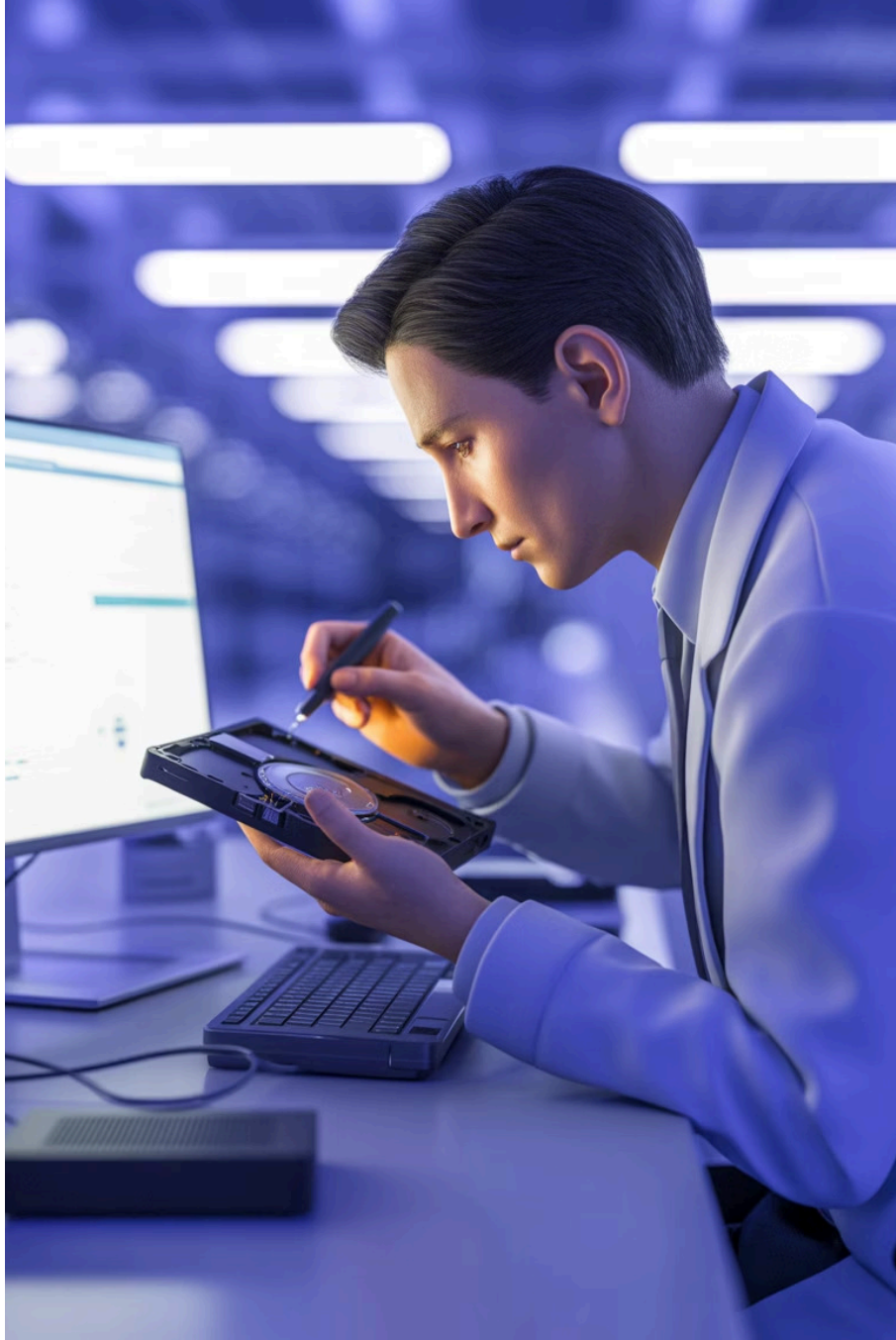
# Akuisisi Bukti Digital: Disk & File System Forensics

Modul 3 — Akuisisi Bukti: Disk & File System Forensics (4–6 jam)

Author: Edy Susanto



# Chapter 1: Metode Akuisisi Bukti Digital

Memahami teknik-teknik fundamental dalam mengumpulkan dan memverifikasi bukti digital dari media penyimpanan

# Metode Akuisisi Utama

## Raw/dd Imaging

Salinan bitwise tanpa kompresi yang menjadi standar emas dalam forensik digital. Menghasilkan duplikasi sempurna setiap bit data dari disk sumber.

## Format E01 (EnCase)

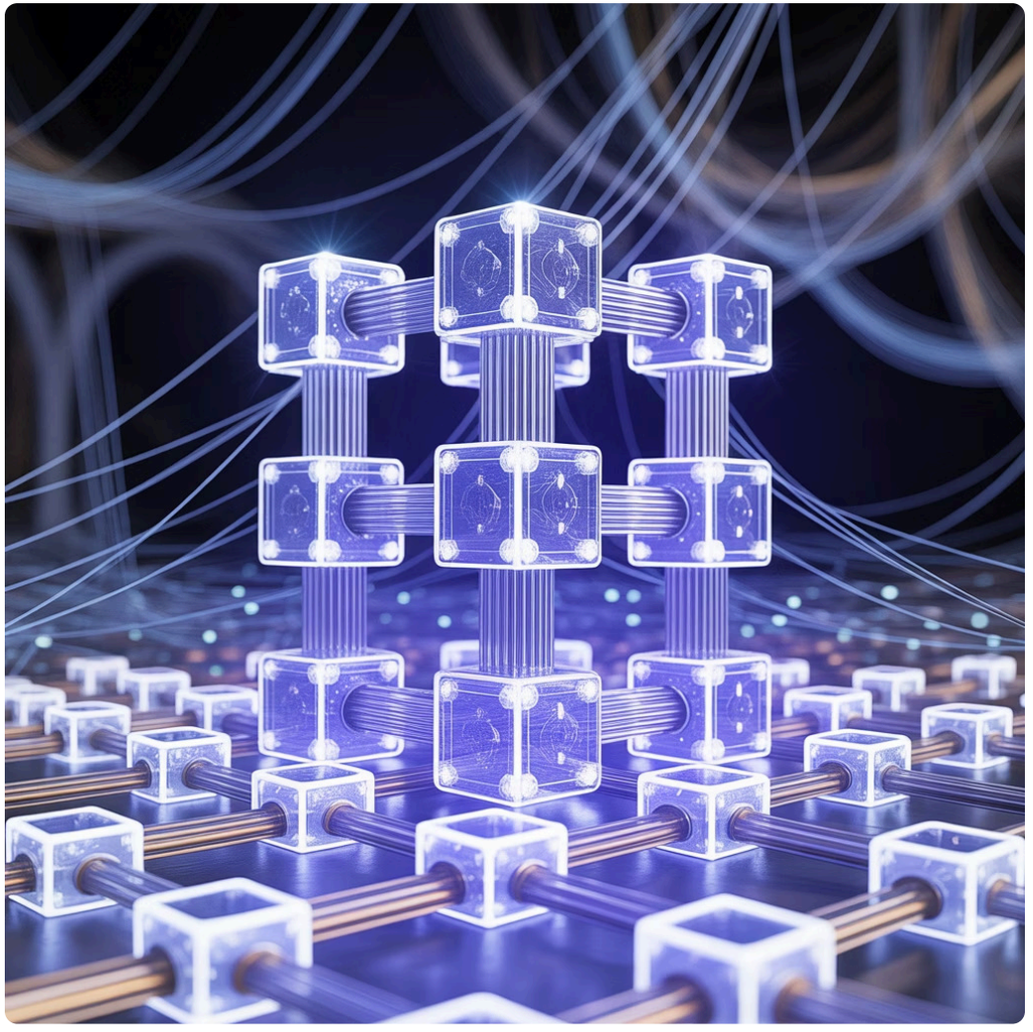
Format proprietary dengan kompresi dan metadata tambahan untuk menjaga integritas. Menyimpan informasi hash dan checksum internal.

## AFF (Advanced Forensic Format)

Format open-source yang fleksibel, mendukung metadata lengkap dan kompresi. Ideal untuk berbagai skenario investigasi.

Author: Edy Susanto

# Pentingnya Verifikasi Data



## Mengapa Verifikasi Krusial?

- Hash MD5 dan SHA-256 memastikan integritas bukti digital tetap terjaga
- Verifikasi mencegah kontaminasi dan modifikasi bukti selama proses akuisisi
- Persyaratan hukum: bukti tanpa verifikasi hash dapat ditolak di pengadilan
- Contoh kasus: pengadilan batal karena hash tidak cocok dengan image asli

Author: Edy Susanto

# Proses Imaging dan Verifikasi

1

## Akuisisi Disk

Membuat salinan bitwise dari media sumber

2

## Generate Hash

Menghitung MD5/SHA dari image hasil

3

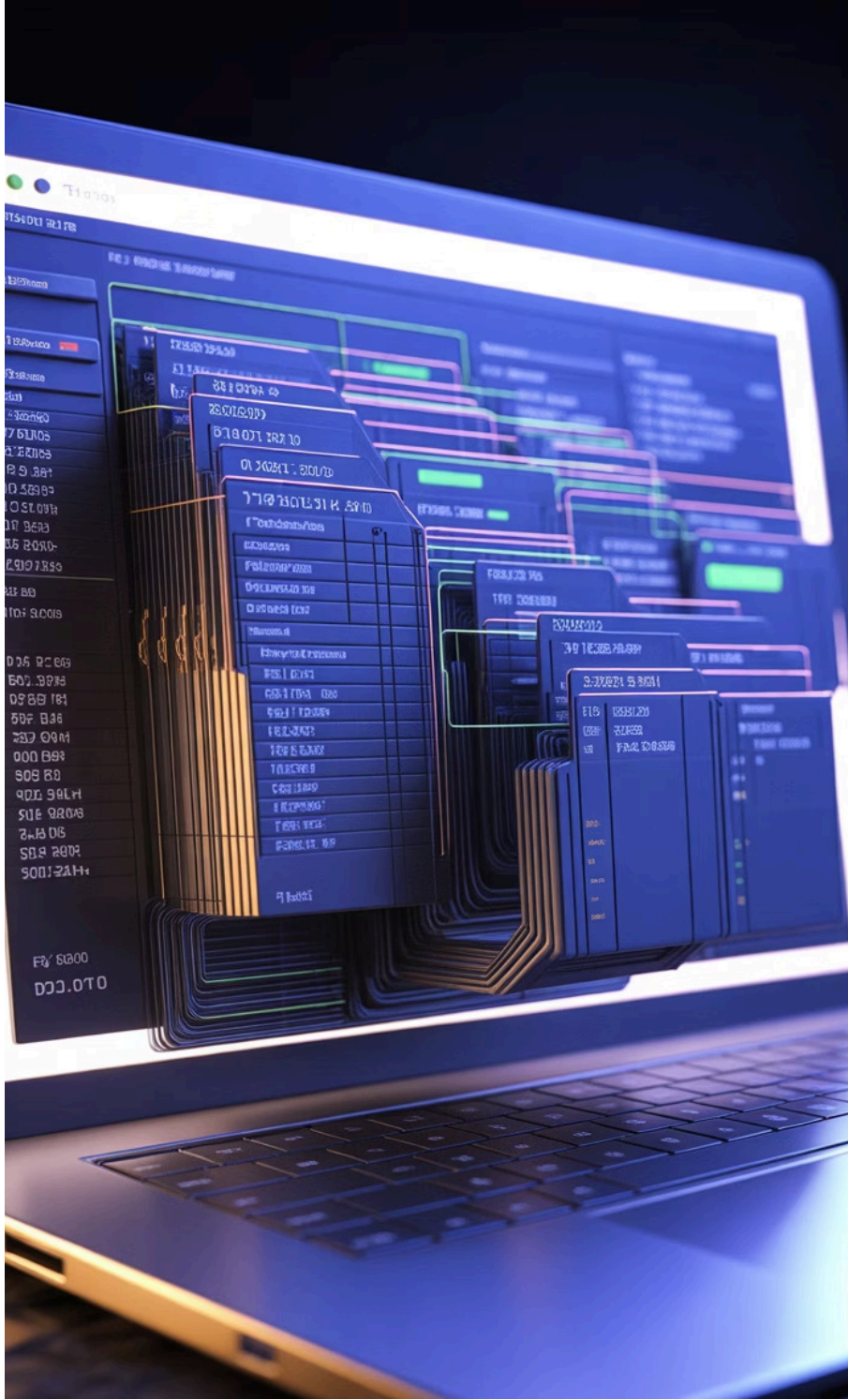
## Verifikasi

Membandingkan hash untuk memastikan integritas

Author: Edy Susanto

# Chapter 2: Struktur File System dan Artefak Penting

Menggali lebih dalam ke dalam arsitektur file system dan metadata yang menyimpan jejak digital penting



# NTFS, FAT, dan ext4: Perbedaan Kunci

### NTFS

Master File Table (MFT) sebagai pusat metadata file. Menyimpan atribut lengkap, timestamp, dan lokasi data. Mendukung enkripsi dan kompresi native.

### FAT

File Allocation Table sederhana dengan struktur dasar. Mudah rusak namun cepat dan kompatibel universal. Umum di USB drive dan SD card.

### ext4

Journaling dan inode system yang robust. Populer di Linux dengan performa tinggi dan dukungan file besar. Journal mencatat semua transaksi.

Author: Edy Susanto

# Artefak Penting dalam Forensik

## 1 MFT (NTFS)

Catatan lengkap setiap file dan direktori, termasuk file tersembunyi dan yang telah terhapus. Menyimpan metadata berharga seperti timestamps dan file attributes.

## 2 $LogFile (NTFS)

Jurnal transaksi file system yang mencatat setiap operasi. Membantu rekonstruksi kejadian dan timeline aktivitas pengguna dengan presisi tinggi.

## 3 Journal ext4

Catatan perubahan file system untuk analisis timeline di lingkungan Linux. Melacak operasi create, modify, dan delete dengan detail lengkap.

Author: Edy Susanto

# Struktur Internal File System

## Master File Table

- Entry untuk setiap file/folder
- Atribut standar dan extended
- Timestamps (MACB)
- Data resident dan non-resident

## $LogFile

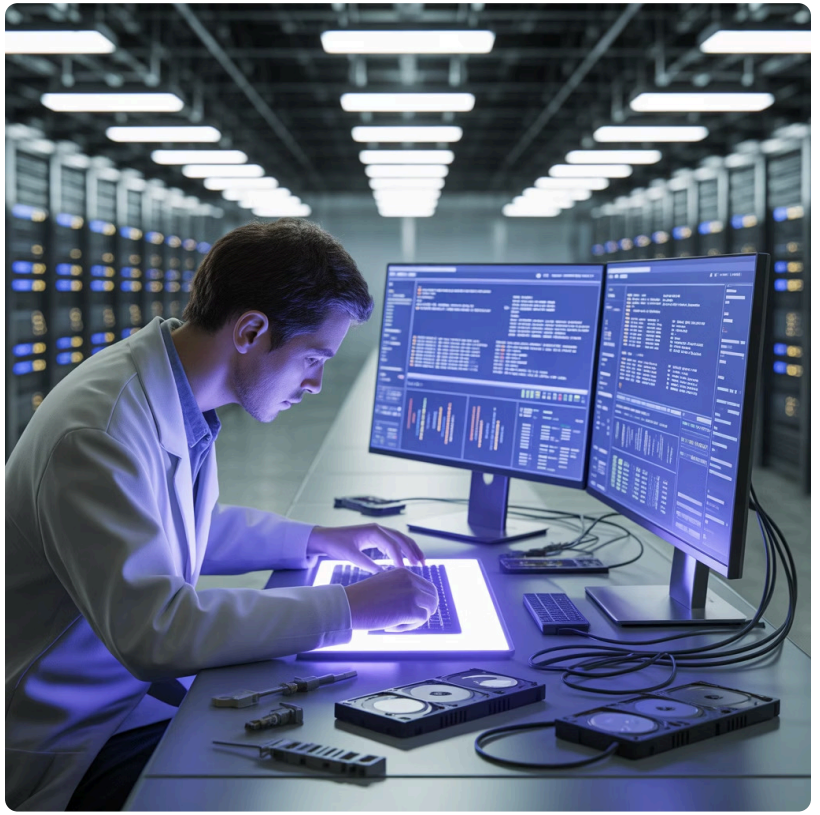
- Redo dan undo operations
- Transaction journaling
- Recovery information
- System consistency data

Author: Edy Susanto

# Chapter 3: File Carving & Recovery

Teknik ekstraksi data canggih untuk mengungkap file yang tersembunyi atau terhapus dari media penyimpanan

# Apa itu File Carving?



## Definisi dan Konsep

Teknik ekstraksi file dari data mentah tanpa bergantung pada metadata file system. Sangat efektif untuk:

- File yang telah terhapus dari recycle bin
- Partisi atau file system yang rusak
- Media yang telah diformat
- Disk yang mengalami korupsi

Menggunakan signature unik file (header/footer) untuk identifikasi dan rekonstruksi data yang hilang.

Author: Edy Susanto

# Teknik File Carving Populer

01

## Header-Footer Carving

Mencari pola byte awal dan akhir file. Contoh: JPEG dimulai dengan FF D8 dan diakhiri FF D9. Teknik paling umum dan cepat.

02

## Structure-Based Carving

Analisis struktur internal file untuk rekonstruksi lebih akurat. Memahami format file secara mendalam untuk hasil optimal.

03

## Content-Based Carving

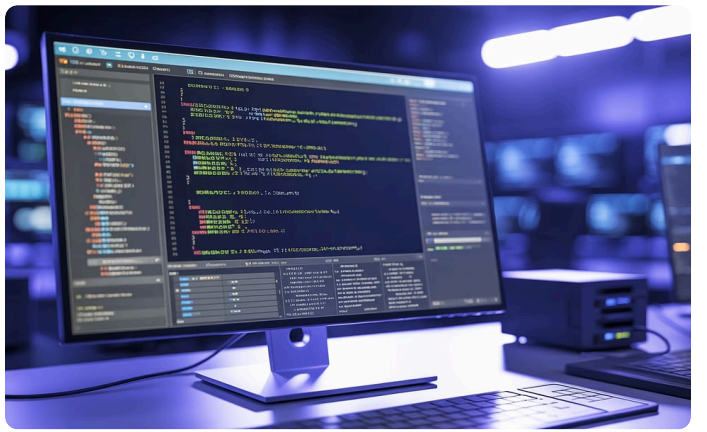
Mengenali konten file berdasarkan karakteristik data saat header/footer hilang. Menggunakan pattern matching dan statistical analysis.

Author: Edy Susanto

# Tools File Carving Terbaik

## Autopsy

Platform open-source dengan GUI intuitif. Mendukung berbagai format file dan modul extensible untuk analisis mendalam.



## Foremost

Tool command-line fokus header/footer carving. Digunakan oleh militer AS dengan kecepatan tinggi dan presisi.

## PhotoRec

Powerful untuk berbagai tipe file dan media. Mengabaikan file system dan bekerja langsung dengan raw data sectors.

Author: Edy Susanto

# Praktik: Akuisisi, Verifikasi, dan Recovery

## Buat Image Disk

Gunakan dd command atau FTK Imager untuk membuat salinan bitwise dari disk target. Pastikan write-blocker aktif.

## Verifikasi Hash

Hitung MD5/SHA-256 dari image dan bandingkan dengan hash asli. Dokumentasikan hasil untuk chain of custody.

## Recover File Terhapus

Gunakan Foremost atau Autopsy untuk melakukan file carving. Identifikasi file signature dan ekstrak data.

## Analisis dan Dokumentasi

Review hasil recovery, catat temuan penting, dan buat laporan forensik lengkap dengan evidence timeline.

Author: Edy Susanto

# Kesimpulan & Langkah Selanjutnya

## Poin-Poin Kunci

- **Akuisisi yang Akurat**

  Bukti digital harus diakuisisi dengan metode yang tepat dan terverifikasi melalui hash cryptographic.

- **Pemahaman File System**

  Menguasai struktur NTFS, FAT, dan ext4 memperkuat kemampuan analisis forensik dan investigasi.

- **File Carving Essentials**

  Teknik carving adalah kunci untuk mengungkap data tersembunyi dan file yang telah dihapus.

- **Praktik Lapangan**

  Hands-on training memperkuat pemahaman teoritis dan mempersiapkan kesiapan investigasi real-world.

### Next Steps

Lanjutkan dengan latihan mandiri dan eksplorasi tools forensik tambahan untuk memperdalam keahlian.

Author: Edy Susanto