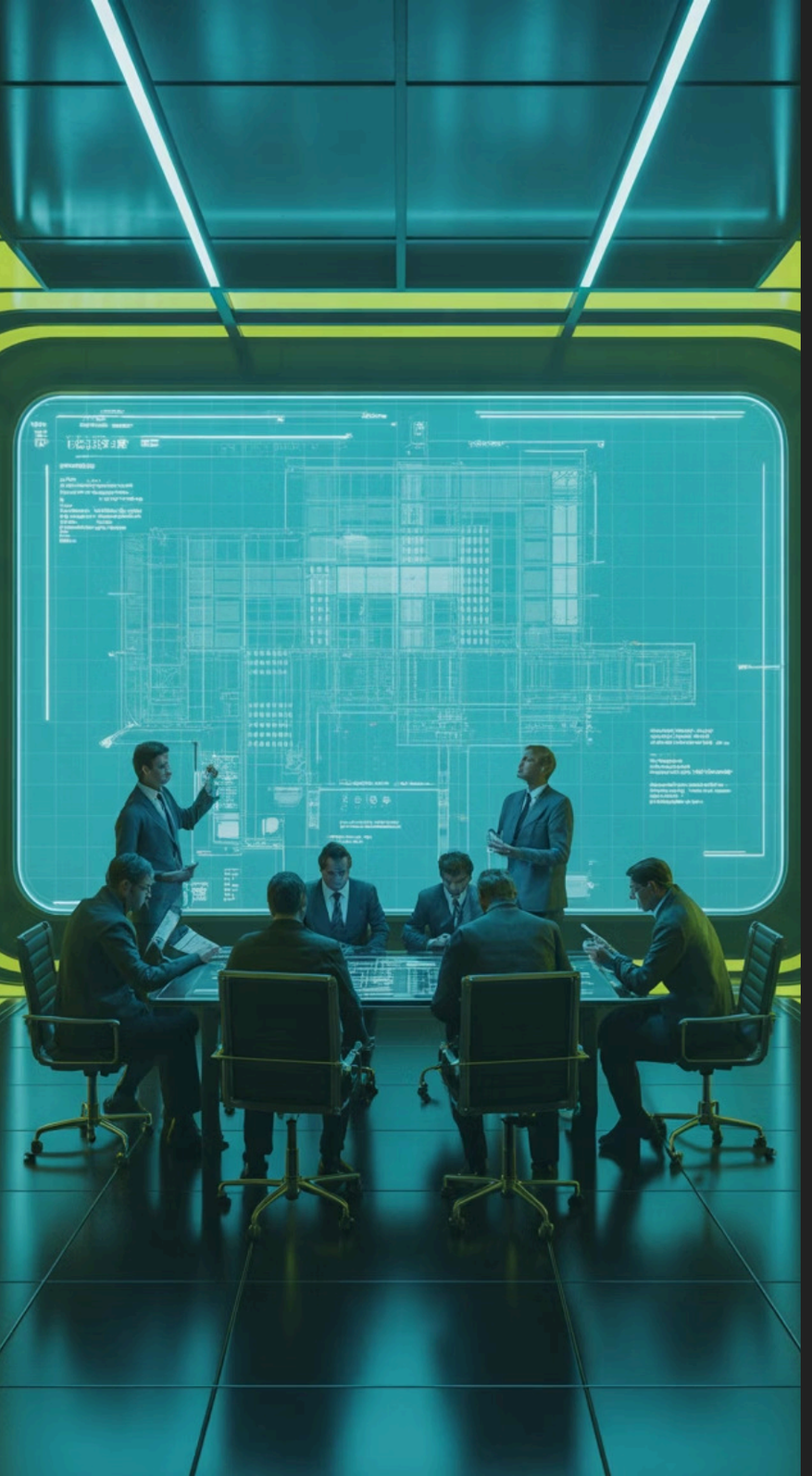
Modul 2 – Persiapan dan Peralatan Forensik

Edy Susanto | Durasi: 3 Jam



Pentingnya Perencanaan Penyelidikan Forensik

Tujuan dan Ruang Lingkup

Menentukan sasaran investigasi yang jelas dan batasan ruang lingkup sejak tahap awal untuk memastikan efektivitas penyelidikan digital.

Kebijakan Organisasi

Menetapkan kebijakan sebagai landasan prosedur forensik yang terstandarisasi dan sesuai regulasi yang berlaku.

Forensic Readiness

Membangun kesiapan organisasi dalam menghadapi insiden digital melalui infrastruktur, prosedur, dan kompetensi yang memadai.

Author : Edy Susanto

Kebijakan Organisasi dan Forensic Readiness

Implementasi Praktis

Standard Operating Procedure (SOP) respons insiden di Badan Siber dan Sandi Negara (BSSN) mengatur tahapan sistematis untuk akuisisi bukti digital yang sah secara hukum.

SOP mencakup chain of custody, dokumentasi lengkap, dan protokol penanganan bukti digital untuk menjaga integritas evidensi.

Manfaat Strategis

- Mengurangi waktu tanggap terhadap insiden keamanan secara signifikan
- Meminimalkan risiko kontaminasi dan kerusakan bukti digital
- Meningkatkan kredibilitas hasil investigasi di pengadilan
- Mengoptimalkan alokasi sumber daya forensik

Studi Kasus: Kegagalan forensic readiness pada kasus kebocoran data 2022 menyebabkan hilangnya bukti krusial karena tidak adanya prosedur backup otomatis dan dokumentasi chain of custody yang memadai.

Author : Edy Susanto

Toolset Forensik Digital: Overview dan Fungsi Utama

1	2	3
FTK Imager	**Autopsy/Sleuth Kit**	**EnCase Forensic**
Tool akuisisi untuk pembuatan forensic image dengan verifikasi hash MD5/SHA. Mendukung berbagai format storage dan menghasilkan image bit-by-bit yang presisi.	Platform open-source untuk analisis mendalam file sistem, recovery data terhapus, ekstraksi metadata, dan timeline analysis dengan antarmuka visual yang intuitif.	Solusi enterprise komprehensif untuk investigasi digital skala besar. Menyediakan fitur akuisisi, analisis, reporting terintegrasi dengan dukungan legal admissibility.

Author : Edy Susanto

Toolset Lanjutan dan Spesialisasi

X-Ways Forensics

Tool powerful dengan efisiensi tinggi untuk analisis data volume besar. Menawarkan fleksibilitas konfigurasi advanced dan kecepatan pemrosesan superior untuk investigator berpengalaman.

Cellebrite UFED

Platform ekstraksi data mobile forensics terdepan. Mendukung ribuan model perangkat untuk recovery SMS, call logs, aplikasi chat, dan data terenkripsi dalam investigasi kriminal.

Volatility Framework

Framework open-source untuk analisis forensik memori volatile (RAM). Mengidentifikasi proses tersembunyi, malware, kredensial, dan artefak yang tidak tersimpan di disk.

Wireshark

Network protocol analyzer untuk capture dan inspeksi lalu lintas jaringan secara real-time. Essential untuk investigasi serangan berbasis jaringan dan analisis komunikasi digital.

Author : Edy Susanto

Lingkungan Laboratorium Forensik yang Ideal

01

Hardware Write-Blockers

Perangkat esensial untuk mencegah modifikasi data selama proses akuisisi. Tersedia dalam bentuk USB, SATA, dan IDE untuk berbagai jenis media penyimpanan.

02

Forensic Workstation

Komputer khusus dengan spesifikasi tinggi: prosesor multi-core, RAM minimal 32GB, storage redundant, dan sistem operasi forensik yang terisolasi dari jaringan produksi.

03

Virtual Laboratory

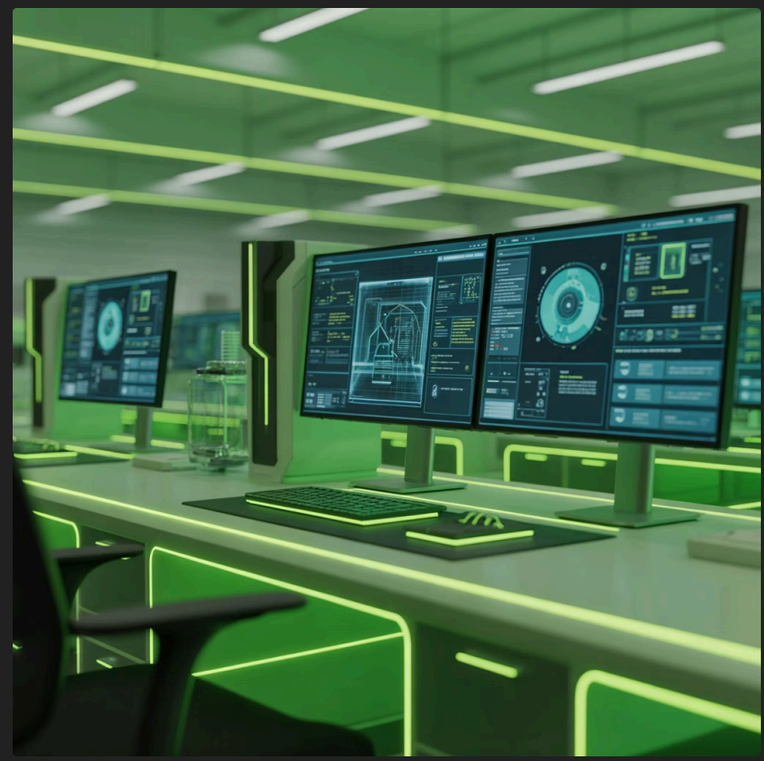
Environment simulasi menggunakan VMware atau VirtualBox untuk pengujian malware, eksperimen tool forensik, dan training tanpa risiko merusak data evidensi asli.

Author : Edy Susanto

Praktik Menyiapkan Forensic Workstation

Tahapan Konfigurasi

1. Instalasi sistem operasi khusus forensik (CAINE, DEFT, atau Windows dengan hardening)
2. Deploy software forensik utama: FTK Imager, Autopsy, X-Ways, dan Volatility
3. Konfigurasi hardware write-blocker dan verifikasi fungsinya
4. Setup isolasi jaringan dengan firewall ketat dan logging komprehensif
5. Implementasi enkripsi full-disk dan access control berbasis role
6. Dokumentasi konfigurasi dan prosedur maintenance berkala



Best Practice: Laboratorium BSSN dan universitas terkemuka menerapkan dual-boot system dengan partisi terpisah untuk analisis Windows dan Linux, meningkatkan fleksibilitas investigasi.

Author : Edy Susanto

Praktik Akuisisi Image dengan USB Write-Blocked

Persiapan Perangkat

Hubungkan media storage target ke forensic workstation melalui USB write-blocker hardware. Verifikasi LED indikator write-protection aktif.

Konfigurasi FTK Imager

Launch FTK Imager, pilih source drive yang ter-write-block. Tentukan destination path, format image (E01/raw), dan segmentasi size sesuai kebutuhan.

Akuisisi dan Verifikasi

Mulai proses imaging dengan kalkulasi hash MD5 dan SHA-1 otomatis. Setelah selesai, verifikasi integritas dengan membandingkan hash source dan image.

Dokumentasi Chain of Custody

Catat metadata lengkap: timestamp, investigator, hash values, dan kondisi media. Simpan log akuisisi sebagai bagian dokumentasi legal.

Author : Edy Susanto

Studi Kasus: Investigasi Forensik Digital Nyata

Kasus Peretasan Data Perusahaan Multinasional 2023

Insiden kebocoran 2.5 juta record pelanggan melalui eksploitasi SQL injection dan privilege escalation. Tim forensik BSSN berkolaborasi dengan penegak hukum dalam investigasi komprehensif.

Toolset yang Digunakan

- EnCase untuk akuisisi server database
- Volatility untuk analisis memory dump mencari malware
- Wireshark untuk rekonstruksi serangan jaringan
- Autopsy untuk timeline analysis dan artifact recovery
- Cellebrite untuk ekstraksi komunikasi pelaku dari mobile device

Dampak Forensic Readiness

Organisasi dengan forensic readiness matang berhasil menyelesaikan investigasi dalam 72 jam versus 3 minggu untuk organisasi tanpa preparasi.

Pelajaran kunci: Dokumentasi chain of custody yang konsisten dan backup otomatis memungkinkan recovery bukti digital yang otherwise hilang permanen.

Author : Edy Susanto

Kesimpulan dan Langkah Selanjutnya

Persiapan Matang

Perencanaan investigasi yang komprehensif dan pemilihan toolset yang tepat merupakan fondasi keberhasilan forensik digital. Investasi dalam infrastruktur dan training memberikan ROI signifikan.

Pelatihan Berkelanjutan

Simulasi rutin di laboratorium forensik dan sertifikasi profesional (CHFI, EnCE, GCFE) memastikan investigator tetap update dengan teknik terkini dan threat landscape yang evolusioner.

Praktik Hands-On

Diskusi interaktif dan latihan langsung dengan tool forensik memperdalam pemahaman konseptual menjadi kompetensi praktis yang applicable di lapangan.

Mulai Praktik Laboratorium | **Akses Materi Tambahan**