan, memodifikasi, atau mengakses suatu file dan pemilikan dan kepemilikan dari data ditanyakan dengan penempatan pokok materi dengan *devices* pada situasi tertentu dan menanggalnya, menempatkan minat file bukan melalui penempatan, menyembuhkan kata sandi yang menandai adanya kepemilikan atau pemilikan, dan muatan file yang mengidentifikasi yang dikhususkan untuk seorang pemakai.

Kemampuan dari *tool*, kesempurnaan ciri, dan sistem operasi itu (seperti, Windows CE, Palm OS, Linux) dan jenis *device* di bawah pengujian menentukan informasi apa yang dapat ditemukan, disembuhkan, dan dilaporkan, dan jumlah usaha yang diperlukan. Area variabilitas meliputi kesembuhan dan pencarian tentang informasi yang dihapus, informasi pada *device* dipasang lagi, atau informasi didalam arsip file bersejarah dimampatkan dengan salah perluasan yang dipanggil namanya [2]. Sebagai contoh, beberapa *tools* yang digunakan untuk mencari-cari bukti yang dapat mengidentifikasi file dengan perluasan file di mana orang lain menggunakan suatu file database tandatangan. Ciri selanjutnya adalah lebih baik menghapuskan kemungkinan data penutup berdasar pada suatu perluasan file yang tidak tetap. Ini terutama benar untuk berbagai jenis file grafik, oleh karena seluruh yang mereka alami biasanya adalah *shrouded* dari pencarian textual.

Mesin pencarian bermain dalam suatu peran penting didalam penemuan informasi yang digunakan untuk menciptakan suatu *bookmarks* dan laporan akhir. Pencarian data untuk hal positif menghasilkan bukti bersifat menuduh mengambil kesabaran dan dapat menjadi waktu pemakaian. Beberapa *tools* mempunyai suatu mesin pencarian sederhana yang persisnya menandingi suatu teks masukan string, membiarkan hanya untuk dilakukan pencarian dasar. *Tools* rumah lain yang lebih cerdas dan memperlihatkan mesin pencarian yang kaya, mempertimbangkan jenis mencari *grep* (pola teladan ungkapan reguler yang disamaratakan), mencakup *wildcard*, penyaringan file dengan perluasan, direktori, dan lain-lain dan catatan *batch* yang mencari-cari jenis isi spesifik (yaitu, alamat e-mail, URL, dan lain-lain). Dengan cara yang sama, kemampuan untuk menemukan dan mengumpulkan gambaran yang secara otomatis kedalam suatu fasilitas perpustakaan grafik umum dapat berbeda antar *tools*. Semakin besar kemampuan alat, semakin pengalaman dengan dan pengetahuan dari *devices* menjadi berharga untuk pemeriksa forensik itu.

Untuk membongkar bukti, spesialis pertama harus melawan latar belakang menyangkut orang yang dicurigai dan keadaan serangan dan menentukan satu set terminologi untuk pengujian itu. Ungkapan pencarian harus dikembangkan didalam suatu pertunjukan sistematis, seperti penggunaan nama kontak yang relevan. Dengan ini, spesialis menciptakan suatu profil untuk potensi penemuan yang berharga yang tidak akan menyelimuti penemuan. Untuk menghapuskan semua kemungkinan penghilangan bukti berharga, data harus secara menyeluruh diperiksa dari permulaan untuk berakhir dengan suatu jendela memori yang disajikan oleh *tool* yang baik maupun *hex editor*. Spesialis perlu mempunyai suatu

tandatangan file database untuk menempatkan *header* dan *footers* file spesifik yang dapat mendorong kearah bukti lebih lanjut, seperti: file grafik, avi file, dan lain-lain.

Sekali ketika data telah secara menyeluruh dicari dan materi relevan di *bookmark*, adalah waktunya untuk menciptakan suatu laporan. Banyak aplikasi forensik datang dengan suatu *built-in* yang melaporkan fasilitas yang mengimport data yang *dibookmark*, membiarkan spesialis untuk mengorganisir laporan, memilih modenya, dan aspek yang lain menyangkut laporan tersebut. Laporan dapat meliputi hal yang berikut: Nama Spesialis, Nomor Jumlah Kasus, Tanggal, Judul, Nama Orang yang dicurigai, Kategori bukti, dan relevansi bukti yang ditemukan. Laporan *software-generated* hanya suatu bagian kecil dari keseluruhan laporan akhir. Laporan akhir berisi laporan yang *software-generated* sepanjang dokumentasi yang dikumpulkan sepanjang keseluruhan siklus, yang meringkas tindakan dari pengujian forensik dan banyak hadiah dari hasil analisa, mencakup membongkar bukti manapun.

Ukuran-Ukuran berikut telah diusulkan sebagai pokok satuan kebutuhan untuk forensik *tool*, dan harus dipertimbangkan apabila suatu pilihan *tool* tersedia:

1. **Usability** (Usabilas) - kemampuan untuk menyajikan data didalam suatu format yang adalah berguna bagi suatu penyelidik.
2. **Comprehensive** (Menyeluruh) - kemampuan untuk menyajikan semua data kepada suatu penyelidik sedemikian sehingga bukti keduanya *inculpatory* dan *exculpatory* dapat dikenali.
3. **Deterministic** - kemampuan *tool* untuk menghasilkan keluaran yang sama apabila diberi satuan instruksi dan data masukan yang sama.
4. **Verifiable** - kemampuan untuk memastikan ketelitian menyangkut keluaran dengan mempunyai akses ke hasil presentasi dan terjemahan intermediate.

Faktor lain didalam memilih perangkat lunak antar *tool* meliputi pertimbangan Daubert:

1. **Quality** (Mutu) - pendukung teknis, keandalan, dan meningkatkan mutu alur versi.
2. **Capability** (Kemampuan) – didukung ciri set, performance, dan kesempurnaan mengenai cirri fleksibilitas dan customisasi.
3. **Affordability** (Affordabilas) - manfaat berharga melawan produktivitas didalam.

9.8 Reporting (Pelaporan)

Pelaporan adalah proses dalam menyiapkan suatu ringkasan terperinci dari semua langkah yang diambil dan kesimpulan yang dicapai didalam penyelidikan dari suatu kasus. Pelaporan tergantung pada semua peserta yang secara hati-hati memelihara suatu catatan dari pengamatan dan tindakan mereka, melaporkan hasil test, dan menjelaskan kesimpulan menarik dari bukti itu. Basis dari suatu laporan yang baik adalah dokumentasi padat, catatan, sket, foto, dan laporan *tool-generated*.

Hasil pelaporan dari suatu pengujian forensik cenderung untuk mengikuti *templates* yang sudah dikenal, *customized* diperlukan oleh keadaan yang spesifik dari tiap penyelidikan. Laporan dari hasil pengujian forensik meliputi semua informasi diperlukan untuk mengidentifikasi kasus dan sumbernya, menguraikan secara singkat hasil percobaan dan penemuan, dan membawa tandatangan dari individu yang bertanggung jawab untuk isinya. Secara umum, laporan dapat meliputi informasi yang berikut [5]:

1. Identitas menyangkut pelaporan agen
2. identifier Kasus atau nomor submission
3. Penyelidik kasus
4. Identitas menyangkut submitter
5. Tanggal tanda terima
6. Tanggal laporan
7. Daftar deskriptif materi yang disampaikan untuk pengujian, mencakup nomor urut, buatan, dan model
8. tandatangan dan Identitas menyangkut pemeriksa
9. Peralatan dan yang disediakan digunakan didalam pengujian
10. Meringkas uraian langkah-langkah yang diambil selama pengujian, seperti pencarian string, pencarian gambaran grafik, dan file penyembuhan dihapus.
11. Pendukung material seperti hasil print computer ttg materi bukti tertentu, salinan bukti digital, dan rantai penjagaan dokumentasi
12. Rincian penemuan:
 - a. File spesifik yang berhubungan dengan permintaan
 - b. File lain, termasuk menghapus file, yang mendukung penemuan
 - c. Pencarian string, kata kunci pencarian, dan teks mencari string

- d. Bukti *Internet-related*, seperti lalu lintas Analisa lokasi jaringan, *chat logs*, *cache files*, e-mail, dan *news group activity*
- e. Analisa gambaran grafis
- f. Indikator kepemilikan, yang mana bisa meliputi data pendaftaran program
- g. Data analysis
- h. Uraian relevan program pada materi yang diuji
- i. Teknik digunakan untuk besembunyi atau menyembunyikan data, seperti encryption, steganography, atribut yang tersembunyi, sekat yang tersembunyi, dan file menyebut keganjilan

13. Laporan Kesimpulan

Banyak perangkat lunak aplikasi forensik mempunyai fasilitas laporan built-in. Pemeriksa hanya perlu meliputi penemuan yang relevan didalam laporan untuk memperkecil kebingungan dan ukuran dari diantara mereka yang meninjau ulang. Laporan yang diotomatkan secara khas berisi komponen kunci berikut : Nomor Jumlah Kasus, Tanggal/Date, *Examiner Name*, Nama Orang yang dicurigai, dan *Files Acquired* (mempertunjukkan hash, data ASCII, penyajian data grafis, dan lain-lain.).

Bukti digital, seperti halnya *tools*, metodologi dan teknik yang digunakan didalam suatu pengujian, sebuah subjek yang sedang ditantang didalam suatu pengadilan atau prosedur formal lain. Kesesuaian dokumentasi adalah penting didalam penyediaan kemampuan individu untuk menciptakan kembali proses dari permulaan untuk mengakhiri. Sebagai bagian dari proses pelaporan, membuat suatu salinan perangkat lunak yang digunakan dan mencakupnya dengan keluaran diproduksi yang sebaiknya. Hal Ini bersangkutan untuk kebiasaan *tools*, karena kebingungan tentang versi dari perangkat lunak yang digunakan untuk menciptakan keluaran dihapuskan, seharusnya hal itu dijadikan diperlukan untuk reproduksi pengolahan forensik yang menghasilkan pada suatu waktu kemudiannya. Praktek yang sama berlaku bagi perangkat lunak *tools* komersil, yang mana bisa diupgrade setelah suatu pengujian diselesaikan.

9.9 Ringkasan pada PDA Seizure

PDA Seizure mempunyai kemampuan untuk memperoleh informasi baik dari *platform* Pocket PC ataupun Palm OS. Dengan mengabaikan jenis PDA yang ada, langkah-

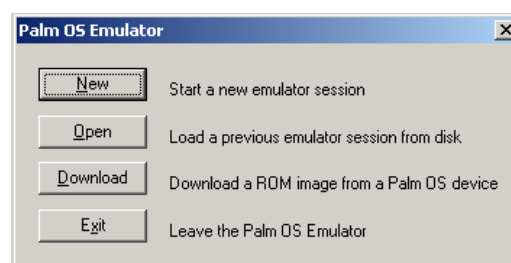
langkah investigasi yang sesuai harus diikuti untuk masing-masing *device*. PDA Seizure memungkinkan pemeriksa untuk menghubungkan alat via USB atau melalui koneksi serial. Pemeriksa harus mempunyai kabel yang benar dan *cradle* untuk memastikan terjadinya koneksi, sinkronisasi perangkat lunak dapat dipertukarkan, dan sumber *backup* batereipun tersedia. Sinkronisasi perangkat lunak memungkinkan pemeriksa menciptakan suatu pertemuan antara suatu PC atau *notebook* dengan *device* atau PDA yang sedang diselidiki (seperti perangkat lunak Microsoft ActiveSync atau Palm HotSync).

Sepanjang prosedur instalasi PDA Seizure, Emulator Palm OS (POSE) juga diinstall pada PC atau notebook tersebut. POSE digunakan untuk melihat data yang dihubungkan dengan Palm *device* dalam lingkungan *desktop*. Data yang diperoleh akan sama persis ketika akan digunakan pada *device* dengan penggunaan sebuah virtual PDA. Penggunaan POSE memungkinkan seseorang untuk melihat data yang tidak didukung oleh *internal viewer* PDA Seizure. Langkah-Langkah berikut menguraikan secara singkat tindakan yang diambil menggunakan POSE dengan PDA Seizure.

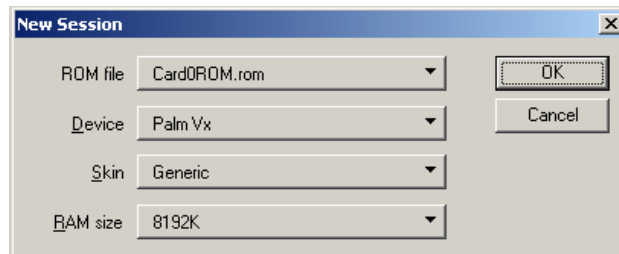
1. Install POSE - Hal ini dilaksanakan sepanjang instalasi PDA Seizure.
2. Memperoleh bukti dari *device*.
3. Dari Menu Bar PDA Seizure pilih : Tools -> Export Semua File.
4. Pengeksporan Semua file menciptakan dua subfolders: Card0-RAM dan Card0-ROM.

Sebagai ganti *download* suatu gambaran ROM yang perlu, pemeriksa dapat menggunakan ROM yang diperoleh untuk kemungkinan dalam meng upgrade ROM.

1. Start POSE: Tools -> Palm Emulator
2. Select New -> Star a new emulator session
3. Select the ROM file -> Other -> Pilih gambaran ROM yang disimpan ke folder Card0-ROM



Gambar 9.3 Pose - Start Emulator



Gambar 9.4 POSE - Select ROM atau Device

Ketika file ROM dipilih, sesi POSE akan dimulai. Untuk melihat file spesifik dalam sesi POSE, *drag* dan *drop* tipe file khusus yang sederhana: PRC, PDB, PQA, dan file PSF ke layar emulator POSE dari folder yang dieksport tersebut. *Screen shot* dibawah adalah contoh dari POSE yang kelihatan seperti setelah mengirim ROM atau RAM dari *device* yang diperoleh. POSE bermanfaat untuk menyediakan aksi yang sebenarnya dan menangkap *screen shots* informasi yang relevan seperti yang ditunjukkan didalam Gambar 9.5 di bawah.

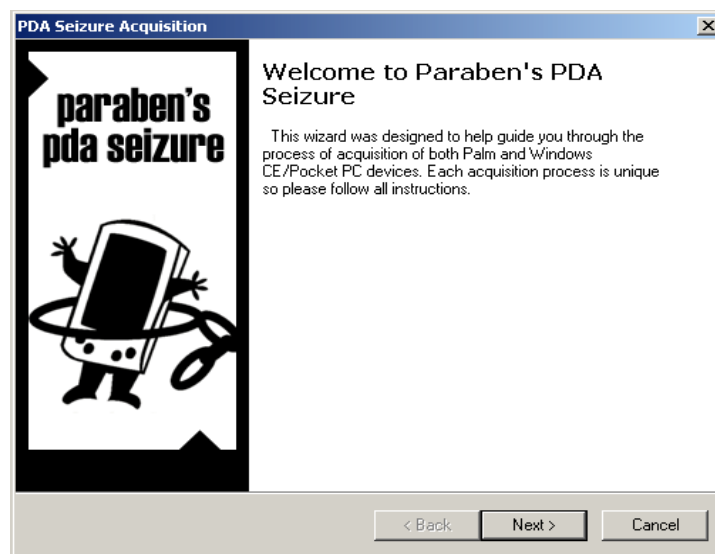


Gambar 9.5 Emulator POSE

POSE bukanlah suatu aplikasi kepemilikan yang dihubungkan dengan PDA Seizure dan dapat *download* secara terpisah serta digunakan pada aplikasi orensic lain yang mempunyai kemampuan untuk memperoleh suatu gambaran ROM dan file database yang dihubungkan.

9.9.1 Langkah Acquisition

Ada dua metoda untuk memulai pengadaan data dari PDA *device*. *Acquisition* dapat ditetapkan melalui *toolbar* dengan menggunakan icon *Acquire* atau melalui *tools* serta pemilihan *Acquire Image*, Pilih start proses *Acquisition* yang manapun. Dengan proses *Acquisition*, gambaran memori dan file keduanya dapat diperoleh. *Device* akan menandai kedua jenis data yang diperoleh. Ketika proses *Acquisition* terpilih, ahli *Acquisition* digambarkan dibawah dalam Gambar 9.6 terlihat panduan pemeriksa untuk melalui proses tersebut.



Gambar 9.6 Acquisition Wizard

Gambar 9.7 di bawah berisi suatu contoh *screen shot* PDA Seizure sepanjang pengadaan suatu Pocket PC (PPC) *device*, mempertunjukkan berbagai bidang yang disajikan oleh *interface*.

File Path	File Name	Type	Create Date	Modify Date	Attr	Size	Status	MD5 Hash
	Registry					221,324	Acquired	8C3B2C3C3D6924743AFF7478EF1BF8C4
	MemImage					93,266,672	Acquired	676B2351D31CF0B44D793D10080CE3D2
(Storage Card)	ignore_my_docs		2003/07/03 01:23:48	2003/07/03 01:18:34	A	0	Acquired	
(Storage Card)	f1.png	.png	2003/07/03 01:24:06	2003/07/03 01:18:34	A	4,545	Acquired	591755C36ACB2AA60AF0FD0B6A4A2A758
(PAQ File Store)	BioSwipe.cpl	.cpl	2003/06/18 07:03:19	2003/07/02 04:35:50	A	2,212	Acquired	91684FCCA3A983C7E1FFBF5F7A525
(PAQ File Store)	ignore_my_docs		2003/06/18 07:03:19	2003/06/18 07:03:19	HA	0	Acquired	
(PAQ File Store)(Compaq)(Nervo)(UserData)	3081.dat	.dat	2003/06/19 01:37:36	2003/06/19 01:37:36	A	1	Acquired	938885ADF00DA089CD634904FD59F71
(PAQ File Store)(Compaq)(Nervo)(UserData)	C05B.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	938885ADF00DA089CD634904FD59F71
(PAQ File Store)(Compaq)(Nervo)(UserData)	6738.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	938885ADF00DA089CD634904FD59F71
(PAQ File Store)(Compaq)(Nervo)(UserData)	4F2C.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	938885ADF00DA089CD634904FD59F71
(PAQ File Store)(Compaq)(Nervo)(UserData)	9E4A.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:37	A	1	Acquired	938885ADF00DA089CD634904FD59F71
(PAQ File Store)(Compaq)(Nervo)(UserData)	Room1.dat	.dat	2003/06/19 01:37:37	2003/06/19 01:37:38	A	540	Acquired	E5C79F3715E93223341B5F52E9A9D1E7
(PAQ File Store)(Compaq)(Nervo)(UserData)	User1.dat	.dat	2003/06/19 01:37:38	2003/06/19 01:37:38	A	72	Acquired	F55948DCC7FF23F25F3002DFA82C08
	mdmlog10.txt	.txt	2003/07/03 03:24:03	2003/07/03 03:24:03	A	54	Acquired	0CA8F822045340EC9F333843DC1D8E6
	GCounterFile.mmf	.mmf	2003/07/03 01:24:40	2003/07/03 01:24:40	HA	10,500	Acquired	98E85D1AF9558CDBEDF4F34C39526BDF
	CIMMapP		2002/06/27 21:00:01	2002/06/27 21:00:01	HA	56	Acquired	BFAC405E80E839787565F92779FC734
	CIMMapG		2002/06/27 21:00:01	2002/06/27 21:00:01	HA	60	Acquired	619E024E9D05CB2A582382E6A7ED600AF
(Program Files)(PHM Tools)	regedit.exe	.exe	2002/11/11 14:58:20	2002/11/11 14:58:20	A	68,608	Acquired	6ED34635F865952A60BCEB8A2F9DC9
(Program Files)	PAQ Image Viewer .hik	.hik	2002/06/27 12:59:50	2002/06/27 12:59:50	A	24	Acquired	33D68F9142A682324CF2714F44778748
(Program Files)(Windows Media Player)	Welcome To Window .vma	.vma	2002/06/27 12:59:50	2002/06/27 12:59:50	A	24	Acquired	818AA698990437EA2178931561C3CA45
(Program Files)(Windows Media Player)	default.skin	.skin	2002/06/27 12:59:50	2002/06/27 12:59:50	A	28	Acquired	6ED00F8218AA666B9727E12C8C8451C9
(My Documents)	f3.png	.png	2003/07/03 01:18:34	2003/07/03 01:18:34	A	4,685	Acquired	78810A8FAC1CE1004D6723F49FC1D1A
(My Documents)	f1.png	.png	2003/07/03 01:18:34	2003/07/03 01:18:34	A	4,545	Acquired	591755C36ACB2AA60AF0FD0B6A4A2A758
(My Documents)	Recording1.wav	.wav	2003/06/18 07:03:18	2003/06/18 07:03:18	A	2,868	Acquired	C3CDF42E1FB0A8B210B74D2D649A7FA0
(My Documents)(Business)	IX.psw	.psw	2003/06/18 07:05:21	2003/06/18 07:05:21	A	8,880	Acquired	D874B0373DE58297C01BA2CF86F4840
(My Documents)(Templates)	Vehicle Mileage Log... .prx	.prx	2002/06/27 12:59:50	2002/06/27 12:59:50	HRA	7,498	Acquired	9C91B6EF8134B471A13300CB64F87134

Gambar 9.7 Acquisition Screen Shot (PPC)

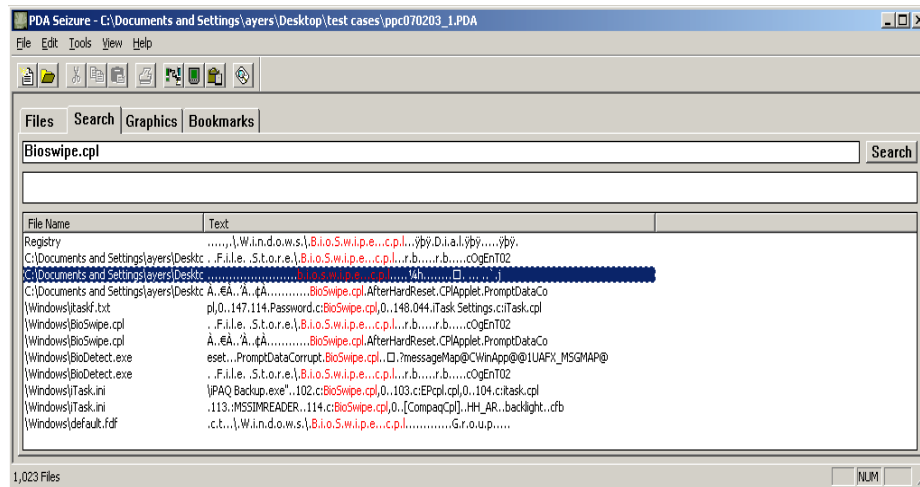
Setelah PPC *acquisition*, PDA Seizure melaporkan masing-masing file individu : *File Path, File Name, File Type, Creation and Modification Dates, File Attributes, File Size, Status, and an MD5 File Hash*. Validasi dari *file hash* yang diambil sebelum dan setelah *acquisition* dapat digunakan untuk menentukan apakah file telah dimodifikasi sepanjang langkah *acquisition*.

Sepanjang proses *acquisition*, **CESeizure.dll** dieksekusi untuk memperoleh daerah memori yang tidak teralokasi. Pemeriksa dibisikkan kotak cek untuk memilih satu atau semua sebelum memperoleh informasi pada PPC *device* berikut : *Acquire Files, Acquire Databases, Acquire Registry, dan atau Acquire Memory*. Masing-Masing file yang diperoleh dapat dipandang dalam teks atau *hex mode* manapun, tergantung pemeriksa memeriksa isi dari semua file yang ada. Dalam rangka melihat file, pemeriksa harus menggunakan salah satu dari pilihan berikut : mengeksport file, meluncurkan suatu aplikasi berdasarkan pada aplikasi yang berjalan atau karena *Palm device* melihat keseluruhan dari POSE.

9.9.2 Fungsi Pencarian

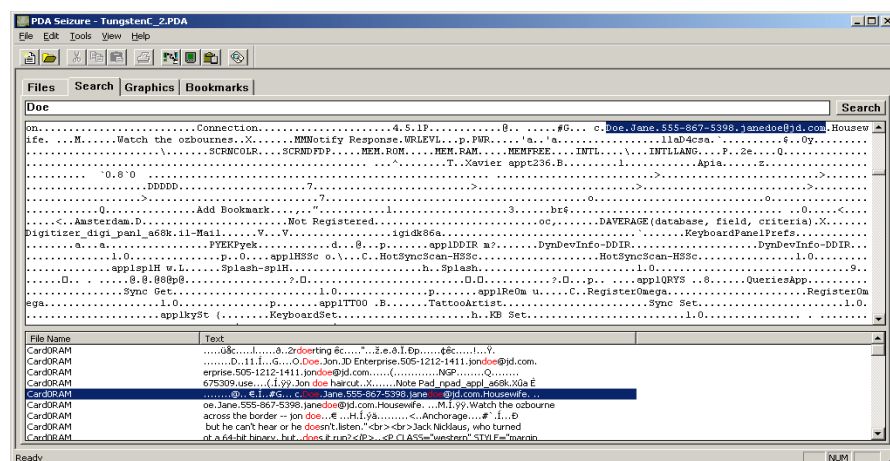
Fasilitas pencarian pada PDA Seizure mengijinkan pemeriksa melakukan query pada isi file. Fungsi pencarian akan mencari isi file dan melaporkan semua kejadian dari string yang ditemukan. *Screenshot* yang ditunjukkan dalam Gambar 3.8 menggambarkan suatu contoh menyangkut hasil yang diproduksi untuk string “Bioswipe.cpl”. Bukan karakter *wildcard*,

seperti tanda asterisk nampak didukung atau fasilitas untuk pengujian suatu subset yang menyangkut file dengan direktori, tipe file, atau nama file.



Gambar 9.8 File Content String Search (PPC)

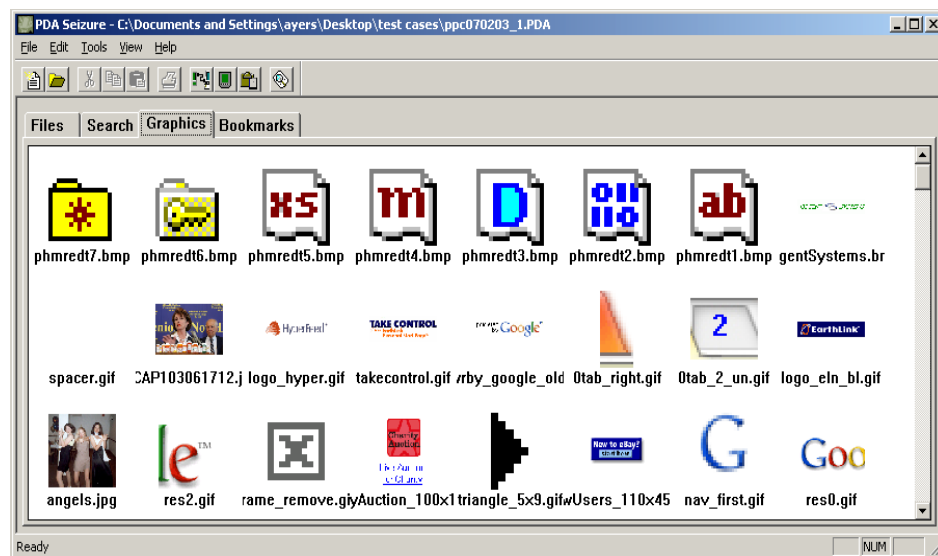
Jendela pencarian menyediakan suatu keluaran memori yang berhubungan dengan pencarian string yang disajikan oleh pemeriksa. Hal ini akan memungkinkan pemeriksa melalui sebagian petunjuk memori dan informasi *bookmark* yang berharga untuk pelaporan yang digunakan dalam hal pengadilan yang teratur atau untuk cara kerja lain. Gambar 3.9 menggambarkan suatu kutipan dari suatu pencarian string dengan nama "Doe" dan isi dapat dilihat pada jendela memori.



Gambar 9.9 Memory Content String Search (PPC)

9.9.3 Graphics Library

Perpustakaan grafik memungkinkan pemeriksa untuk menguji koleksi file grafik yang terlihat pada *device* yang dikenali dalam *file extension*. File grafik yang dihapus tidak nampak dalam perpustakaan tersebut. Suatu peningkatan penting perpustakaan grafik adalah mengidentifikasi dan meliputi yang didasarkan pada file grafik, tandatangan file (yaitu, nilai header dan footer yang diketahui) melawan *file extension*. melakukan identifikasi file dengan tandatangan akan sangat memakan waktu dan dapat menyebabkan data kunci hilang. Jika ada file grafik yang dihapus, mereka harus dikenali melalui memori windows dengan melakukan suatu pencarian string untuk mengidentifikasi sisa-sisa file. Bagaimanapun, kesembuhan keseluruhan gambaran akan menjadi sulit karena isinya mungkin dimampatkan oleh *filesystem* atau tidak boleh berada pada memori yang berdekatan, dan beberapa bagian mungkin tidak bisa dipulihkan. Hal ini juga memerlukan pengetahuan mengenai struktur data yang dihubungkan untuk menambah komponen bersama dengan baik. Gambar 9.10 menunjukkan suatu gambaran *screen shoot* yang diperoleh dari suatu Pocket PC 2002 *device*.

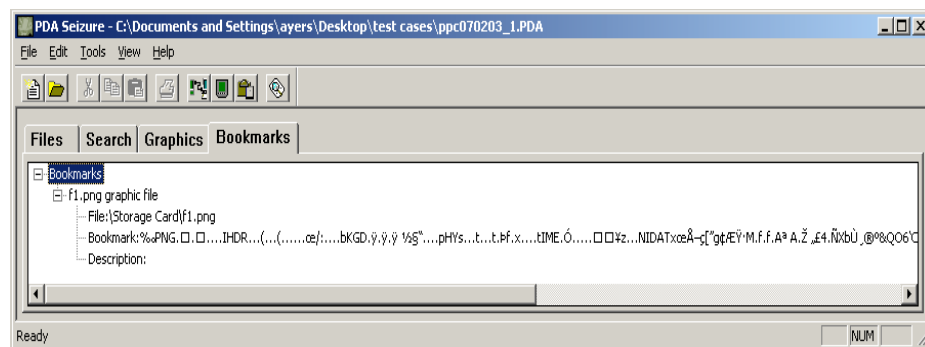


Gambar 9.10 Graphics Library (PPC)

9.9.4 Bookmarking

Selama suatu penyelidikan, pemeriksa forensik sering mempunyai gagasan untuk informasi di mana mereka sedang melihat berdasarkan keadaan dari informasi dan peristiwa yang telah diperoleh. Petunjuk *Bookmarking* mengijinkan pemeriksa forensik untuk menandai materi yang ditemukan menjadi relevan ke penyelidikan tersebut. Kemampuan seperti ini memberi pemeriksa *tools* untuk menghasilkan laporan spesifik kasus yang berisi informasi

penting yang ditemukan sepanjang pengujian dalam suatu format yang pantas untuk dipresentasikan. Petunjuk *Bookmarking* dapat ditambahkan untuk berbagai potongan informasi yang ditemukan dan masing-masing file individu dapat diekspor untuk analisa lebih lanjut jika perlu. Seperti yang digambarkan dalam Gambar 9.11 di bawah adalah suatu contoh menyangkut ciptaan suatu *Bookmarking* pada suatu file grafik yang ditemukan pada kartu *storage*. Seperti disebutkan lebih awal, file ditemukan dan *bookmark* diekspor ke PC dan dipandang dengan suatu aplikasi yang pantas untuk jenis file yang dipermasalahkan.

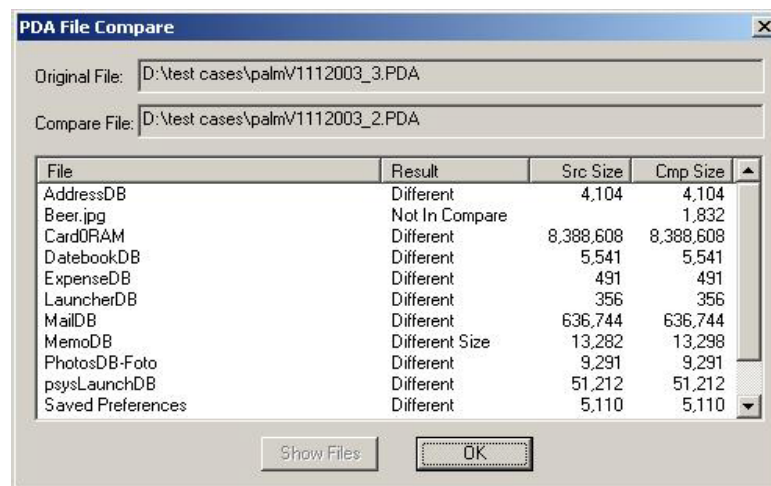


Gambar 9.11 Bookmark Creation (PPC)

9.9.5 Additional Tools

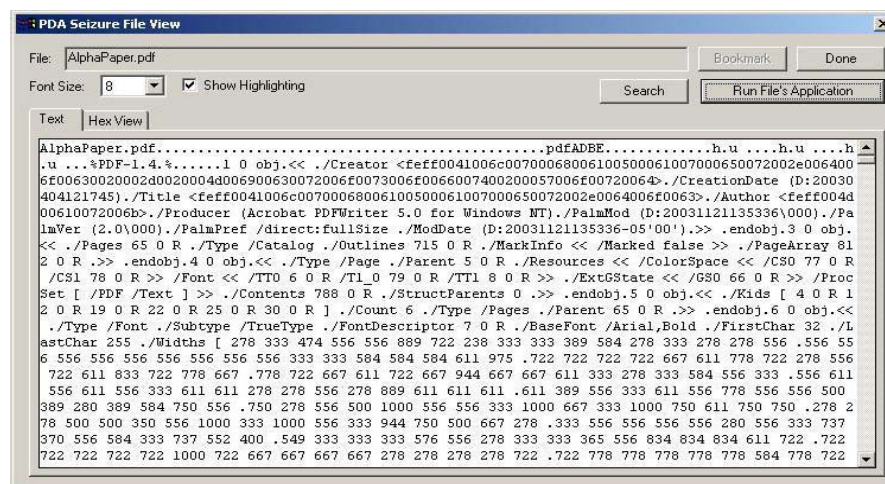
Export All Files : Pemeriksa mempunyai kemampuan untuk mengekspor semua file yang dilaporkan setelah langkah *aquisition* telah diselesaikan. Setelah file diekspor, sebuah folder diciptakan berdasarkan pada nama file kasus, dengan dua subfolder: masing-masing untuk RAM dan ROM. Tergantung atas jenis file, isi dapat dipandang dengan suatu aplikasi *desktop* yang dihubungkan dengan suatu alat emulator spesifik.

PDA File Compare : PDA Seizure mempunyai suatu fungsi built-in yang bandingkan dengan file *aquisition*. Untuk beroperasi, bandingkan corak satu file yang terisi ke dalam program, kemudian membandingkan melauai pilihan menu *tool* ke file yang lain . File dibandingkan dengan kode hash berdasarkan pada hasil yang ditunjukkan dalam suatu kotak dialog nama file, hasil dari perbandingan, dan ukuran pada setiap file .*pda*. *Double-Click* file, atau sorot file dan klik tombol "Show Files", pops-up *side-by-side* file *hex view* keduanya dengan perbedaan yang ditunjukkan dengan tanda merah. Perbandingan file PDA dapat digambarkan di bawah pada Gambar 9.12.



Gambar 9.12 PDA File Compare (Palm OS)

PDA Seizure File View : Yang digambarkan dalam Gambar 9.13 adalah contoh PDA Seizure File Viewer. File yang belum dihapus mempunyai pilihan untuk lihat dalam *hex* atau teks manapun, atau dengan fungsi "aplikasi yang berjalan", yang memanggil suatu aplikasi yang dihubungkan untuk memajukan data pada mesin lokal pemeriksa. Yang belakangan mengijinkan grafik dan file lain untuk diketik dalam format file ASCII yang standart untuk dilihat.



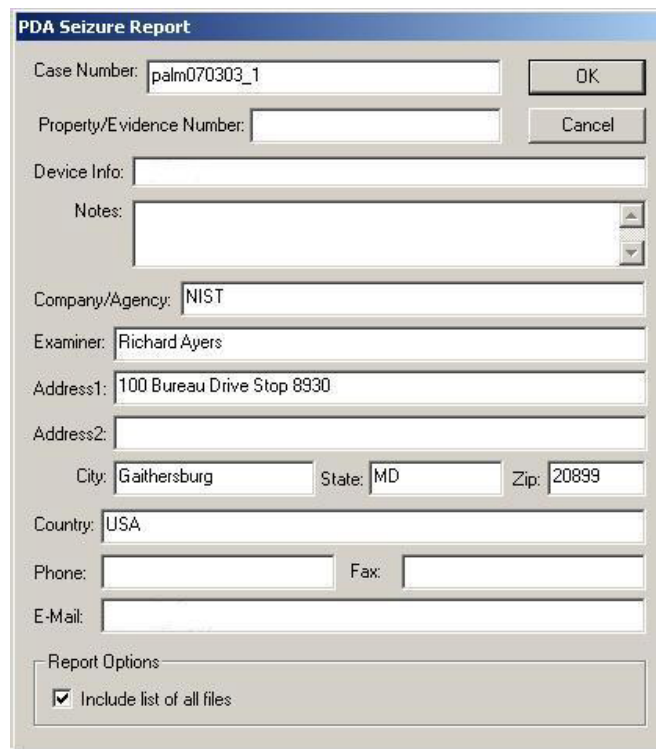
Gambar 9.13 File View (Palm OS)

9.9.6 Report Generation

Pelaporan adalah suatu tugas penting untuk pemeriksa. PDA Seizure menyediakan seorang *user interface* untuk *Report Generation* yang akan mengijinkan pemeriksa untuk masuk dan mengorganisir informasi spesifik dari suatu kasus. Masing-Masing kasus berisi

sejumlah identifikasi dan informasi lain yang dikhususkan untuk penyelidikan serta tujuan pelaporan, seperti digambarkan dalam Gambar 9.14 dibawah.

Ketika laporan telah dihasilkan dan menghasilkan menghasilkan sebuah file a.html untuk pemeriksa, termasuk file yang di *book-marked*, total file diperoleh, waktu *aquisition*, informasi alat, dan lain-lain. Jika file dimodifikasi sepanjang langkah *aquisition*, maka laporan akan mengidentifikasinya.



PDA Seizure Report

Case Number: palm070303_1 OK

Property/Evidence Number: Cancel

Device Info:

Notes:

Company/Agency: NIST

Examiner: Richard Ayers

Address1: 100 Bureau Drive Stop 8930

Address2:

City: Gaithersburg State: MD Zip: 20899

Country: USA

Phone: Fax:

E-Mail:

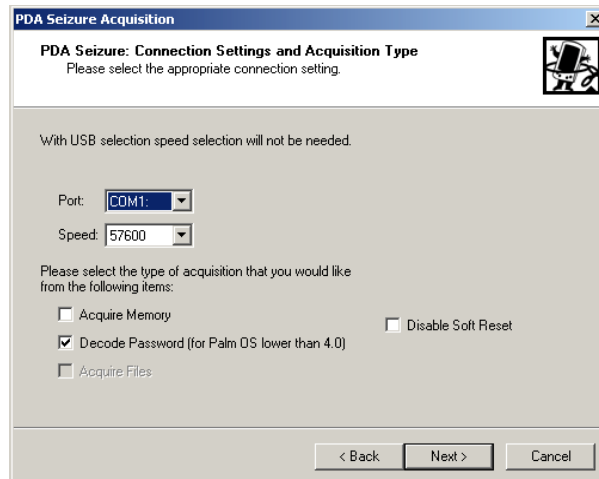
Report Options

☒ Include list of all files

Gambar 9.14 Report Generation

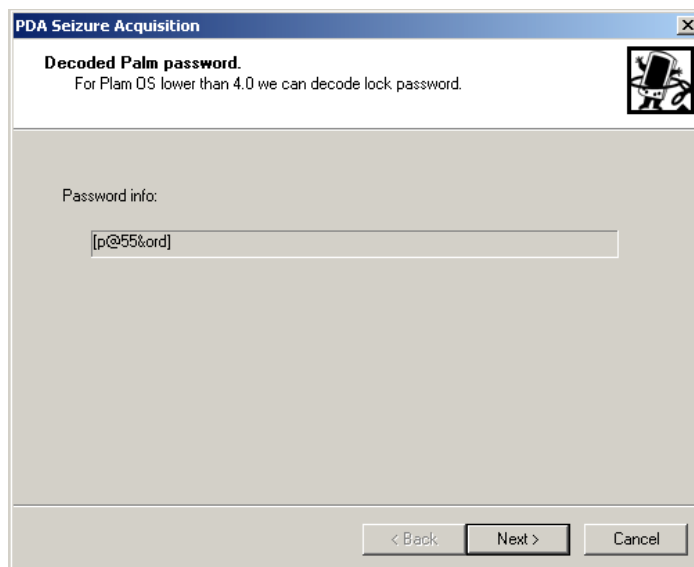
9.9.7 Password Cracking

PDA Seizure mempunyai kemampuan untuk meng*crack* kata sandi untuk Palm OS prior sebelum versi 4.0. Berkaitan dengan suatu rencana *password-encoding* yang dapat dibalik, adalah mungkin untuk memperoleh suatu format yang disandikan, menentukan kata sandi yang nyata, dan mengakses para pemakai data pribadi. *Password Cracking* untuk Windows CE tidak didukung. *Screenshots* yang digambarkan di bawah menguraikan secara singkat proses memperoleh *password* dari *device* yang dikunci. Langkah pertama akan dipilih adalah *Decode Password*.



Gambar 9.15 Password Crack Step 1 (Palm OS)

Ketika pemeriksa telah memilih *Decode Password*, langkah yang berikutnya akan meletakkan *device* kedalam *console mode*. Setelah alat didalam *console mode*, *password* akan ditunjukkan berdasarkan pada layar seperti digambarkan didalam Gambar 9.16, dengan membiarkan pemeriksa dengan kemampuan untuk membuka kunci alat dan mulai pengadaan informasi normal.



Gambar 9.16 Password Crack Step 2 (Palm OS)

DAFTAR PUSTAKA

1. Abdul Kadir dan Terra Ch. Triwahyuni, Pengenalan Teknologi Informasi, Andi, Yogyakarta, 2003.
2. Frank J.Defler, Jr, Panduan Menggabungkan LAN, PT.Elex Media Komputindo, Jakarta,1992.
3. Bukti Digital, Kunci Penguak Kejahatan Cyber
www.pcmedia.co.id
4. Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response
<http://csrc.nist.gov/publications/nistpubs/index.html>
5. Cybercrime and Intellectual Property
www.solusihukum.com
6. Seputar Cybercrime
<http://www.cybertech.cbn.net.id>
7. Cybercrime Act 2001
www.findlaw.com.au
8. Firewall Pada Linux
www.ristishop.com

Apendiks A

Akronim

API	– Application Programming Interface
ASCII	– American Standard Code for Information Interchange
CF	– Compact Flash
Codec	– Coder-Decoder
CIR	– Consumer Infrared
CRC	– Cyclical Redundancy Check
dd	– duplicate disk/data dump
DLL	– Dynamically Linked Library
GDI	– Graphics Device Interface
GPS	– Global Positioning System
GPRS	– General Packet Radio Service
GSM	– Global System for Mobile Communications
GWES	– Graphics, Windowing, and Events Subsystem
IDE	– Integrated Drive Electronics
IPsec	– Internet Protocol Security
IrDA	- Infra Red Data Association
JFFS2	– Journaling Flash File System, Version 2
JTAG	– Joint Test Action Group
LCD	– Liquid Crystal Display
LED	– Light Emitting Diode
MMC	– Multi-Media Card
OAL	– Original Equipment Manufacture Adaptation Layer
OEM	– Original Equipment Manufacture
OS	– Operating System
PC	– Personal Computer
PDA	– Personal Digital Assistant
pdd	– Palm data dump/duplicate disk
PFF	– Palm File Format
PIM	– Personal Information Management
PIN	– Personal Identification Number
POSE	– Palm Operating System Emulator
PPC	– Pocket PC
PPTP	– Point-to-Point Tunneling Protocol
RAM	– Random Access Memory
RAPI	– Remote Application Programming Interface
ROM	– Read Only Memory
SD	– Secure Digital
SHA1	– Secure Hash Algorithm, version 1
SSH	– Secure Shell
TCP/IP	– Transmission Control Protocol/Internet Protocol
TFT	– Thin Film Transistor
UART	– Universal Asynchronous Receiver/Transmitter
URL	– Uniform Resource Locator

USB	– Universal Serial Bus
WiFi	– Wireless Fidelity
WinCE	– Windows CE
XIP	– eXecute In Place

Apendiks B

Daftar Kata

Acquisition – Suatu proses yang akan menduplikasi, mengcopy atau menggambarkan bukti digital.

Analysis – Pengujian dari data yang diperoleh untuk nilai arti dan probative dari suatu kasus.

Authentication Mechanism – Perangkat keras atau mekanisme berbasis perangkat lunak yang memaksa para pemakai untuk membuktikan identitas mereka sebelum mengakses data pada suatu alat.

Bluetooth – Suatu protokol wireless yang mengijinkan dua alat Bluetooth untuk berkomunikasi dengan satu sama lain dalam suatu jarak pendek (misalnya, 30 meter).

Brute Force Password Attack – Suatu metode dalam mengakses suatu alat yang dihalangi melalui berbagai percobaan kombinasi dari kata sandi numeric atau alphanumeric.

Buffer Overflow Attack - Suatu metode pemuatan lebih sejumlah ruang dalam suatu buffer, yang dapat berpotensi overwrite dan memori corrupt dalam data.

Chain of Custody – Suatu proses yang menafsirkan pergerakan bukti melalui lifecycle pengumpulan, perlindungan, dan analisa dengan dokumen masing-masing orang yang menangani bukti, waktu atau hari proses dikumpulkan atau ditransfer, dan tujuan untuk perpindahan itu.

Compressed File – Suatu file yang dikurangi dalam ukuran melalui aplikasi dari tekanan algoritma, biasanya dilakukan untuk menyimpan ruang disk. Tindakan dalam memampatkan suatu file akan membuatnya tak terbaca ke kebanyakan program sampai file tidak dimampatkan. Kegunaan tekanan yang paling Umum adalah PKZIP dan Winzip dengan ekstensi .zip.

Cradle – Suatu stasiun yang memotong, yang menciptakan alat penghubung antara suatu PC pemakai dan PDA, dan memungkinkan baterai dan komunikasi di charge kembali.

Cyclical Redundancy Check – Suatu metode untuk memastikan data belum diubah setelah dikirim melalui suatu saluran komunikasi.

Deleted File – Suatu file yang telah secara logika, tetapi tidak harus secara fisik, dihapus dari sistem operasi, mungkin untuk menghapuskan bukti berpotensi bersifat menuduh. Penghapusan file tidak selalu perlu menghapuskan kemungkinan penyembuhan semua atau bagian dari data yang asli tersebut.

Digital Evidence – Informasi elektronik yang disimpan atau yang dipancarkan dalam format biner.

Duplicate Digital Evidence – Suatu salinan suatu reproduksi digital yang akurat dari semua object data yang diisi pada item fisik yang asli dan media yang dihubungkan

(seperti flash memory, RAM, ROM).

Electromagnetic Interference – Suatu gangguan electromagnetis yang menyela, menghalangi, atau jika tidak menurunkan pangkat atau membatasi capaian electronics/electrical peralatan yang efektif.

Electronic Evidence – Nilai informasi dan data investigasi yang disimpan atau yang dipancarkan oleh suatu alat elektronik.

Encryption – Prosedur manapun yang digunakan dalam ilmu membaca sandi untuk mengkonversi text datar ke dalam teks kode untuk mencegah seseorang tetapi penerima yang diharapkan dari pembacaan data itu.

Examination – Suatu tinjauan ulang teknis yang membuat bukti yang kelihatan dan pantas untuk dianalisis atau dites dilakukan pada bukti untuk menentukan ketidakhadiran atau kehadiran data spesifik.

Exculpatory Evidence – Bukti yang cenderung mengurangi kemungkinan kesalahan atau rasa bersalah.

eXecute in Place – Suatu fasilitas yang mengijinkan kode untuk dieksekusi secara langsung dari flash memory tanpa memuat kode ke dalam RAM.

File Name Anomaly – Suatu tidak sepadan antara file yang internal dan perluasan eksternal; suatu file yang bertentangan atau tidak tetap dengan isi dari file itu (misalnya, menamai ulang suatu grafik file dengan suatu file non grafik).

File Slack – Ruang antara akhir logis dari file dan akhir dari unit alokasi akhir untuk file itu.

Filesystem – Suatu mekanisme perangkat lunak yang menggambarkan cara file dinamai, disimpan, diorganisir, dan diakses pada volume yang logis dari memori yang dipartisi.

Flash ROM – memori non- volatile yang dapat ditulis.

Forensic Copy – Suatu reproduksi bit-for-bit yang akurat menyangkut informasi pada suatu alat elektronik atau media yang berhubungan, yang integritas dan kebenaran siapa telah dibuktikan dengan menggunakan suatu algoritma yang diterima.

Forensic Specialist – Menempatkan, mengidentifikasi, mengumpulkan, meneliti dan menguji data selagi memelihara pemeliharaan dan integritas suatu rantai penjagaan informasi tegas yang ditemukan.

Global Positioning System – Suatu sistem untuk menentukan posisi dengan membandingkan isyarat radio dari beberapa satelit.

Hardware Driver - Aplikasi yang bertanggung jawab untuk penetapan komunikasi antar perangkat keras dan perangkat lunak program.

Hashing – Proses penggunaan suatu algoritma mathematical melawan data untuk menghasilkan suatu nilai klasifikasi berupa contoh data tersebut.

Heap – Suatu struktur data perangkat lunak yang digunakan untuk alokasi memori

dinamis.

Image - Suatu salinan tepat bit-stream data elektronik pada suatu alat, yang dilakukan dalam suatu cara yang memastikan informasi tidak diubah.

Inculpatory Evidence - Bukti yang cenderung untuk meningkatkan kemungkinan rasa bersalah atau kesalahan.

Loop-Back Mode – Suatu sistem operasi fasilitas yang memungkinkan suatu alat untuk menjulang via suatu loopback menunjuk dan memandang secara logika pada PC itu.

Misnamed Files – Suatu teknik untuk menyembunyikan suatu isi file dengan mengubah nama file kepada sesuatu atau tidak bahaya mengubah perluasan nya kepada suatu jenis file berbeda, memaksa pemeriksa untuk mengidentifikasi file dengan tandatangani file melawan file perluasan.

Password Protected – Kemampuan untuk melindungi suatu file menggunakan akses kata sandi mengendalikan, melindungi isi data dari yang sedang dipandang dengan penonton yang sesuai kecuali jika kata sandi yang sesuai dimasukkan.

Personal Digital Assistant (PDA) – Suatu handheld komputer yang bertindak sebagai suatu alat untuk membaca dan menyampaikan dokumen, pos elektronik, dan media elektronik lain di atas suatu mata rantai komunikasi, dan untuk pengaturan informasi pribadi, seperti suatu name-and-address database, to-do list, dan appointment calendar.

Personal Information Management (PIM) Applications – Suatu inti satuan aplikasi yang menyediakan padanan yang elektronik dari suatu agenda, buku alamat, notepad, dan pemilik kartu bisnis.

Probative Data – Informasi yang mengungkapkan kebenaran dari suatu pernyataan tanpa bukti.

Steganography – Ilmu pengetahuan dan seni dalam berkomunikasi dengan cara yang menyembunyikan keberadaan komunikasi. Sebagai contoh, gambaran pornografi seorang anak dapat tersembunyi di dalam file gambaran grafis yang lain , file audio, atau format file lain.

Synchronization Protocols – Protokol yang memungkinkan para pemakai untuk memandang, memodifikasi, dan mentransfer/update data PDA dari PC atau sebaliknya. Dua protokol sinkronisasi yang paling umum adalah: Activesync Microsoft'S dan and Palm's HotSync.

Thread– Suatu kelompok instruksi yang digambarkan yang melaksanakan bagian pengujian dari kelompok yang digambarkan dengan cara yang sama lain, tetapi dengan sumber daya dan memori yang berbagi menyangkut proses dimana mereka menjadi anggota.

Universal Serial Bus (USB) – Suatu penghubung perangkat keras untuk peripheral berkecepatan rendah seperti keyboard, mouse, joystick, scanner, printer, dan telephony.

Volatile Memory – Memori yang kertas kehilangan isinya ketika listrik mati.

Write-Blocker – Suatu alat yang memungkinkan penyelidik untuk menguji media ketika mencegah data ditulis dari yang terjadi pada pokok materi media.

Write Protection – Metoda data pencegahan pada perangkat keras atau perangkat lunak yang sedang ditulis dalam suatu disk atau medium lain.