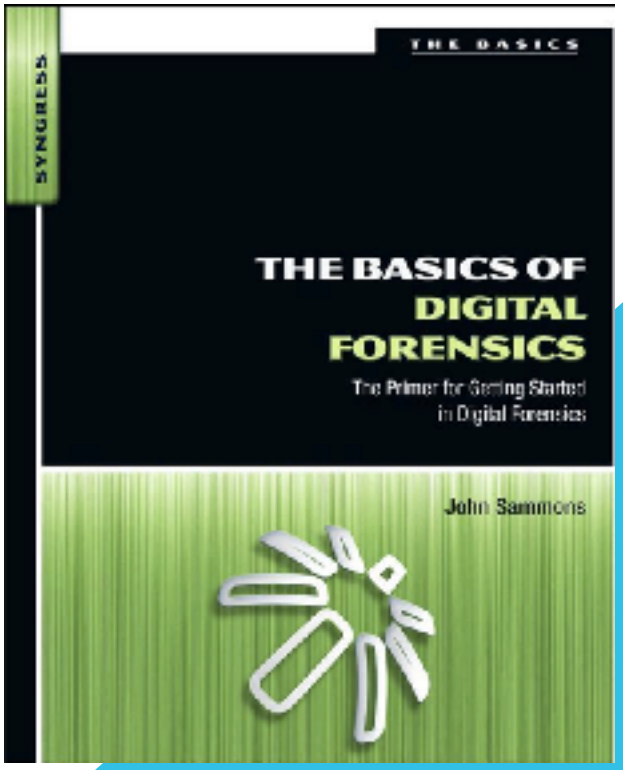


3. LABS DAN TOOLS

TOPICS

- Laboratorium Forensik
- Kebijakan dan Prosedur
- Quality Assurance
- Hardware dan Software
- Akreditasi vs. Sertifikasi

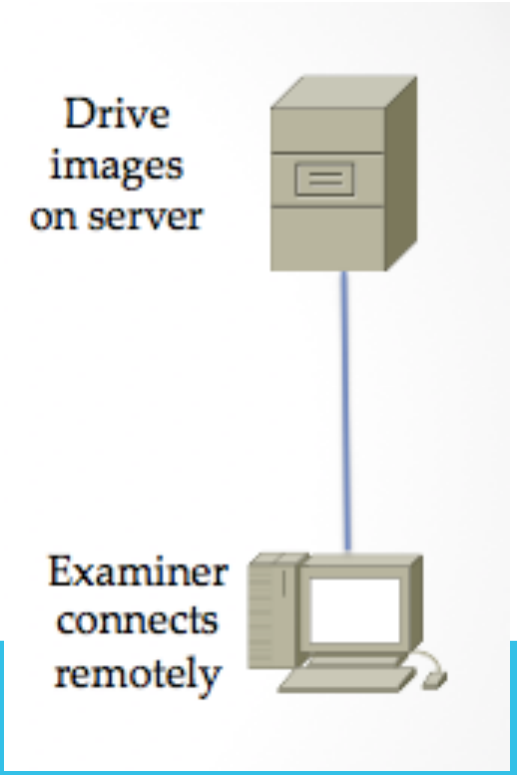
LABORATORIUM FORENSIK

FORENSIC LABORATORIUM

- Sebagian besar dijalankan oleh lembaga penegak hukum
- Laboratorium kriminal FBI di Quantico, VA adalah terbesar di dunia
- Regional Computer Forensic Laboratory (RCFL)
  - Program FBI
  - 16 fasilitas di seluruh AS
  - Mereka memproses smartphones, hard drives, GPS units, dan flash drives

LABORATORIUM VIRTUAL

- Repositori Barang Bukti repositori terpisah dari Pemeriksa
- Bagaimana FBI melakukannya
- Menghemat uang, meningkatkan akses ke resource
- Role-based access
  - Penyidik dan pihak manajemen mendapatkan akses penuh
  - Penyidik , jaksa, dan pengacara mendapatkan akses yang terbatas



HAL PENTING DENGAN VIRTUAL LABS

Security

- Harus bisa mempertahankan integritas atau barang bukti akan tidak diterima di pengadilan

Performance

- Dibutuhkan konektivitas kecepatan tinggi

Cost

KEAMANAN LAB

Pengamanan Fisik

- Jauhkan orang yang tidak berhak dari daerah-daerah penting
  - Komputer pemeriksa
  - Tempat penyimpanan Barang Bukti
- Gunakan Kunci, kartu gesek, kode akses
- Kontrol akses digital lebih baik daripada menggunakan kunci
- Simpan bukti audit untuk mendukung chain of custody
- Proteksi dari kebakaran, banjir, dll.

CHAIN OF CUSTODY

- Barang bukti harus dicatat saat masuk dan keluar dari penyimpanan
- Evidence log harus lengkap

WORK IN ISOLATION

- Pemeriksaan forensik komputer harus tidak terhubung ke Internet
- Hal ini untuk menghindari argumen mengenai kontaminasi oleh malware
- Barang Bukti drive bisa jadi berisi malware
  - Lakukan scan dengan software antivirus

EVIDENCE STORAGE

Pengamanan Data

- Melindungi bukti dari segala gangguan
- Tahan api dan tahan air

Evidence log

- mencatat siapa yang masuk, kapan, dan apa yang mereka hapus atau kembalikan

Data storage lockers harus terkunci

KEBIJAKAN DAN PROSEDUR

STANDARD OPERATING PROCEDURES (SOPS)

- Dokumen yang berupa kumpulan rincian barang bukti, pemeriksaan, dll
- Dibutuhkan untuk memastikan konsistensi dan reabilitas
- Sangat penting untuk menghadapi pertanyaan-pertanyaan di pengadilan
- Situasi yang tidak biasa terkadang membutuhkan penanganan khusus

BEST PRACTICES FOR EVIDENCE COLLECTION

- Untuk mempertahankan keaslian barang bukti, ikuti prosedur secara berurutan (Jangan gunakan komputer atau melakukan pencarian pada barang bukti)

1. Foto komputer dan sekitarnya
2. Jika komputer tidak aktif jangan menyalakannya
3. Jika komputer menyala foto layar
4. Kumpulkan data live - mulai dengan image RAM (live Respon secara lokal atau secara remote melalui F-Response) dan kemudian kumpulkan data live lain "yang dibutuhkan" seperti status koneksi jaringan, login pengguna, proses yang sedang berjalan dll.
5. Jika enkripsi hard disk terdeteksi (gunakan tool seperti Zero-View) misalnya enkripsi disk Disk PGP - kumpulkan ”logical image" dari hard disk menggunakan dd.exe, Helix – baik secara lokal atau jarak jauh menggunakan F-Response
6. Cabut kabel listrik – Jika komputer berupa laptop dan tidak mati ketika kabel dicabut maka keluarkan baterai

BEST PRACTICES FOR EVIDENCE COLLECTION

7. Gambar dan beri label semua kabel
8. Dokumentasikan semua nomor model dan nomor seri perangkat
9. Lepaskan semua kabel dan perangkat
10. Periksa HPA lalu buat image hard drive menggunakan write blocker, Helix atau imager hardware
11. Kemas semua komponen (menggunakan anti-static evidence bags)
12. Sita semua media penyimpanan tambahan (buat image masing-masing dan simpan perangkat asli dalam in anti-static evidence bags)
13. Jauhkan semua media dari magnet, pemancar radio dan elemen yang dapat merusak lainnya
14. Kumpulkan instruksi manual, dokumentasi dan catatan
15. Dokumentasikan semua langkah yang digunakan dalam penyitaan

From link : Ch 3a: Best Practices In Digital Evidence Collection

ANTI STATIC BAG

QUALITY ASSURANCE

QUALITY ASSURANCE

- Sebuah sistem dokumentasi yang baik untuk menjamin akurasi dan reliabilitas
- Penilaian report oleh Pihak Lain (peer review)
- Penanganan barang bukti
- Dokumentasi Kasus
- Pelatihan Tenaga Laboratorium

REVIEWS

Technical review

- Fokus pada hasil dan kesimpulan
- Apakah hasil yang dilaporkan didukung dengan bukti?

Administrative review

- Memastikan semua dokumen ada dan dilengkapi dengan tepat

PROFICIENCY TESTING

- Kompetensi pemeriksa harus dipastikan dan didokumentasikan
- Open test
  - Pemeriksa mengetahui bahwa mereka sedang diuji
- Blind test
  - Pemeriksa tidak menyadari bahwa mereka sedang diuji
- Internal test
  - Dilakukan oleh lembaga itu sendiri
- External test
  - Dilakukan oleh lembaga independen
- Hasil harus didokumentasikan

When Experts Lie

Fred Zain

- West Virginia State Police ahli forensik yang bersaksi dalam ratusan kasus pidana
- Sangat persuasif di pengadilan
- ..... Menjadi “bintang” forensik, yang dicari oleh jaksa yang ingin menang untuk meyakinkan pada kasus yang sulit

BERBOHONG

- Memalsukan kredebilitasnya sendiri
- Pemalsuan dan pengubahan barang Bukti
- Menghukum orang yang tidak bersalah untuk sex crimes tahun 1997
  - Ia dibebaskan ketika bukti DNA membuktikan dia tidak bersalah
  - Menggugat State of West VA
  - Mengekspos Fred Zain
- Pelaku Sebenarnya tertangkap 24 tahun kemudian

- Link Ch 3b: When Experts Lie: Fred Zain

TOOL VALIDATION

- Setiap tool, perangkat lunak atau perangkat keras, harus diuji sebelum digunakan pada kasus aktual
- Catatan kertas diperlukan untuk membuktikan ini

DOKUMENTASI

- Case File
  - Case submission forms (pelaporan kasus)
  - Requests for assistance (Permintaan bantuan)
  - Chain of custody reports (laporan urutan peristiwa)
  - Examiner's notes (catatan pemeriksa)
  - Crime scene reports (Laporan TKP)
  - Examiner's final reports (Laporan akhir pemeriksa)
  - Copy of search authorizatity (kopi surat penggeledahan)

Semua dikumpulkan dalam berkas perkara

- Preprinted forms untuk menjaga keseragaman

CATATAN PEMERIKSA

- Harus cukup rinci untuk memungkinkan pemeriksa lain untuk meniru proses
  - Berdiskusi dengan saksi kunci termasuk jaksa dan penyidik
  - Penyimpangan yang ditemukan dan tindakan yang diambil
  - OS versi & patch
  - Passwords
  - Perubahan yang dibuat untuk sistem yang dilakukan oleh tenaga laboratorium dan penegak hukum
- Bisa bertahun-tahun sebelum sidang, dan Anda akan perlu memahami catatan yang dibuat

LAPORAN AKHIR PEMERIKSA

- Dokumen resmi yang dikirim ke jaksa. penyidik , pengacara lawan, dll
- Ingat pembaca nonteknis
- Hindari jargon, akronim, dan rincian yang tidak perlu

ISI LAPORAN AKHIR PEMERIKSA

- Identitas agen pelapor
- ID Kasus #
- Identitas pelapor dan penyidik kasus
- Tanggal penerimaan dan laporan
- Penjelasan rinci tentang item bukti yang diajukan
  - Nomor seri, merek, model, dll.
- Identitas pemeriksa
- Deskripsi langkah yang diambil selama proses pemeriksaan
- Hasil dan kesimpulan

BAGIAN LAPORAN AKHIR PEMERIKSA

- Kesimpulan
  - Deskripsi singkat hasil
- Rincian Temuan
  - File yang berkaitan dengan permintaan
  - File yang mendukung temuan
  - Email, Web Cache, chat log, dll
  - Kata kunci pencarian
  - Bukti kepemilikan perangkat
- Glossary

DIGITAL FORENSIC TOOLS

DIGITAL FORENSIC TOOLS

NIST's Forensic Tool Testing Project

- Link

  Ch 3c: NIST Computer Forensic Tool Testing Program

CONTOH LAPORAN

1 Results Summary by Requirements

- **An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device.**
  For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive.

- **An HWB device shall return the data requested by a read operation.**
  For all test cases run, the device always allowed commands to read the protected drive.

- **An HWB device shall return without modification any access-significant information requested from the drive.**
  For all test cases run, the device always returned access-significant information from the protected drive without modification.

- **Any error condition reported by the storage device to the HWB device shall be reported to the host.**
  For all test cases run, the device always returned error codes from the protected drive without modification.

HARDWARE TOOLS

- Cloning perangkat
- Perangkat Cell phone acquisition
- Write blockers
- Portable storage devices
- Adapters
- Kabel
- Dan banyak lagi

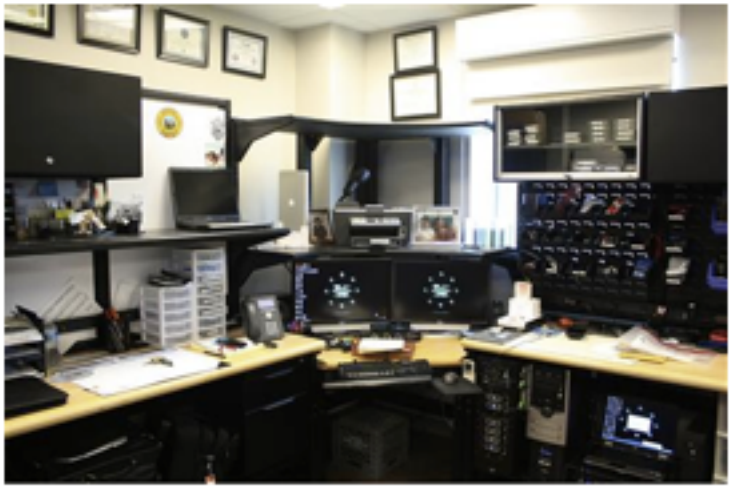


Figure 3.1 One of the workstations in the West Virginia State Police Digital Forensics Lab located at the Marshall University Forensic Science Center. (Courtesy of Cpl. Bob Boggs).

Dari buku

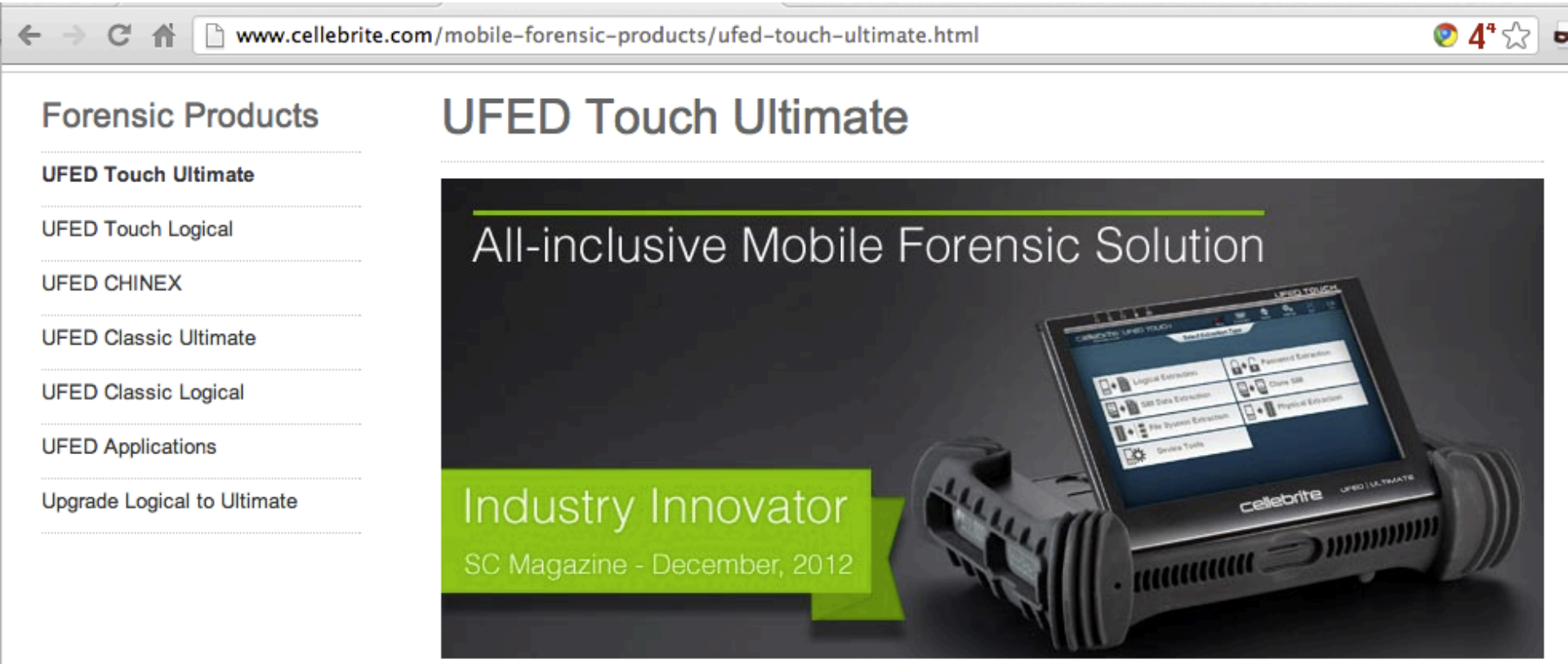
REKOMENDASI KOMPUTER

- Multiple multicore processors
- RAM sebesar mungkin
- Hard disk Kapasitas besar, dan cepat
- FTK 4 merekomendaikan :
  - 64-bit processor, Quad core
  - 8 GB RAM
  - dedicated 150 GB hard disk untuk PostgreSQL database; SSD atau RAID lebih diutamakan
  - 1 GB network
- Link Ch 3d: FTK 4 Hardware Requirements

NON-PC HARDWARE

Cellebrite's UFED

- Supports lebih dari 3,000 jenis telephone (Link Ch 3e: Cellebrite - Mobile Forensics and Data transfer solutions)



Link

Ch 3f: Creating a Cellular Device Investigation Toolkit: Basic Hardware and Software Specifications

PARABEN

- Bersaing dengan Cellebrite
- Mendukung lebih dari 4.000 ponsel, PDA, dan unit GPS

Device Seizure and Device Seizure ToolBox

$1,595

http://www.paraben-forensics.com/catalog/

Device Seizure gathers data from supported phones and devices. Device Seizure ToolBox is the cables for the supported phones. They are available individually at a cost of $895 for Device Seizure and $749 for the Device Seizure ToolBox. A one-year maintenance subscription is $180.

CLONERS DAN KITS

Hardware Cloners

- Lebih cepat, bisa mengkloning beberapa drive sekaligus
- Memiliki kemampuan write protection, hash authentication, drive wiping, audit trail…

TKP kits

- Diilengkapi dengan Perlengkapan untuk mengumpulkan bukti digital
- Pena, kamera digital, media clean storage media, evidence bags, evidence tape, formulir laporan, spidol …

SOFTWARE: OPEN-SOURCE

SIFT: SANS Investigative Forensic Toolkit

SIFT Workstation is free, based on Ubuntu

Link Ch 3g: SANS SIFT KitWorkstation: Investigative Forensic Toolkit Download

SIFT CAPABILITIES

- Windows (MSDOS FAT, VFAT, NTFS)
- Mac (HFS)
- Solaris (USF)
- Linux (ext2/3/4)
- File carving
- Menganalisis file systems
- Web history
- Recycle bin
- Memory
- Timeline

SIFT CAPABILITIES

Evidence Image Support

- Expert Witness (E01)
- RAW (dd)
- Advanced Forensic Format (AFF)

SIFT CAPABILITIES

- The Sleuth Kit (File system Analysis Tools)
- log2timeline (Timeline Generation Tool)
- ssdeep & md5deep (Hashing Tools)
- Foremost/Scalpel (File Carving)
- WireShark (Network Forensics)
- Vinetto (thumbs.db examination)
- Pasco (IE Web History examination)
- Rifiuti (Recycle Bin examination)
- Volatility Framework (Memory Analysis)
- DFLabs PTK (GUI Front-End for Sleuthkit)
- Autopsy (GUI Front-End for Sleuthkit)
- PyFLAG (GUI Log/Disk Examination)

COMMERCIAL TOOLS

EnCase & FTK memiliki fungsi yang sama

- Searching
- E-mail ananysis
- Sorting
- Reporting
- Password cracking

ENCASE & FTK

Search tools

- E-mail addresses
- Names
- Phone numbers
- Keywords
- Web addresses
- File types
- Date ranges

DON'T TRUST TOOLS

- Menggunakan tool tanpa memahami apa yang dilakukannya bisa menjadi perangkap
- Verifikasi semua temuan dengan tool kedua, seperti hex editor sederhana
- Cari tahu bagaimana data bisa berada pada sistem dan apa artinya

TOOLS SERBAGUNA LAINNYA

- Acquisition, verification, searching, reporting, wiping, dll.)
  - SMART
  - ProDiscover
  - X-Ways Forensics
  - Helix (Linux-based)
  - Raptor (Linux-based)

TOOLS LAIN

Mac Tools

- Softblock
- Macquisition
- Blacklight
- BlackBag
- Mac Marshall

TOOLS LAIN

Dossier dari LogiCube

- Hardware acquisition

Tableau

- Write-blockers

Weibetech

- Write-blockers

AKREDITASI V. SERTIFIKASI

AKREDITASI

Menetapkan kebijakan dan prosedur laboratorium kriminal

- ASCLD / LAB melakukan hal ini
  - Sangat sulit untuk dicapai
  - Tidak mungkin diterapkan pada setiap laboratorium
- ASTM juga melakukan akreditasi laboratorium

SERTIFIKASI

Berlaku untuk pemeriksa, bukan untuk lab

- SWGDE Kompetensi Inti untuk Sertifikasi Praktisi Forensi
  - Prosedur pra-pemeriksaan dan masalah hukum
  - Media penilaian dan analisis
  - Data recovery
  - Analisis spesifik pemulihan data
  - Dokumentasi dan pelaporan
  - Penyajian temuan
- Link Ch 1h: SWGDE (Scientific Working Group on Digital Evidence)