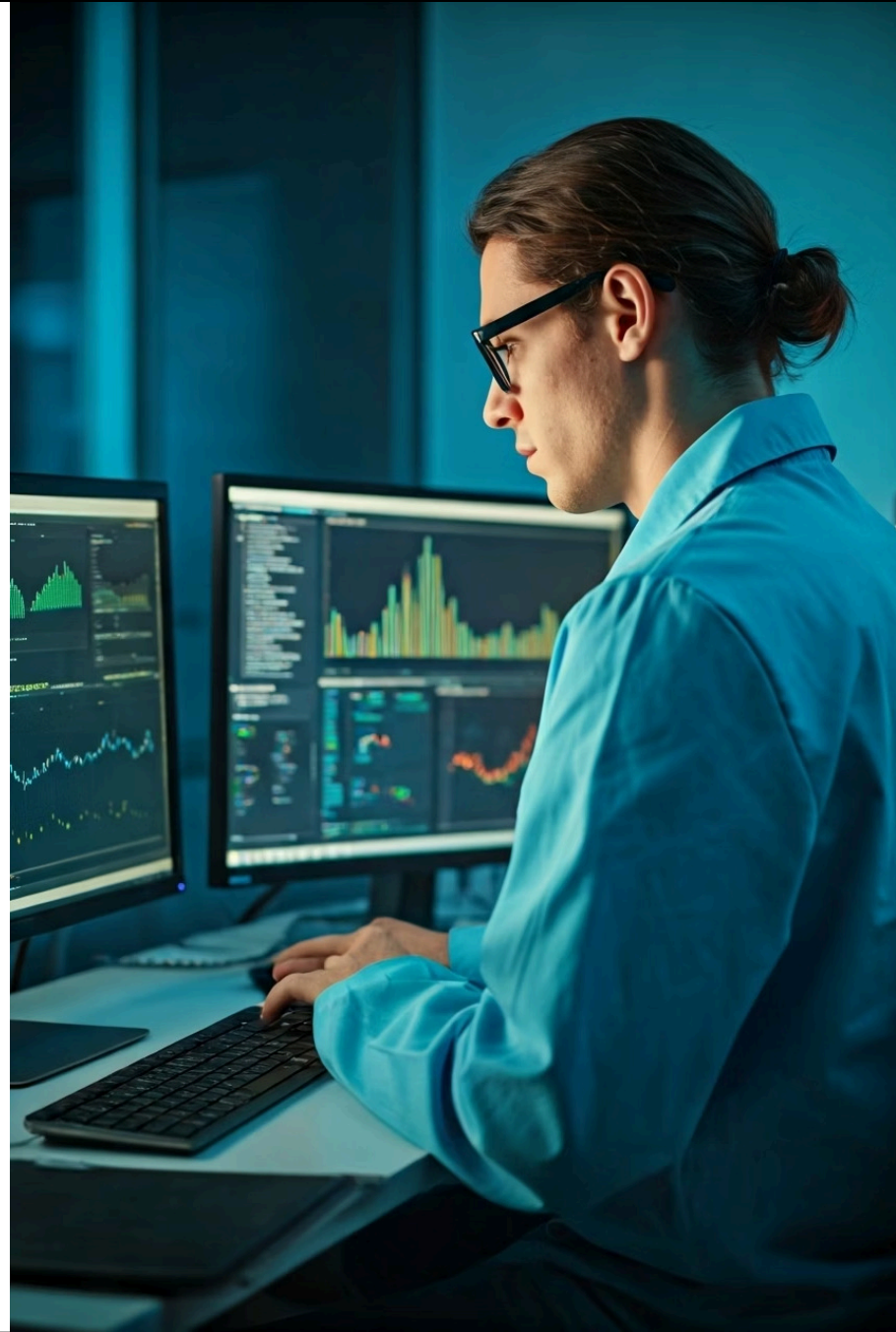
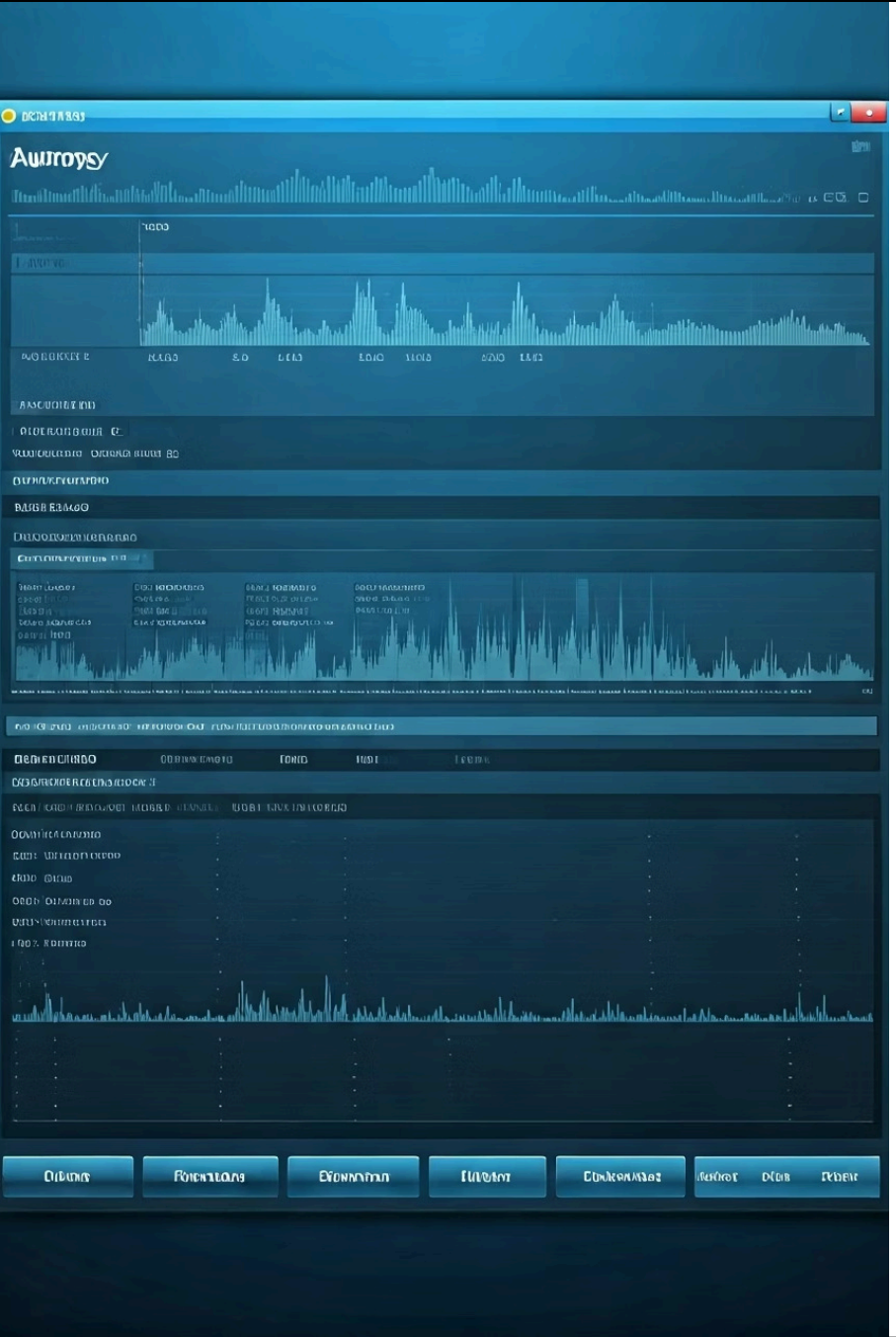
Ultimate Forensics Toolkit

Digital forensics tools empower investigators to uncover crucial evidence. This presentation explores the most effective tools for modern cyber investigations.





Autopsy: The Digital Investigator's Workbench

Comprehensive Analysis

Examines disk images, mobile devices, and diverse digital media formats.

Artifact Recovery

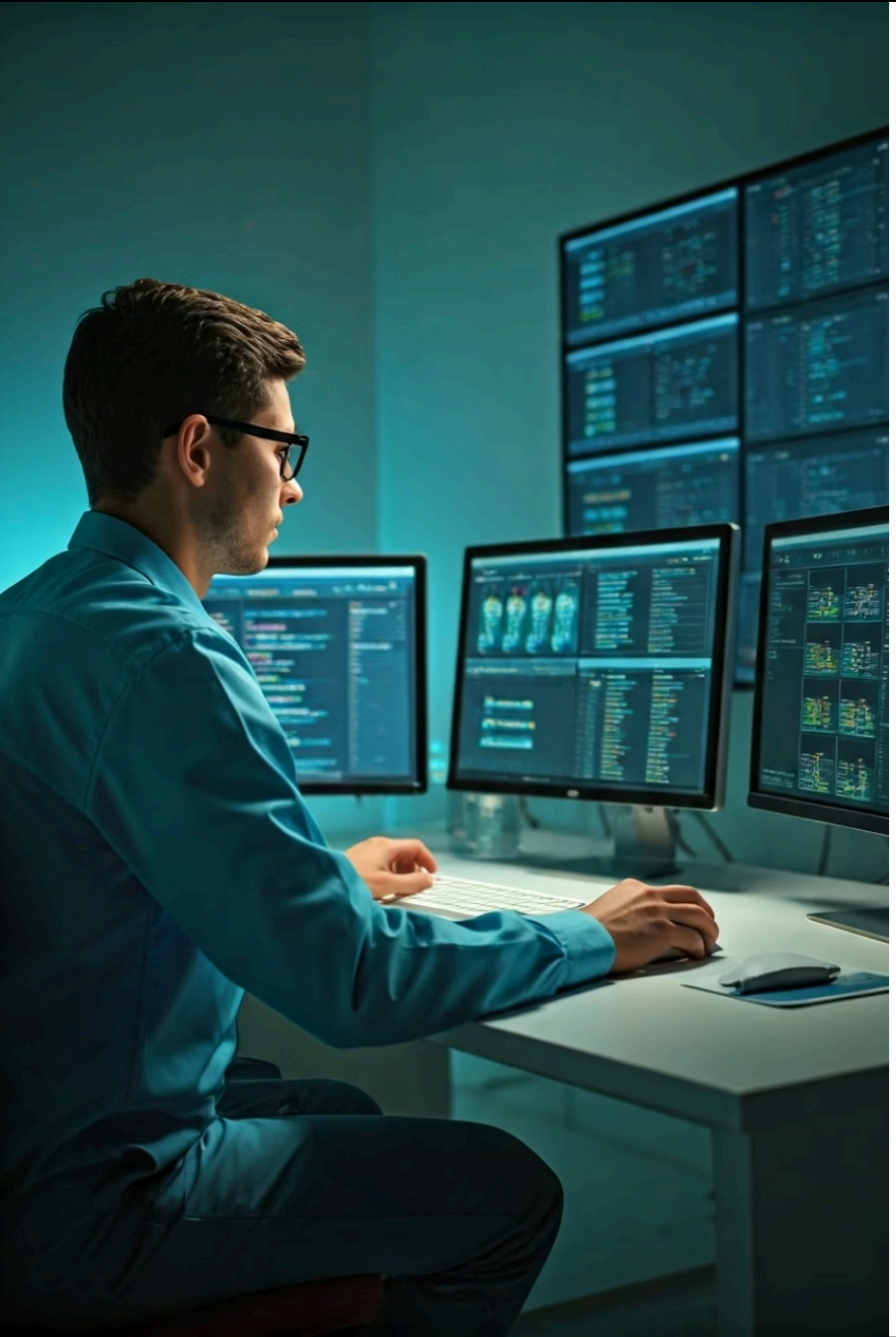
Extracts browser history, registry data, emails, and chat messages.

Timeline Construction

Creates chronological sequences of events across multiple sources.

Keyword Searching

Locates specific terms across vast datasets with advanced filtering.



Specialized Autopsy Add-on Modules

Media Analysis

- Video Triage splits videos into thumbnails
- Perceptual Hash creates image fingerprints

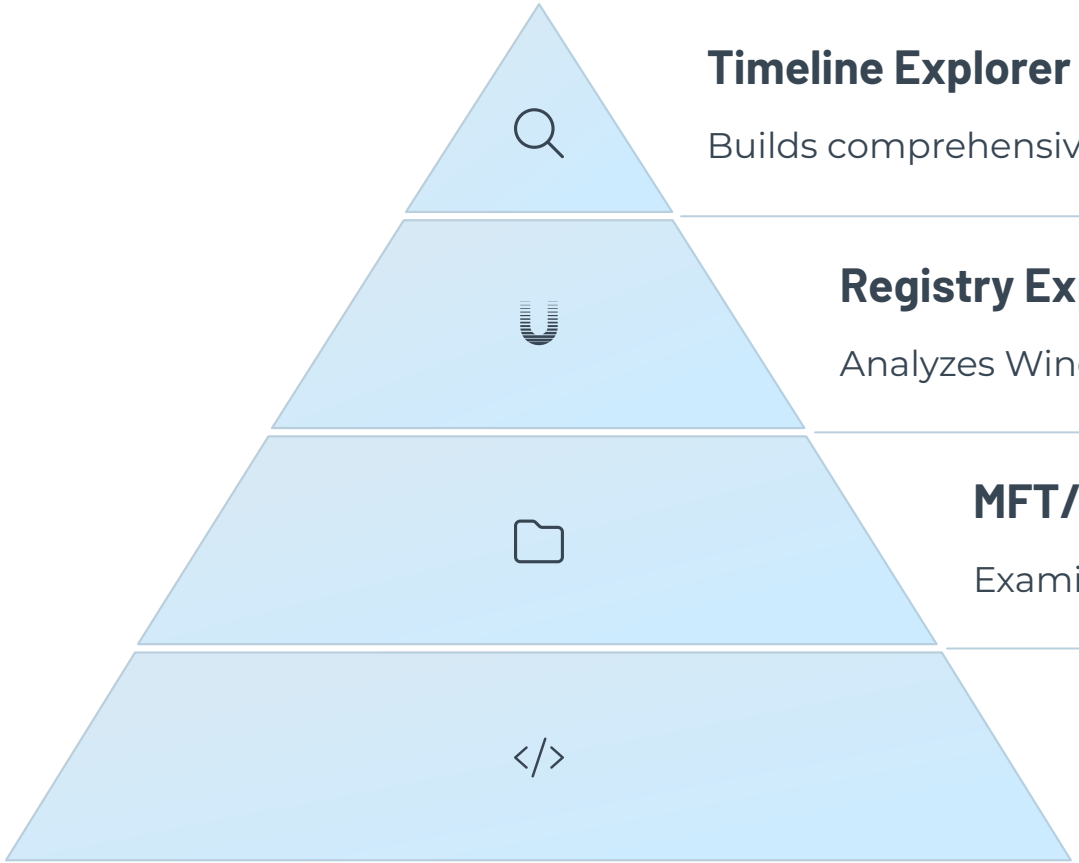
Advanced Filtering

- Code Signing Certificate Verification
- Golden Image Comparison identifies changes

Content Processing

- Text Gisting analyzes foreign-language content
- Log Forensics extracts Windows log data

Eric Zimmerman's Forensic Suite



Timeline Explorer

Builds comprehensive event chronologies

Registry Explorer

Analyzes Windows Registry artifacts

MFT/ShellBags/JumpList Tools

Examines file system and user activities

Command-line Utilities

Enables automation and batch processing

Registry and Execution Analysis Tools

Amcache Parser

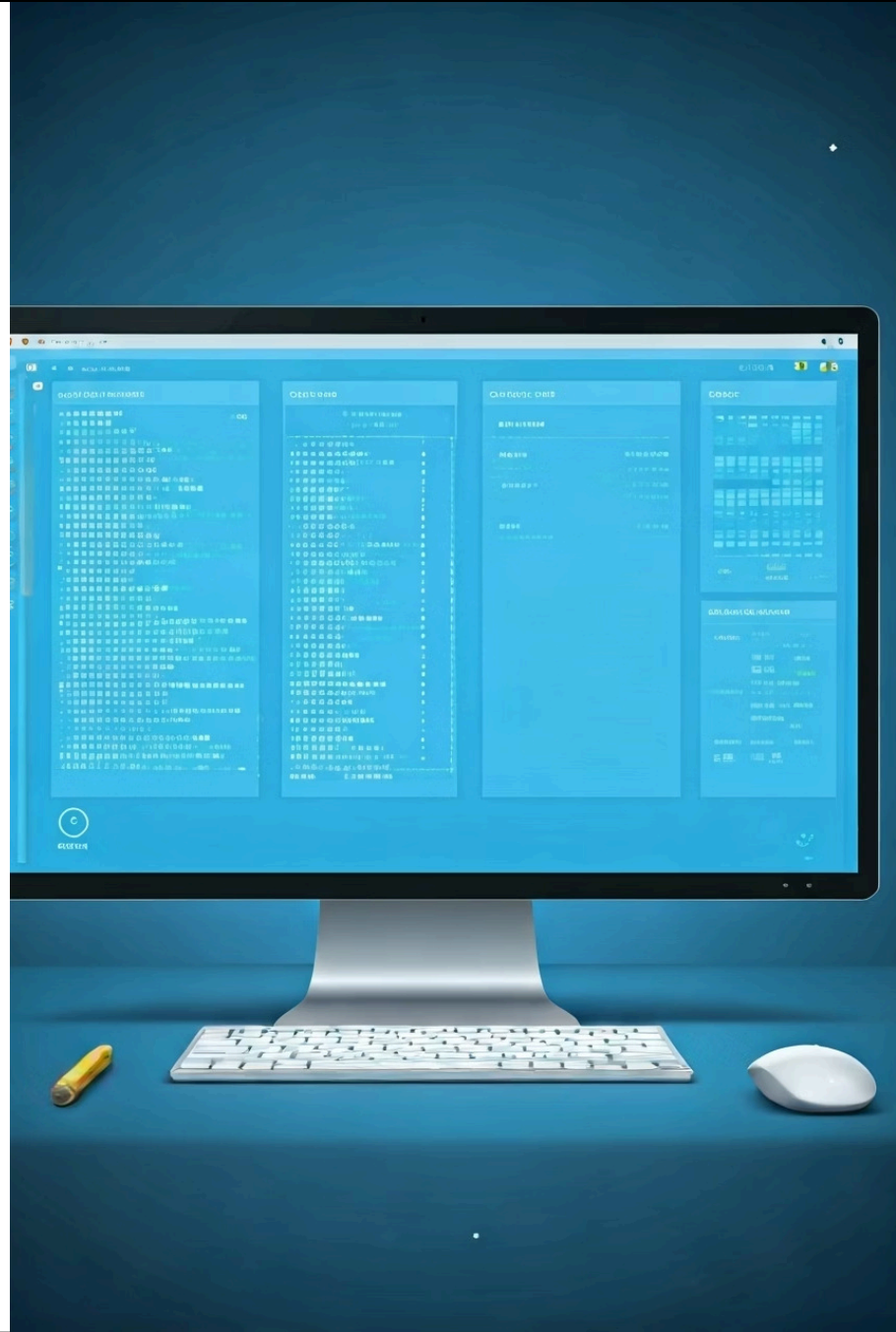
Identifies executed programs and unassociated files. Reveals application activity even after deletion.

AppCompatCacheParser

Extracts ShimCache data with executable paths. Provides timestamps for program execution evidence.

WxTCmd

Parses Windows 10 Timeline database. Recovers 30-day history of user activities.



User Activity Forensics Tools

ShellBags Explorer

Tracks folders users interacted with. Reveals navigation even after deletion.

MFTExplorer

Analyzes file table entries. Recovers information about deleted files.

JumpList Explorer

Parses recently used files. Shows application-specific user tasks.

Timeline Explorer

Correlates events chronologically. Enables complex filtering of activities.

Disk-Level Analysis Tools

MH-Nexus HxD

A powerful hex editor for examining raw data at the byte level.

- Opens large files efficiently
- Calculates checksums
- Performs binary comparisons
- Enables memory editing

Disk Editor Functions

Provides low-level access to critical disk structures.

- Examines MBR and GPT
- Analyzes file system metadata
- Recovers damaged partitions
- Inspects hidden sectors

Data Sanitization and Security

Identify Media

Catalog all storage devices requiring sanitization. Document media types and capacities for verification.

Select Erasure Method

Choose appropriate KillDisk sanitization standard. Different standards offer varying security levels.

Verify Completion

Confirm successful data destruction. Generate certificates for compliance documentation.