DETEGO GLOBAL

DETEGO SUITE PRO

TECHNICAL SPECIFICATIONS 2026 R2

TABLE OF CONTENTS

DETEGO SUITE PRO

Detego Suite Pro is designed to enable novices and expert users to forensically extract, analyse and report on data from a range of devices, including laptops, computers, servers and various storage media such as SD/Micro SD Cards, USBs and optical discs like CDs, DVDs, and Blu-ray discs.

Equipped with globally patented technology, the platform offers unparalleled data extraction speeds, precise and rapid triage, intelligent workflow automation, and AI-powered analytics, all contributing to quicker case resolutions.

Originally developed to meet the rigorous demands of special forces operatives and intelligence agencies requiring swift results in lab and field environments, Suite Pro has evolved into a user-friendly solution that's trusted by investigators in the military, law enforcement and corporate spaces.

This end-to-end platform simplifies investigative processes and reduces complexities and costs while supporting forensics teams worldwide with interface options in Arabic, French, German, Italian, Japanese, Spanish, Swedish, and Brazilian Portuguese. It also eliminates the need for extensive training on multiple systems, helping you save time and resources.

Suite Pro includes:

- **Ballistic Imager:** The world's fastest forensic imaging tool with patented technology that enables you to rapidly secure data from computers, laptops and servers up to 8x faster than the industry average.
- **Field Triage:** A portable tool with patented technology that’s perfect for investigating data on computers, laptops, servers, and loose media. It empowers investigators by identifying and alerting them about data related to investigations through a red-amber-green visual alert system.
- **Media Acquisition:** An intuitive tool that enables the simultaneous acquisition and analysis of data from multiple devices. Use Media Acquisition to acquire, analyse and act on critical data from removable media, mobile devices, computers, and hard drives, and make on-the-spot decisions by accessing live previews of the data being captured.
- **Fusion:** This tool enables investigators to leverage AI-powered link-building capabilities to uncover connections between people, places, devices, and cases.
- **Analyse AI+:** Detego Analyse AI+ integrates all forensic acquisitions and leverages powerful AI analytics and automation to provide in-depth analysis, intelligence, and court-ready reports. This solution comes with fully automated analytical workflows, semantic search, AI-powered object detection, face recognition, AI transcription and translation, Optical Character Recognition (OCR), PhotoDNA matching, password decryption (on more than 300 file types), MD5 and SHA1 hash-matching, and more.

BALLISTIC IMAGER

FOR COMPUTERS, LAPTOPS, AND SERVERS

Ballistic Imager is the world's fastest forensic imaging tool. Patented for its unparalleled speed and ability to split imaging processes using multiple collectors, Ballistic Imager is the ideal choice for time-critical investigations by police teams, military units, intelligence agencies, and corporate investigators.

Its lab and field-tested capabilities provide imaging speeds that are 8x faster than the industry average and significantly reduce acquisition times. Ballistic Imager's intuitive interface is designed for ease of use, enabling non-technical users to master its functions with just 30 minutes of training.

Ballistic Imager comes standard with Detego Analyse AI+ – a central hub for securely storing, managing, and analysing case data and exhibits acquired through Detego and third-party platforms.

Key features:

- Forensically secure data from hard disks in minutes.
- Deploy on computers and laptops running Windows, Mac, or Linux.
- Swiftly secure data from servers.
- Achieve blisteringly fast data capture speeds by splitting the imaging process using multiple collectors and utilise all available ports.
- Extract data in live or boot environments.
- Benefit from MD5, SHA1, and SHA256 validation.
- Stop extractions before completion without losing data.
- Recover deleted data.
- Deploy without removing hard drives from target devices.
- Rapidly extract RAM data.
- Present captured data as an E01, DD, or Ex01 image.
- Enjoy greater mobility thanks to its portable and compact design.

KEY FEATURES IN DETAIL

Easily deployable forensics

Designed to overcome challenges encountered by field and lab-based investigators, the Ballistic Imager software can be licensed to portable storage devices, making it a compact acquisition tool ideal for any setting.

Non-technical users can easily navigate its user-friendly interface and conduct forensically sound data extractions with a brief 30-minute training session.

Rapid imaging capabilities

Recently, a leading covert agency used Ballistic Imager to successfully image a 1TB drive in just 4 minutes and 34 seconds, showcasing its remarkable speed. The imaging speed of Ballistic Imager depends on the target device's specifications.

For example, a modern SSD equipped with USB C and eSATA ports will image faster than a 5-year-old HDD device. Nevertheless, Ballistic Imager's unique capability to divide the imaging process among multiple collectors ensures it consistently surpasses other imaging solutions in speed, regardless of the age or specs of the device.

Indicative imaging speeds/times

Here are the average speeds that you can expect for a mid-level specification of a 512GB and 1TB machine:

- Dell Latitude, 512GB Drive, SSD, USB C = 12 mins 59 secs.
- Dell Latitude, 1TB Drive, SSD, USB C = 25 mins 47 secs.

BALLISTIC IMAGER TECHNICAL DETAILS

Imaging Formats	• DD on image • E01 optional rebuild • Ex01 optional rebuild
Compression Modes	• No compression • Best compression • Fast compression
Hash Verifications	• MD5 only • MD5 and SHA1 • MD5 and SHA256
Supported Operating Systems	• Windows • macOS • Linux
Image Splitting	Unlimited secondary collectors

FIELD TRIAGE

FOR COMPUTERS, SERVERS, AND LOOSE MEDIA

Field Triage is a highly portable field-based solution, perfect for investigating data on computers, laptops, servers, and loose media. Field Triage uses keywords and hash-matching technology to swiftly identify and alert users about data related to investigations without running time-consuming extractions and analytical processes.

Field Triage enables users to make quick decisions in time-critical scenarios, thanks to its patented red-amber-green visual alert system. This visual confirmation allows the user to determine the severity of the content or activity contained on the device and determine whether further investigation or arrest is necessary.

A 'Red' warning indicates that known files have been detected, for example, an MD5, SHA1, or SHA256 hash linked to an IIOC, ICAC, CSAM, or counter-terrorism file. An 'Amber' alert happens when suspicious content such as a pre-defined keyword, IP address, MAC address, or other value (in any language) is matched. If no amber or red criteria has been met at the end of the acquisition, the indicator will turn 'Green', meaning the target computer is clear of a specific search type.

Key features:

- Deploy it anywhere using a removable storage device or external hard drive.
- Rapidly acquire usernames and passwords and swiftly identify data that's critical to investigations.
- Effortlessly customise it for use across a range of investigation types, including modern slavery, fraud, insider trading, harassment, Indecent Images of Children (IIOC), Internet Crimes Against Children (ICAC), human trafficking, and terrorism.
- Speed up investigations by leveraging its advanced automation capabilities.
- Accelerate evidence discovery with the all-new Xpress HashScan mode, offering speeds that are 6x faster for pictures and video files, and 3x faster for all file types
- Use data from the Child Abuse Image Database (CAID) and Project VIC to fast-track IIOC, CSAM, and ICAC investigations.
- Get users up and running in minutes with its simple, easy-to-use interface that's ideal for non-technical users.

KEY FEATURES IN DETAIL

The swift acquisition of usernames and passwords

Detego Field Triage can swiftly scan a target laptop, computer, or server and extract a complete list of usernames and passwords used on the device in under 30 seconds. This easy-to-use feature enables investigators of any technical skill level to access this information quickly.

Users have the option of viewing these passwords in real time or can opt to examine a more comprehensive report at a later stage. (Note: This feature is limited to only retrieving usernames for macOS systems.)

Ease of deployment

Designed to overcome challenges encountered by field and lab-based investigators, Detego Field Triage can be licensed to portable storage devices, making it a compact acquisition tool ideal for any setting.

Non-technical users can easily navigate its user-friendly interface and conduct forensically sound data extractions with a brief 30-minute training session.

Highly configurable search profiles

- **Quick Config Mode:** Tailored for urgent investigations, this setting allows immediate access to essential evidence and intelligence in time-sensitive scenarios.
- **One-Click Physical Extraction:** Effortlessly create a complete image of a target device's physical drive with a single button press.
- **Select a Stock Profile:** Use one of the pre-set extraction profiles crafted for rapid results and quick investigative wins.
- **Re-Use the Latest Profile:** Easily repeat the most recently used acquisition profile on the Field Triage device.
- **Custom Profile Creation:** Set up your device with bespoke configurations to align with specific investigative goals, adapting to various operation types and crime categories (ICAC, fraud, counterterror, etc.).
- **Profile Loading and Execution:** Custom profiles enable rapid deployment of Field Triage by staff, regardless of their technical expertise, accommodating various investigation needs. Once these profiles are created, they are easily transferable onto USB drives. This allows investigators, irrespective of their experience level, to efficiently use these tools on target devices, ensuring data acquisitions are secure and adhere to forensic best practices.

FIELD TRIAGE TECHNICAL DETAILS

Extraction Jobs*	• Memory extraction • Decryption (beta) • System information • Password finder • Internet artefacts • Logical extraction • File carve • Device matrix • Physical image **The availability of certain features may vary for macOS devices*
Memory Extraction*	• Live system memory: extract RAM • Offline system memory: extract hibernation file, extract swap file, extract page file **The availability of certain features may vary for macOS devices*

Imaging Format	• E01 • Ex01 • DD
LZ4 compression	• On/Off
Hash Verifications	• MD5 only • MD5 and SHA1 • MD5 and SHA256
Software Write Blocking	• Optional
Logical Extraction Parameters	• Date and time (or regardless of) • Recent timestamps • File size: larger than, less than, between
File Systems	• ntfs (NTFS) • iso (ISO9690 CD) • hfs (HFS and HFS+) • APFS (live extraction + DD images acquired from non-chipped Apple hardware) • raw (raw data) • swap (swap space) • memory (RAM data) • FAT (FAT12, FAT16, FAT32, and FAT64) • ext (EXT2, EXT3 and EXT4) • ufs1 (UFS1, UFS2) • vhd • extx (EXTX)
Drive Type	• USB flash drives • USB hard drives • SATA hard drives • IDE hard drives • Memory cards (CF, SD, SDXC etc.)

Logical Extraction – File Type Categories	• Picture (169) • Document (129) • Camera • Audio (43) • Email (12) • Cryptography (28) • Video (139) • Archive (54)
Logical Extraction - Extended File Type Categories	• 3D • Code • Data • Database • Disk image • E-book • Executable • System
System Information*	• User information • Connected networks • Installed programs • OS install information • USB history • Run commands • Recent applications • Default applications • Recent files • Typed paths • User assist data • Hardware **The availability of certain features may vary for macOS devices*
Password Extraction*	• FileZilla • Firefox

	• Mozilla • Thunderbird • Google Chrome • Opera • Windows Vault • Microsoft Edge **The availability of certain features may vary for macOS devices*
File Carve – File Signatures*	• Picture (169) • Document (129) • Camera • Audio (43) • Email (12) • Cryptography (28) • Video (139) • Archive (54) • 3D • Code • Data • Database • Disk image • E-book • Executable • System **The availability of certain features may vary for macOS devices*
Investigative Quick Wins Profiles	For rapid results, choose Field Triage. Simply connect the tool to a target device, and, in a few steps, a forensic examiner can have access to valuable insights, significantly speeding up the investigative process and increasing the possibility of an instant conviction. **Run Stock Profile:** Recent: • Recent documents • Recent pictures

	• Recent videos Phones: • Phone Backups User: • User desktop • User downloads • Microsoft Office files history • Windows 10 timeline • WaitList.dat file File Types: • RAW camera images • All email files • All torrent files • ASD stream Apple: • iTunes Lockdown file • OSX keychains • Terminal logs (OSX) • OSX iCloud • OSX global preferences • OSX user preferences • OSX Trash Windows: • Event logs • Temporary files • Jump list files • Registry hives and hive backup • AmCache files • App compatibility cache • Setup API dev log directory • Windows Recycle Bin

MEDIA ACQUISITION

FOR USB DEVICES AND REMOVABLE MEDIA

Media Acquisition, a key component of our award-winning Unified Digital Forensics Platform, is a rapid, automated, and user-friendly forensic acquisition tool. It efficiently extracts data from a wide range of removable media including USB devices, SD and micro SD cards, portable external drives, as well as IDE and SATA drives, CDs, DVDs, and Blu-ray discs. Trusted globally by law enforcement teams, military units, intelligence agencies, and major enterprises, Media Acquisition is renowned for reducing investigation backlogs.

Designed for both field operatives and lab analysts, Media Acquisition offers an intuitive interface that swiftly acquires and analyses data from multiple devices. Its real-time data viewing capability and patented red-amber-green alert system enable users to make informed decisions on the spot.

Key features

- Simultaneously secure and analyse data from multiple removable devices.
- Use advanced inspection tools to view a target's file tree before extraction.
- Get live views of logical data as it streams into the platform.
- Recover deleted data using powerful carving tools.
- Acquire data from hard drives removed from damaged systems.
- Receive automated alerts about suspicious data with Detego's patented red-amber-green visual alert system.
- Automate data analysis based on pre-defined criteria such as hash values, keywords, levels of nudity, face watchlists, and more.
- Focus on data that's relevant to investigations by triggering selective artefact extractions.
- Forensically image target devices in Ex01, E01 or DD formats.

MEDIA ACQUISITION TECHNICAL DETAILS

Extraction Jobs	• System information • Internet artefacts • Password finder • Logical extraction • File carve • Physical image Extraction Targets • Physical disk – Acquires data from a disk and all partitions • Mounted drive – Acquires data from a single partition • Image file – Acquires data from a pre-imaged device • Directory – Acquires files from within a specified directory • Mobile and tablet – Acquires data from mobile and tablet devices • Network agent – Acquires data from a remote device
Imaging Formats	• Ex01 • E01 • DD

E01/Ex01 Compression	• No compression • Best compression • Fast compression
Hash Verification	• MD5 only • MD5 and SHA1 • MD5 and SHA256
Software Write Blocking	Optional
Logical Extraction Parameters	• Date and time (or regardless of) • Recent timestamps • File size: larger than, less than, between
File Systems	• ntfs (NTFS) • iso (ISO9690 CD) • hfs (HFS and HFS+) • APFS (DD images only acquired from non-chipped Apple hardware) • raw (raw data) • swap (swap space) • memory (RAM data) • FAT (FAT12, FAT16, FAT32 and FAT64) • ext (EXT2, EXT3 and EXT4) • ufs1 (UFS1, UFS2), • vhd, • extx (EXTX)
Drive Type	• USB flash drives • USB hard drives • SATA hard drives • IDE hard drives • CDs/DVDs • Memory cards (CF, SD, SDXC etc.)
Logical Extraction – File Type Categories	• Picture • Camera

	• Document • Audio • Email • Cryptography • Video • Archive
Logical Extraction – Extended File Type Categories	• 3D • Code • Data • Database • Disk Image • E-book • Executable • System
System Information	• User information • Connected networks • Installed programs • OS install information • USB history • Run commands • Recent applications • Default applications • Recent files • Typed paths • User assist data • Hardware
Password Extraction	• FileZilla • Firefox • Mozilla • Thunderbird • Google Chrome

	• Opera • Windows Vault • Microsoft Edge
File Carve – File Signatures	• Picture (169) • Document (129) • Camera • Audio (43) • Email (12) • Cryptography (28) • Video (139) • Archive (54) • 3D • Code • Data • Database • Disk image • E-book • Executable • System
Intuitive Interface	The Detego Analyse Viewer provides an easy-to-use gallery panel for investigators to examine and apply tags to all acquired data. Media Acquisition also has an inbuilt omni-viewer capable of opening and viewing acquired files, irrespective of the format.
Simultaneous Imaging and Analysis	A single case can often have multiple exhibits; use Media Acquisition to speed up the investigative process by imaging and analysing multiple removable devices at once.
Speed	Define the logical acquisition parameters to extract all files, or target individual artefacts such as pictures, videos, documents, and emails to fast-track investigations.
Recover Deleted Data	A core benefit of the Detego platform is that carving can be performed on multiple exhibits simultaneously.
Flexibility	Use one single tool to acquire data from multiple types of removable media, including SD cards, micro SD cards, hard drives, image files, and many more.

	The system also supports the ingestion of E01 and Ex01 forensic images created by Digital Intelligence TX1 Imager devices.
Simple-To-Use	Plug and play functionality with simple options that yield rapid results for both technical and non-technical users.

FUSION

ADVANCED LINK ANALYSIS ACROSS DIGITAL EXHIBITS

Fusion enables investigators to leverage advanced link-building capabilities to expose connections between people, places, devices, and cases.

Key features:

- Connect the dots and expose hidden links across digital exhibits.
- Access file properties, internet artefacts, communication history (email addresses, call events, contacts, messages, credentials, etc.), device information, financial data, and keywords to rapidly identify and link suspects.
- Filter data using thousands of preconfigured variables, including GPS coordinates, hash matches, and EXIF data.
- Instantly view links that exist between cases by using its visual preview functionality.
- Create custom whitelists to prevent displaying known/approved links.
- Get users up and running with a minimal training overhead thanks to its intuitive user interface.

Key Product Features in Detail	• **Intuitive interface:** The easily navigable interface allows users to choose the cases they want to link to and the areas in which they want to find the links. • **Visual previews:** Instantly view the number of links that exist between any two cases. • **Group links by type:** Drill down into links grouped by type and examine items such as all the messages exchanged between two individuals, identical files that exist in two exhibits, etc. • **Ignore unwanted links:** Upload whitelists to prevent links that have been given the OK from displaying.
File Properties	Links file hashes, file names, EXIF metadata from 2 or more exhibits regardless of device type, e.g., an iPhone or a Windows laptop.
Internet Artefacts	Links files by URLs, remote IP addresses, search terms
Communications	Email addresses, call events, contacts, messages, credentials
Device Properties	MAC addresses, device serials, installed applications

Finance	Bank cards
Keyword Match	Exhibit keyword matches
Whitelist Files	Removes known linked files such as system files and OEM program files to declutter linkage to just user-generated data (the NRSL dataset, for example).

ANALYSE AI+

ADVANCED ANALYTICS, INTELLIGENT WORKFLOW AUTOMATION, AND COURT-READY REPORTS

Detego Analyse AI+ is a powerful analytical platform that integrates forensic acquisitions from Detego solutions and third-party tools, harnessing advanced AI analytics and automation to conduct in-depth analyses, uncover forensic evidence, and generate court-ready reports.

- Fast-track evidence discovery with advanced analytical workflows and swift text and keyword matching.
- Utilise AI-powered face recognition to sift through vast image and video datasets, identifying suspects, witnesses, and persons of interest in seconds (Analyse AI+ detects over 20 faces per second, 4x faster than the industry average).
- Instantly detect AI-generated pictures and videos by conducting swift metadata analysis.
- Benefit from faster evidence processing with up to 5x faster extraction for DD images without hash-matching (3x with hash-matching) and up to 4x faster for E01 images without hash-matching (1.5x with hash-matching).
- Minimise manual data sifting with AI-powered semantic search, rapidly identifying broader concepts and contexts such as “distressed children”, “masked men holding weapons at night”, or “screenshots of customer account details”.
- Leverage AI-powered detection tools to swiftly identify critical content such as weapons, drugs, nudity, indecent images, and more in record time.
- Match locations and objects with powerful image search tools, using reference images or the “show similar” feature to detect specific signs, symbols, movements, patterns, and designs.
- Extract text crucial to investigations from pictures and videos with Analyse AI+’s multi-language Optical Character Recognition (OCR) feature.
- Translate and transcribe audio and video content from 50+ languages to English at speeds exceeding 1,000 words per minute.
- Run offline document translation to translate text from over 100 languages into English, or conduct cross-language translations.
- Pinpoint modified images using the PhotoDNA matcher, identify altered content, or match images with hash values relevant to investigations.
- Decrypt passwords and access encrypted files in over 300 formats, including Word documents, locked Zip files, phone backups, and more.
- Redact sensitive data across a range of documents including PDFs, DOCX files, PPTXs, JPGs, other popular picture formats, and more (currently in BETA mode).

- Export communications including chats, text messages, emails, and more in RSMF format for efficient review in Relativity.
- Enhanced BitLocker support enables decryption of forensic images with multiple partitions, including mixed encrypted and unencrypted volumes secured by different keys. Detego now automates the process by adding a Decryptor job on image selection, requiring only the known key.
- New support for the .ctm1 format enables more targeted analysis with smaller mapping regions. Both .ctm1 and .mbtiles formats are available offline for uninterrupted access.
- Uncover hidden files with advanced steganography detection tools.
- Perform AI-powered analytical workflows offline, ensuring greater data security.

Detego Analyse AI+ Automation	With automation at its core, the Detego Analyse AI+ platform enables investigators to better focus their time and efforts by taking on complex and manually intensive tasks. In just a few clicks, you can set up a customised workflow ready to acquire, analyse, and generate detailed reports on intelligence taken from digital media. Simply connect the device to the machine running Detego Analyse AI+, select the necessary workflow, and let the software take care of the rest.
Benefits of Detego Automation	• A reduced backlog of digital forensic cases. • Reduced complexity of the digital forensic process. • Better utilisation of highly skilled and experienced workforce. • Ensures a fully compliant evidential chain equating to court-ready evidence. • Significant cost and efficiency savings. • Faster convictions and more guilty pleas. • Increased speed of investigations.
Notable Analytical Processes	**AI Face Recognition and Face Watchlists:** Accelerate investigations with highly accurate face recognition watchlists. Easily upload photos of suspects, witnesses, or victims, and match them against images and videos in seconds. When used on a standard laptop/computer, our rapid matching technology identifies over twenty faces per second, 4x faster than the industry average.

	Investigators can also pinpoint persons of interest faster with Analyse AI+'s advanced semantic search. Add filters to face recognition to identify persons in specific locations, performing certain actions, holding objects, or displaying particular emotions. For example, find a suspect pointing a gun at another person, identify someone loading people into a boat, or recognise a distressed child in a warehouse. **AI-Generated Picture and Video Detection:** As AI-generated images and videos become increasingly prevalent in investigations, Analyse AI+ introduces a new AI Image Detector. This workflow helps investigators quickly identify AI-generated content by analysing metadata, providing accurate results in seconds. **Semantic Search:** Don't be limited by keywords; use AI-powered semantic search to identify specific concepts and contexts within your image and video evidence. Rapidly identify broader concepts like "men in masks with automatic weapons in London at night", "drug deals in a black sports car belonging to a specific brand", "screenshots of customer account details", "uniformed teams holding flags with terror-related symbology", and more. **Semantic Text Searching:** Find relevant evidence based on meaning, context, and sentiment rather than relying solely on exact keyword matches. By understanding the intent behind a search, Detego Analyse AI+ can surface relevant chats, emails, documents, and other text-based evidence even when the exact search terms do not appear within the content. **AI-powered Similar Image Identification:** Tap into powerful similar image search capabilities by uploading reference images or simply use the "show similar" feature on existing images. Quickly match anything from specific locations, signs, movements, and objects through to patterns or designs on wallpaper, graffiti or clothes. **AI Transcription and Indexing:** Save time by automating the conversion of audio to text. Use the new AI transcription feature to accurately transcribe and index words from audio and video files such as voice notes, video messages, social posts, and voicemails in minutes. Achieve transcription speeds that are well over 1,000 WPM. Eliminate the need to review hours of audio and video recordings manually. Identify data related to investigations by using advanced text and keyword matching capabilities on the data indexed from audio/video files.

	Real-time AI translation: Go beyond offline document translation and unlock the power of live AI translation for audio and video content. You can now translate videos and audio in 100+ languages to English in real time, facilitating efficient international and cross-border investigations. **AI-powered Offline Language Translation:** Detego Analyse AI+ includes an all-new AI-powered Detego offline translator which replaces the GIST translator found in previous versions. Supporting 100 languages (see supported languages below), this feature allows users to conduct swift and accurate cross-language translations, enhancing accessibility and facilitating efficient multi-region/cross-border investigations. **Picture and Video Analytics:** Detect objects of forensic interest contained within digital images and video files. By using advanced AI, this engine can detect specific items like weapons, drugs, passports, and vehicles. This analytical process considerably reduces the time an examiner spends manually viewing images, allowing them to perform other critical investigative tasks. By using advanced artificial intelligence, this engine can detect specific objects contained in images and create the respective tags that are useful for forensic investigations. Such objects include weapons, drugs, vehicles, people, human faces, bicycles, motorcycles, trains, license plates, cattle, laptops, drones, and PCB. **Indecent Image Detection:** By using advanced artificial intelligence, this engine can process media and detect any forms of indecency, such as nudity, in the respective media files, and create the respective tags, which are useful for forensic investigation. The module also detects images of school-age children, as well as babies and toddlers. **Symbol Detection:** By using advanced artificial intelligence, this engine can process media and detect any forms of symbols, such as terror-related symbols, and create the respective tags, which are useful for forensics investigations. **Multi-Language Optical Character Recognition (OCR):** Normalise items like signs, number plates, screenshots, and scans into digital writing so that otherwise hidden data can be rapidly keyword searched and matched.

	This plugin enables the conversion of different types of media files into English text based on multiple languages such as French, Arabic, Russian, Spanish, Kiswahili, Swedish, and Urdu, among other languages, so that any keywords can be rapidly searched and eventually matches created. **PhotoDNA:** Designed by Microsoft, this technology gets around negative hash matches by comparing the similarities between images in a pixel-by-pixel manner. Scans images for PhotoDNA hash matches and tags items that contain similarity matches. **Video Frame Processor:** Scan the content of an exhibit's video files, compose visual content into still frames at specific pre-defined intervals, and analyse the JPEG images generated from the captured frames for incriminating evidence using other analytical processes. **EXIF Processor:** Uncover EXIF metadata embedded in image files created by any camera, including mobiles and smartphones. Discover camera data, initial capture time, phone model, operating system, geographic location (longitude and latitude), and much more. **UAV Processing:** Parse information from numerous types of UAV, including DJI Phantom 3, Phantom 4 Pro, Inspire 1, and Mavic Pro drone models, as well as Drone Forensics Software like V2 and CFID devices. The data is extracted using Detego Media Acquisition and can be immediately processed to view interactive maps of routes flown, take-off location details, payload drop-off, power usage, and more. **Passware Integration:** We have partnered with Passware to integrate its industry-leading solution fully into the Detego Unified Forensics Platform. This partnership allows users to seamlessly identify encrypted evidence and recover and break through passwords from 250+ file types, all from one platform. **YARA-Based Scanning:** Quickly identify files, memory artefacts, and backup data that may contain malware, malicious code, or indicators of compromise. By automatically scanning digital evidence against custom YARA rules, investigators can swiftly surface suspicious content for further examination, reducing manual review and accelerating threat-focused investigations.

	Hundreds More Features: • Threaded messaging views • Cached webpage rebuilder • Lucene text indexing • Standalone reports • Enhanced evidence viewer • Rule-based access rights • Centralised case management • Automated reporting • Tag and index all extracted items • Deleted data carving • EWF and DD imaging • MD5 and SHA1 hash-matching • Advanced keyword analysis • Steganography detection • Parse data from hundreds of apps • KML exporter for mapping

ANALYSE AI+ TECHNICAL DETAILS

Automated Job Processing	Create and save custom job queues to acquire, process, and report on data. (See the Media Acquisition section)
Memory Ingestion	Ingests and analyses memory files: • .mem • .bin • Swapfile • Pagefile • hiberfil
Memory Analysis	Perform the parsing of: • URLs from memory files • Emails from memory files

	• MAC addresses from memory files • IPv4 from memory files • IPv6 from memory files • GPS from memory files • Telephone numbers (UK) from memory files • Telephone numbers (US) from memory files • Credit card numbers (Visa) from memory files • Credit card numbers (Mastercard) from memory files • Credit card numbers (Amex) from memory files • Credit card numbers (Diners Club) from memory files • Credit card numbers (Discover) from memory files • Credit card numbers (JCB) from memory files
Imaging Formats	• Ex01 • E01 • DD
Forensic Image Verification	Supported
Analyse App Data (Computer)	Performs the analysis of application (app) data extracted and parsed from popular social networks • Messengers • Web browsers • Navigation • Productivity • Travel • Finance • Fitness • Multimedia apps
Analyse App Data (Mobile)	Performs the analysis of mobile application (app) data extracted and parsed from popular social networks • Messengers • Web browsers • Navigation

	• Productivity • Travel • Finance • Fitness • Multimedia apps
Text Analytics	Performs analysis on the respective indexed text, e.g., document content, and classifies it based on language, sentiment, and key themes. **Key Phrases Analysis (Documents):** Processes the contents of documents to determine key phrases in the body of text by analysing the frequency of word appearance and its co-occurrence with other words in the text. **Language Classification (Documents):** Applies language classification to documents based on the most dominant languages found within the text and supports 176 languages. • Afrikaans • Albanian • Alemannic German • Amharic • Arabic • Aragonese • Armenian • Assamese • Asturian • Avar • Azerbaijani • Bashkir • Basque • Bavarian • Belarusian • Bengali • Bihari • Bishnupriya Manipuri • Bosnian • Breton • Bulgarian • Burmese • Buryat • Catalan • Cebuano • Central Bikol • Chavacano • Chechen • Chinese • Chuvash • Cornish • Corsican • Croatian • Czech • Danish • Doteli

	• Dutch • Emilian-Romagnol • Erzya • Estonian • Finnish • Galician • German • Guarani • Haitian Creole • Hill Mari • Hungarian • Ido • Indonesian • Interlingue • Italian • Javanese • Kannada • Karachay-Balkar • Khmer • Konkani • Kurdish • Lao • Latvian • Lhasa Tibetan • Lithuanian • Lombard • Lower Sorbian • Macedonian • Malagasy • Malayalam • Maltese	• Egyptian Arabic • English • Esperanto • Fiji Hindi • French • Georgian • Greek • Gujarati • Hebrew • Hindi • Icelandic • Ilocano • Interlingua • Irish • Japanese • Kalmyk Oirat • Kapampangan • Kazakh • Komi • Korean • Kyrgyz • Latin • Lezgian • Limburgish • Lojban • Low German • Luxembourgish • Maithili • Malay • Maldivian • Manx

	• Marathi • Meadow Mari • Mingrelian • Mongolian • Neapolitan • Newar • Northern Luri • Occitan • Ossetian • Palatine German • Piedmontese • Portuguese • Quechua • Romansh • Russian • Sardinian • Scots • Serbo-Croatian • Sindhi • Slovak • Somali • Spanish • Swahili • Tagalog • Tamil • Telugu • Turkish • Tuvan • Upper Sorbian • Uyghur • Venetian	• Mazanderani • Minangkabau • Mirandese • Nahuatl • Nepali • North Frisian • Norwegian • Odia • Pashto • Persian • Polish • Punjabi • Romanian • Rusyn • Sanskrit • Scottish Gaelic • Serbian • Sicilian • Sinhala • Slovene • South Azerbaijani • Sundanese • Swedish • Tajik • Tatar • Thai • Turkmen • Ukrainian • Urdu • Uzbek • Veps

	• Vietnamese • Walloon • Welsh • West Frisian • Wu Chinese • Yiddish • Yue Chinese • Volapük • Waray • West Flemish • Western Punjabi • Yakut • Yoruba • Zaza **Sentiment Analysis (Messages):** Performs analysis of messages where the content is identified on a scale of positive to negative. Messages can then be filtered on the calculated sentiment. **Cryptocurrency Identification (Documents/Messages):** Identifies Bitcoin addresses within text and extracts them as separate evidence records. Address checksums are validated to remove false positives and support Bech32 and Base58 encodings.
AI Transcription and Translation	**Languages supported for AI transcription and translation of audio and video content.** • Afrikaans • Amharic • Armenian • Azerbaijani • Basque • Bengali • Breton • Burmese • Chinese • Czech • Dutch • Estonian • Finnish • Galician • Albanian • Arabic • Assamese • Bashkir • Belarusian • Bosnian • Bulgarian • Catalan • Croatian • Danish • English • Faroese • French • Georgian

	• German • Haitian • Hawaiian • Hindi • Icelandic • Italian • Javanese • Kazakh • Korean • Latin • Lingala • Luxembourgish • Malagasy • Malayalam • Maori • Modern Greek (post 1453) • Nepali (macrolanguage) • Norwegian Nynorsk • Panjabi • Polish • Pushto • Russian • Serbian • Sindhi • Slovak • Somali • Sundanese • Swedish • Tajik • Tatar • Thai	• Gujarati • Hausa • Hebrew • Hungarian • Indonesian • Japanese • Kannada • Khmer • Lao • Latvian • Lithuanian • Macedonian • Malay (macrolanguage) • Maltese • Marathi • Mongolian • Norwegian • Occitan (post 1500) • Persian • Portuguese • Romanian • Sanskrit • Shona • Sinhala • Slovenian • Spanish • Swahili (macrolanguage) • Tagalog • Tamil • Telugu • Tibetan

	• Turkish • Ukrainian • Uzbek • Welsh • Yoruba • Turkmen • Urdu • Vietnamese • Yiddish
AI-powered Offline Language Translation	**Languages supported for AI-powered Offline Language Translation** • Afrikaans (af) • Arabic (ar) • Azerbaijani (az) • Belarusian (be) • Bengali (bn) • Bosnian (bs) • Cebuano (ceb) • Welsh (cy) • German (de) • English (en) • Estonian (et) • Fulah (ff) • French (fr) • Irish (ga) • Galician (gl) • Hausa (ha) • Hindi (hi) • Haitian; Haitian Creole (ht) • Armenian (hy) • Igbo (ig) • Icelandic (is) • Japanese (ja) • Georgian (ka) • Central Khmer (km) • Amharic (am) • Asturian (ast) • Bashkir (ba) • Bulgarian (bg) • Breton (br) • Catalan; Valencian (ca) • Czech (cs) • Danish (da) • Greek (el) • Spanish (es) • Persian (fa) • Finnish (fi) • Western Frisian (fy) • Gaelic; Scottish Gaelic (gd) • Gujarati (gu) • Hebrew (he) • Croatian (hr) • Hungarian (hu) • Indonesian (id) • Iloko (ilo) • Italian (it) • Javanese (jv) • Kazakh (kk) • Kannada (kn)

	• Korean (ko) • Ganda (lg) • Lao (lo) • Latvian (lv) • Macedonian (mk) • Mongolian (mn) • Malay (ms) • Nepali (ne) • Norwegian (no), • Occitan (post 1500) (oc) • Panjabi; Punjabi (pa) • Pushto; Pashto (ps) • Romanian; Moldavian; Moldovan (ro) • Sindhi (sd) • Slovak (sk) • Somali (so) • Serbian (sr) • Sundanese (su) • Swahili (sw) • Thai (th) • Tswana (tn) • Ukrainian (uk) • Uzbek (uz) • Wolof (wo) • Yiddish (yi) • Chinese (zh)	• Luxembourgish; Letzeburgesch (lb) • Lingala (ln) • Lithuanian (lt) • Malagasy (mg) • Malayalam (ml) • Marathi (mr) • Burmese (my) • Dutch; Flemish (nl) • Northern Sotho (ns) • Oriya (or) • Polish (pl) • Portuguese (pt) • Russian (ru) • Sinhala; Sinhalese (si) • Slovenian (sl) • Albanian (sq) • Swati (ss) • Swedish (sv) • Tamil (ta) • Tagalog (tl) • Turkish (tr) • Urdu (ur) • Vietnamese (vi) • Xhosa (xh) • Yoruba (yo) • Zulu (zu)

Analyse App Data (Windows and Mac)	Performs the analysis of Windows and macOS Application's data found in the respective exhibit; includes: **Windows:** • Recycle bin • Windows event logs • Jump lists • Microsoft Excel • Microsoft Word • Microsoft PowerPoint • AmCache • AppCompatCache • Windows 10 timeline • Setupapi.dev.log • USB user • Windows EDB • Link files (.lnk) • Open/save MRU • SRUM (System Resource Usage Monitor) • BAM (Background Activity Moderator) • Start menu search • WinRAR • 7-Zip • Adobe Reader • Windows mail app • Volume shadow copy • WhatsApp desktop app • Chrome desktop browser • Mozilla desktop browser • Internet Explorer • Cortana • Microsoft Edge

	• UC browser • Microsoft Edge – Chromium • Opera browser • Signal desktop app • Skype • VLC **macOS:** • Quarantine events • User preferences • Bash history • Dock • Global preferences • Internet accounts • Login info • Event logs • Trash • Spotlight shortcuts
Video Frame Processor	This analysis process scans video file contents in the exhibit and produces frames at the specified regular intervals.
OCR (image to text)	The Optical Character Recognition (OCR) analysis method extracts textual data from pictures and indexes it for eventual searching and keyword matching. It supports the following 103 languages: • Afrikaans • Albanian • Amharic • Arabic • Armenian • Assamese • Azerbaijani • Bengali • Basa Jawa • Basa Sunda • Basque • Belarusian • Bisaya • Bosnian • Breton • Bulgarian • Burmese • Catalan/Valencian • Cherokee • Chinese (simplified)

	• Chinese (traditional) • Croation • Danish • Dutch/Flemish • Esperanto • Faroese • Finnish • Gaelic/Scottish Gaelic • Georgian • Greek • Hebrew • Hungarian • Indonesian • Irish • Japanese • Kannada • Khmer • Korean • Lao • Latvian • Lithuanian • Macedonian • Malayalam • Māori • Mongolian • Occitan • Persian • Portuguese • Romanian • Sanskrit • Sinhala	• Corsican • Czech • Divehi • English • Estonian • Filipino • French • Galician • German • Gujarati • Hindi • Icelandic • Inuktitut • Italian • Javanese • Kazakh • Kiswahili • Kyrgyz • Latin • Lea Faka-Tonga • Luxembourgish • Malay • Maltese • Marathi • Nepali • Odia • Polish • Pushto/Pashto • Russian • Serbian • Slovak

	• Slovenian • Swedish • Tajik • Tatar • Thai • Tigrinya • Ukrainian • Uyghur • Vietnamese • Western Frisian • Yoruba • Spanish • Syriac • Tamil • Telugu • Tibetan • Turkish • Urdu • Uzbek • Welsh • Yiddish
Text Indexing	This analytical process performs indexing of all evidence items in the respective exhibit, including textual content from documents, pictures, and audio, which enables eventual searching and keyword matching. Supported file formats include: **Documents:** • Word Documents (Office 2007+) • Excel Documents (Office 2007+) • PowerPoint Documents (Office 2007+) • Microsoft OneNote Documents • Word Documents (Office 97-2003) • Excel Documents (Office 97-2003) • PowerPoint Documents (Office 97-2003) • OpenOffice/LibreOffice Documents • Rich Text Documents • PDF Documents • General Markup Documents • Plain Text Documents **Emails:** • Outlook EML files • Outlook/Exchange MSG files • Outlook/Exchange OST or PST files

	Databases: • ESE database files • SQLite database files **Operating System:** • Event log files • Jump lists • Registry hive files • Memory dump files • Windows shortcuts • NTFS Change • Internet Explorer history files • PList and binary PList files **Others:** • E-Books in EPUB format • VCard files • Unknown file types (using Apache Tika) • Unknown file types (using binary strings scan) • Fallback to binary strings scan
File Header Checking	File header checking detects potential manipulation of file extension to disguise the true file. It identifies any mismatch between its named file extension and the actual file content.
Keyword Matching	Keyword matching enables the scanning of all the indexed evidence items, including pictures and documents, for matches against the selected keyword list. The respective matches are tagged with the item ID and the respective keywords that were matched. • Performs keyword matching from a single selectable keyword list • Performs keyword matching from multiple selectable extant keyword lists concurrently • Allows the creation of a new keyword list • Allows the configuration of an existing keyword list
Hash-matching	Matches evidence file hashes against pre-known hash data sets. It can be used to categorise safe/ignorable files or flag known 'bad' files. Supported hashes include MD5 and SHA1 hash list.

PhotoDNA	Performs PhotoDNA hashing and subsequent tagging (repeated).
EXIF Processor	Performs scanning of file contents in the respective exhibit for any presence of EXIF metadata.
Compound File Extractor	Performs data extraction from compressed files such as .zip, .rar, among others.
OCR (image to text)	Performs OCR (image to text).
Steganography Detection	Performs scanning of file contents in the respective exhibit to check for any steganography.
Drone Parser	Performs drone data parsing.
RSMF Exporter (Relativity)	Exports chats, text messages, and emails directly into RSMF format. This streamlines the review and analysis of communication data, improving overall case management for those using Relativity.
AI Generated Image Detector	This workflow helps investigators quickly identify AI-generated pictures and videos by analysing metadata, providing accurate results in seconds.
Redaction Editor (BETA)	Redact sensitive data across a wide range of file types, including: *.pdf, .doc, .docx, .dotx, .rtf, .txt, .ppt, .pptx, .jpg, .jp2, .png, .bmp, .webp, .tiff* Easily manage confidential information with options to undo, redo, edit, group, or delete redactions as needed.
Exhibit Comparison	The platform includes a forensic comparison tool designed to identify state changes on a device by comparing a baseline exhibit to a post-deployment snapshot. This system generates a merged exhibit using colour-coded tags for the rapid identification of modifications between the two points in time. Items within the comparison are categorised based on their status: • **No Change:** Items that are identical in both exhibits. • **Removed:** Items identified in the baseline but absent from the post-deployment snapshot. • **Added:** Items not present in the baseline but detected in the post-deployment snapshot. • **Changed:** Items present in both exhibits that demonstrate modified content or metadata properties.

FILTERING AND SORTING EXHIBIT DATA

Emails	Including but not limited to: • Email • Email cc • Email to • Date and time • Source
Device	Including but not limited to: • Make • Model • Serial numbers • Front/back camera
File Property and Metadata	Including but not limited to: • Accessed • Altitude • Author • Created • LastAccessedTimestamp • LastAutoConnectTimestamp • LastConnectTimestamp • LastDetectedTimestamp • LastUpdatedTimestamp • LastUseTimestamp • LastViewedTimestamp • LastVisitedTimestamp • Location • Longitude • MacAddr

	• EXIFdata KeyPhrases • Keyword • KeywordListName • Latitude • Make • Model • Modified • Publisher • ReadTimestamp • RealExtension • ReceivedTimestamp • Recipient • RequiresBruteForce • Sender • SentTimestamp • SerialNumber • Size • Source • Subject • Tags • Time • Timestamp • Topic • UserInput • Username • VisitCount • FileSystem
Document Metadata	**Common** • Content-Type • Content-Length

	• resourceName **Dates** • Creation-Date • Last-Modified • dcterms:created • dcterms:modified **Author/Producer** • producer **PDF Specific** • pdf:PDFVersion • pdf:docinfo:creator • pdf:docinfo:producer • pdf:encrypted • pdf:hasXFA • pdf:hasXMP **Office documents** • Template • meta:save-date • cp:revision • meta:character-count • meta:character-count-with-spaces • meta:print-date **Security** • Access Permission: Modify • Access Permission: Extract