STRIKE™ v1.22
Technical Specifications

Rapid, automated digital media exploitation

STRIKE™ (System for TRIaging Key Evidence™) is an extremely fast, accurate and easy-to-use digital media exploitation kit.

STRIKE™ is designed to assist Special Operations Forces, Law Enforcement Officers, Homeland Security Personnel and Counterintelligence / Human Intelligence Agents conducting digital evidence collection and analysis activities with little to no training.

Non-technical operators are provided with a portable, automated system to rapidly extract data and analyze information, in-field in real-time, from captured digital devices and media in a forensically sound manner. Some examples include USB flash drives, multimedia cards, SIM cards, cell phones, CDs/DVDs, portable media players, hard drives and computers.

The self-contained kit is well suited for counterterrorism operations, force protection activities, interrogations, checkpoint screenings and criminal investigations, where time is of the essence.

STRIKE™ is the only digital evidence capture and triage device of its kind, designed for speed and simplicity, providing actionable intelligence within minutes - not hours, days or weeks.

12633 Challenger Pkwy, Suite 270, Orlando, FL 32826
[P] 407.999.9870 • 877.433.2526 | [F] 407.999.9850 | strike@keywcorp.com

w w w . k e y w c o r p . c o m

Rev. G

v1.22 - What's New

- All new browser support:
  - Added analysis of Firefox, Chrome, Safari and new versions of Internet Explorer
  - Added real time web cache reconstruction for all supported browsers
  - Added separate reports for user web browsing history, including web searches, social media and mapping activity
- User Experience updates:
  - User may customize default home screen and sessions view
  - Current session name and media type now visible in screen title of all session views
  - Administration tab order has been reorganized for more efficient user interaction
- Added ability to automatically perform triages on newly connected media
- Added ability to export (to a .zip) items in all listing and thumbnail views
- Added targeting and analysis support for WebP image type and WebM video file type
- Path prioritization analyzes user data first
- Updated known good and known bad hash sets
- Updated coreference database
- Updated virus definitions
- Provided Mission Plans no longer extract XML files by default to eliminate extraneous results
- New and improved hardware support

Supported Devices / Media

- USB 1.0, 2.0 and 3.0 flash drives
- IDE, SATA and SCSI hard drives
- FireWire (IEEE 1394), PCMCIA (including ExpressCard) and USB hard drives
- GSM SIM cards
- Memory cards
  - Compact flash (type 1 and 2)
  - Secure digital cards (high capacity SDHC, extended capacity SDXC, miniSD and microSD with additional adapters)
  - xD-picture cards
  - Memory sticks (Sony, PRO, DUO, PRO DUO, Magic Gate and M2 with additional adapters)
  - MultiMedia cards
  - IBM MicroDrives
- Cell/Satellite Phones
  - Nokia 3120 Tri-band GSM World Phone
  - Thuraya Hughes 7101 Satellite/GSM phone (additional data cable required)
  - Expanded cell phone and SIM card support when using Cellebrite UFED
- CD/DVD/VCDs
- Disk images including uncompressed DD, Expert Witness Compression Format (EWF-E01/S01) and Advanced Forensic Format (AFF)
- Workstation and laptop computers over Ethernet (reboot method)
- Portable audio devices including Apple iPod devices
- GPS Devices including Garmin eTrex HC series

Device / Media Identification and Reporting

- Operating Systems
  - Microsoft Windows 95, 98, NT, 2000, ME, XP, Vista, 7, 8 and 10
    - Including users, installed programs, registered owner and organization and more
  - Linux: Debian, Ubuntu, Red Hat, Fedora and SUSE
    - Including users, logs and more
  - Mac OS
- Support for dual-boot and multi-partitioned systems to include prioritization
- File Systems Supported
  - NTFS
  - FAT12, FAT16 and FAT32
  - EXT2 and EXT3
  - HFS+
  - ISO 9660 levels 1-3 plus Joliet and Rock Ridge (CDs/DVDs)
  - UDF (DVDs)
  - Linux Logical Volumes (LVM 1 and 2)
- Disk images
- Cell phones and SIM cards (IMSI, IMEI and ICCID)

Supported File Types for Analysis

- Documents
  - Microsoft Office – Word, Excel and Power Point
  - OpenOffice – Writer, Calc, Impress and Math
  - Portable Document Format (PDF)
  - Plain text (including ASCII, UTF-8, UTF-16 and ISO 8859)
  - Rich Text Format (RTF)
  - eXtensible Markup Language (XML)
  - Electronic Business Card
  - NMEA log files
- Email
  - Microsoft Outlook and Outlook Express
  - Microsoft Windows Address Book
  - Netscape
  - Email message (RFC822 and MBOX format)
- Internet
  - HyperText Markup Language (HTML)
  - Microsoft Internet Explorer, Mozilla, Firefox, Chrome, Safari and Netscape history formats
- Images
  - GIF, JPEG, TIFF, BMP, PNG, PPM,PBM and WebP
  - OpenOffice – Draw
- Databases
  - Microsoft Access
  - Comma Separated Values (CSV)
  - SQLite 3.0
  - Apple .plist
  - Windows event logs
  - Registry file for Windows NT
- Audio
  - MP3, M4A, WMA, OGG, WAV and more
- Video
  - MPEG, WMV, AVI, Flash, QuickTime, 3GP/3G2, WebM and more
- Archives
  ZIP, RAR, TAR and GZIP for collection with or without analysis

Analysis Capabilities

- Extract both active and deleted files for analysis
  - After the initial triage, running a re-triage will reuse already extracted files to improve performance
  - Iterative searches may be performed after the device or media has been removed
- Carve media for JPEG/GIF images for analysis
- Analyze items for inclusion or exclusion by MD5 hash value
  - Excludes Known Good (STRIKE includes a database of 51 million hashes) and Ignorable (user defined) hash sets
  - Includes and identifies Known Bad and Notable (user defined) hash sets
- Normalize text and image items to a consistent format for analysis
- Find keywords and textual patterns in documents and meta-data
- Identify and categorize NMEA log files
- Identify languages contained in documents (enhanced with STRIKE Advanced)
- Identify and categorize multilingual named entities (Advanced only)
- Provide Co-reference resolution of certain pattern matches and named entities

- Text indexing in all supported languages (enhanced with STRIKE Advanced)
- Detect visual objects in images such as human faces, adult content or text
- Detect steganographic signatures in images
- Extract relevant meta-data from items such as office documents, images (EXIF), video and audio files
  - Identify images with camera-specific EXIF data
- Recursively extract embedded content from compound documents, archives and compressed files
  - Individual email messages are extracted with relationships and attachments intact
  - Images contained in PDF files are extracted
- Detect and identify password protected / encrypted Microsoft Word, Excel, PDF, OpenOffice, MPEG 4 audio (m4p) and Windows Media Audio (wma) files
- Detect and display DTMF within audio/video files
- Reconstruct web page views based upon analysis of web cache content for Internet Explorer, Google Chrome, Safari and Mozilla Firefox.
- Search for GPS coordinates and geodata references (enhanced with STRIKE Advanced)
- Reconstruct email threads from individual email messages
- Generate baseline profiles and perform comparative analysis on computers
- Analyze Cellebrite files
- Registry and Event Log handlers normalize data into plain text for analysis
- Automatic analysis mode allows multiple devices to be queued for analysis

Mission Resources and Planning

- Create, edit, copy, delete, import and export mission plans
- Specify targeting and restriction rules to limit analysis to specific types of files, locations or time ranges
- Enable and adjust the relative score of most parameters including name, path, file type, date ranges, keyword matches and results of image analysis such as detection of faces and adult content
- Create, edit, copy, delete, import and export the keyword and pattern lists contained in the mission
  - Automatic translation of English keywords to other languages using pre-installed Arabic, Persian (Farsi) and Spanish dictionaries
  - Import keyword lists in text, CSV or Excel formats
  - Keywords in particular languages may be disabled without modifying the keyword list
  - Keyword lists will cross reference against Named Entities (with or without translations)
  - Default pattern lists provide the ability to search for formatted dates, credit card numbers, social security numbers and network addresses
  - Pattern lists utilize POSIX regular expressions
- Provide custom “red light” and “green light” messages to the operator when analysis results meet a specified threshold
- Define a global or per-device default mission plan
- Compare mission plans

Evidence Review

- STRIKE provides two different modes to review evidence
  - Expert mode allows full access to control the analysis process and view results
  - Novice mode restricts the operator to a simpler operational scenario and specific mission parameters
- Device or media identification begins automatically when attached and a notification is provided to direct the operator to information as it becomes available
  - Summary device report information is provided with the ability to access more detailed information
  - Device information is updated as it is discovered
- The analysis process is initiated when the operator specifies a mission plan to use
- Items become available for review immediately
- Textual items (listed below) are normalized in the original language, highlighted and additional information is displayed when selected (such as annotations, translations/transliterations and co-reference information)
  - Keyword hits
  - Patterns hits
  - Named Entities
- Advanced search (with indexing turned on) instantly finds content, metadata, file name, score, date, language, flagged/noted or named entity (STRIKE Advanced only) hits available from a dropdown menu
  - Individual searches can be combined for more complex searching and are more robust when using STRIKE Advanced
- Image items are displayed to fit completely on the screen
  - Images may be zoomed and panned
  - Images may be gray scale toggled
  - Simply touch the image to highlight detected faces including orientation
- Video items display thumbnails of screenshots with the optional controls to play the video if supported
- Audio items display an icon with controls to play the audio if supported
- Additional information about the item is available including original path, MD5, score justification and any document meta-data extracted during normalization
- A sortable file system viewer is available
- Navigate to lists of related parent and sibling items when appropriate
- Items may be flagged and annotated for later review
- An item list of flagged/noted files is available for quick review or export to external media
- Individual files may be directly exported to external media with optional anti-virus scan
- All item listings may be sorted by terms that are appropriate for the grouping such as file name, date, score and file size (for List All) or keyword, translation and count (for Items by Keyword)
- Thumbnail gallery of image and video items are available when appropriate
- Items are grouped by various criteria such as score, date, type, language, keyword, keyword list, pattern list and file system
- Special items are grouped by criteria such as deleted, hidden, known bad, notable, virus infected, DTMF, various operating system specific categories, password protected, containers and images with faces, adult content, steganography, web activity, text or camera EXIF data
- Named entities (STRIKE Advanced only) are also grouped in special items under the categories of geopolitical entities, identifiers (Lat/Long, IPv4, phone numbers, money, email, credit card numbers, URL and distance), location, nationality organization, person, product, religion, temporal and title
- Named entities may be sorted by occurrence to discover the most common references on the media
- Lists of items located in the Recycle Bin, My Documents or Desktop are available when appropriate
  - Items recovered from the Recycle Bin will be correlated back to the original user and have the original file name restored when possible
- Certain additional data views become available after the primary analysis completes
  - Any email analyzed is available in a threaded and sortable listing when appropriate
  - A timeline view of file system activity and event logs is available when appropriate
  - Geodata references are plotted on a globe when appropriate
- Items may be securely deleted
- Longer text files may be summarized in the original document language
- Files may be viewed in a Hex Viewer

- The triage session itself may be annotated with additional information including GPS coordinates
- Geodata results are grouped visually on a map and navigable by map view and colored by hit type
- Default views may be defined for session review

Remote After Action Review (Web Interface)

- The web-based interface duplicates most of the functionality listed in the Evidence Review section
- Summary report providing detailed device information, operator notes and the time/date of analysis
- Columns maybe sorted by header title
- Graphical charts summarizing the item distribution by MIME type, score and hash category are available
- Reports of items not analyzed including supported items not targeted, unsupported items and items that failed identification, extraction or normalization are available as appropriate
- Item lists of files not eligible for analysis, items whose score fell below the mission specified threshold and any recovered system files (Microsoft Windows registry, Linux passwd/shadow files, etc.) are provided for review as applicable
- Download disk images generated during analysis

- The following are not available from the Web Interface:
  - Post-triage analysis features such as the email, file system and geodata viewer
  - Editing the file and triage session level annotations
  - The compound and related item views
  - Web cache view

Archive

- The archive is a compressed and optionally encrypted file containing triage session information
- The Microsoft Windows utility constructs a static index of HTML files which duplicates many of the functionality and features available in the Remote After Action Review
- Geodata may be exported in common KML/KMZ formats
- A separate TSV file may be exported that contains a list of all of the files discovered during triage

Local Administration

- Import and export STRIKE mission and triage session data to removable media devices such as flash drives, hard drives, CD/DVD media
- Manage mission planning resources including keyword lists, pattern lists and notable/ignorable hash lists
  - Create, edit, copy, import, export and delete keyword and pattern lists
    - Keyword lists may be imported as plain text, CSV, Microsoft Word, Microsoft Excel or EnCase file
    - Keyword and pattern lists may contain up to 100,000 items
  - Import notable/ignorable hash sets
- Manage triage sessions stored on the local hard drive
  - Triage session archive generation and regeneration
  - Export triage session archives to removable storage devices with optional virus scanning and scrubbing
  - Export disk images created during analysis to removable storage devices
  - Delete one or more triage sessions
  - Import triage session archives from other STRIKEs
- Backup and restore Mission Configuration Archives to duplicate mission plans and resources on another STRIKE
- Securely delete all mission resources and triage sessions
- Generate a baseline profile for use in comparative analysis on computers
- Update STRIKE to use the latest antivirus software, audio and video codecs and known good/bad hash sets
- Update the antivirus definitions via an active internet connection
- Change the default passwords for expert and novice users and the web interface
- Delete items stored on the system that fall below the respective mission plan threshold to free additional space for analysis results
- Toggle the system setting to encrypt and password protect exported triage session archives
- Boot STRIKE into an operating system that appears to be a typical Linux distribution
- Configure network settings for AutoIP, DHCP or static IP addressing

Remote Administration (Web Interface)

- Import and export STRIKE mission plans and mission planning resources via a web browser
- Manage mission planning resources including mission plans, keyword lists and pattern lists
- Change the default passwords for expert and novice users and the web interface
- Backup and restore Mission Configuration Archives to move mission plans and resources to another system
- Delete items stored on the system that fall below the respective mission plan threshold to free additional space for analysis results
- Review network status
- Review information for notable and ignorable hash sets
- Uses a secure network connection

Other Features

- Hard drives, USB drives, memory cards and floppy disks are able to be forensically imaged
- All media and devices are examined in a forensically sound manner
- Update or reset STRIKE from disc media
  - Optionally preserve existing triage sessions, mission plans and resources
  - STRIKE is installed as a 64-bit operating system for enhanced performance
- The STRIKE User's Guide is available on the system
- Instructional information and pictures are provided within the application for identifying and connecting various device/media types
- Zeroize capability (DOD-level erase of STRIKE)
- STRIKE monitors and reports battery usage, storage capacity, connectivity of devices and network status
- Advanced or PIN based login
- Network file shares may be created for import/export and triage of forensic image files.
- The STRIKE display may be viewed on an external device (projectors, monitors, etc)

Advanced Linguistics Analysis

- Available only in STRIKE v1.22 Advanced
- Additional analysis options available in Mission Planning
- Improved Language Identification
- Named Entity extraction, grouping and translation/transliteration
- Improved Co-Reference resolution matching
- Full text indexing in original language
- Enhanced AAR and Archive results
- Improved Foreign Language Display
- Improved Textual Search and File Sorting
- Advanced Geodata analysis for detecting text based locations.

NOTE: STRIKE v1.22 Advanced provides significantly enhanced analysis on the same files that are recovered by STRIKE v1.22 Standard. This provides the end-user with substantially more specific, actionable information to work with in the field.