Feature	Autopsy	X-Ways	AXIOM
	https://sleuthkit.org/autopsy/docs/user-docs/4.0/	http://www.x-ways.net/winhex/manual.pdf	https://www.magnetforensics.com/docs/axiom/html/Content/Resources/PDFs/Magnet%20AXIOM%20User%20Guide.pdf
Parse Image Format	Data Sources section	Interpret Image File as Disk (p82)	Supported Images and Fiel Types (p31)
Validate Disk Image	E01 Verifier Module - “computes a checksum on E01 files and compares with the E01 file's internal checksum to ensure they match.”		Image hashing and image hash verification (P242)
Identify Partitions			
Process File System (live/non-allocated)		Refine Volume Snapshot (p137)	Deleted files recovered and carved, but 'known deleted file' artefacts only are kept if not the same (p245)
Identify Files (Carving)	PhotoRec Carver Module - “carves files from unallocated space in the data source and sends the files found through the ingest processing chain.”	File header search (p140), file recovery by type (p170)	Reprocess artifacts with carving (P151)
File Type Identification	File Type Identification Module - “identifies files based on their internal signatures and does not rely on file extensions.”	File Type Categories (p119), File type verification (p143)	Custom file types (p138)
File Specific Processing - *Embedded files*	Embedded File Extraction Module - “opens ZIP, RAR, other archive formats, Doc, Docx, PPT, PPTX, XLS, and XLSX and sends the derived files from those files back through the ingest pipeline for analysis. This module expands archive files to enable Autopsy to analyze all files on the system. It enables keyword search and hash lookup to analyze files inside of archives	Extraction of internal metadata (p143), archive exploration (p147), uncovering embedded data (p150)	Search archives and mobile backups (P115)
File Specific Processing - *Content Viewers*	Content Viewer - parse and display specific file types	Viewer functionality p99	
File Specific Processing - *EXIF*	EXIF Parser Module - “extracts EXIF (Exchangeable Image File Format) information from ingested pictures”		Extract EXIF (p145)
File Specific Processing - *Email*	Email Parser Module - “identifies Thunderbird MBOX files and PST format files based on file signatures, extracting the e-mails from them. It adds email attachments as derived files.”	Email extraction (p148)	Export Emails (p221)
File Specific Processing - *OS Artefacts*	RegRipper is run	Registry report, Refine snapshot (including volume shadow copies) (p101)	Windows Registry (p182)
File Specific Processing - *Encrypted Files*		Encryption Detection (p157)	Decrypt APFS, Bitlocker, others (Passware plugin) (p35)
File Specific Processing - *Databases*			SQLite viewer (p180) LevelDB viewer (p181)

Feature	Autopsy	X-Ways	AXIOM
Keyword Searching/Indexing	Keyword Search Module - “Autopsy tries its best to extract the maximum amount of text from the files being indexed. First, the indexing will try to extract text from supported file formats, such as pure text file format, MS Office Documents, PDF files, Email, and many others. If the file is not supported by the standard text extractor, Autopsy will fall back to a string extraction algorithm.”	Simultaneous search (p104), keyword indexing (p158)	add keywords to a search, use of regex (p119) keyword searching (p117) Character encodings (p117)
Timeline Generation	Timeline - display extracted timestamps from file system, web activity, and others including: messages, calls, email, recent documents, installed programs, exif metadata, devices attached	Events List (p115)	View evidence on a timeline (p173)
Location Extraction	Has location feature	Locations extracted from EXIF (p38)	offline map server - render points on a map (p255)
Other Entity Extraction	Predefined regex for credit cards, phone numbers etc.		
File Browsing/Searching (name, path, size, type etc)	Set of rules to match specific files based on file name or path patterns, or file search by attributes e.g. name, size, dates and times	Can be achieved through filtering (p20)	Discover Connections (p165) Explorer the File System (p177)
Automated Result Extraction	"extracts user activity as saved by web browsers (including web searches), installed programs, and the operating system.." allows you to analyze SQLite and other files from an Android device the module should be able to extract the following: Text messages / SMS / MMS, Call Logs, Contacts, Tango Messages, Words with Friends Messages, GPS from the browser and Google Maps, GPS from cache.wifi and cache.cell files	For example browser events are parsed in event extraction (p116)	Conversation view (p162)
Image Processing (images/videos)		OCR (p126), Excire photo analysis with AI (p128), capture still images from videos, picture analysis and processing (skintone) (p154)	OCR (p120) detect skin tone (p145) video previews with stills (p146) photoDNA (p208)
AI-based Content Flagging			Analyse chats (magnet.AI) (p131)
Mismatched File Signatures	Extension mismatch’ uses the results from the File Type Identification and flags files that have an extension not traditionally associated with the file's detected type.		
File Hashing/Matching	“The Hash Database Lookup Module calculates MD5 hash values for files and looks up hash values in a database to determine if the file is known bad, known (in general), or unknown.”	Hash database (p120), also PhotoDNA (p123), blockwise hashing (p140)	Hashing (p122) Managing hash sets (p127)