



Timeline Based Digital Forensics Analysis

Digital forensics is changing rapidly, cyber-attacks are getting more sophisticated and incident response is getting more important. Nowadays, digital forensics analysis is not simply to parse artifacts or recover deleted items. Instead, digital forensics analysts are trying to answer questions like what happened, when, why, how did it happen and if possible also who did it. Adversaries interact and leave footprints everywhere on digital systems. Digital forensics analysts analyze systems for user activity around the time of incidents. Timeline-based digital forensics analysis will help analysts to find various artifacts pointing to the same evidence which will substantiate the same fact and increase overall weight of evidence.

ArtiFast

ArtiFast is the latest solution from Forensafe Software Solutions which can take disks, image files and folders as input to recover artifacts. All artifacts, carved in different formats like plaintext, XML, binary, Registry, encrypted, compound or complex, will go through parsing where forensically valuable time-centric data is extracted. Not all artifacts are the same, thus parsed entries will go through normalization which will help evidence to be organized in a clear and precise way. Extracted data is saved and sorted chronologically in databases. Effective user interface provides efficient searching, filtering, coloring and reporting to digital forensics analysts.

Why ArtiFast?

There are hundreds of events happening every minute on digital systems. The huge amount of data generated by timeline analysis may easily overwhelm digital forensics analysts. Timeline-based digital forensics tools should provide abilities to make investigators job of finding evidence among millions of records easier. To solve this, ArtiFast supports indexing, powerful filtering and searching. ArtiFast provides both "Artifact" and "Timeline" views to digital forensics analysts. Furthermore, ArtiFast handles case management via workspaces to create more efficient analysis environment.

Supports 2100+ Artifacts and Counting
Supports wide-range of Artifact types

Multi OS Support
Supports Windows, Android, iOS, macOS, Linux and File artifacts

Easy Yet Advanced Filtering
Granular filtering through user friendly interface
Ability to write your own filter with easy-to-learn query language

Search Faster
Quick search with flexible data filtering feature

Organized Timeline
Coloring Ability based on Artifact type
Ability to add Bookmarks and Notes

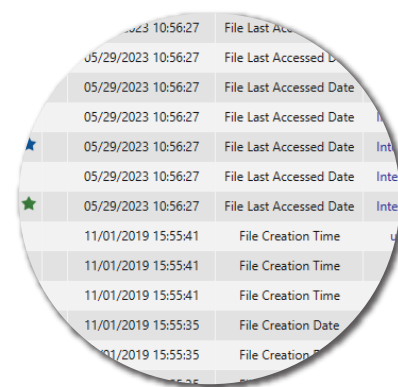
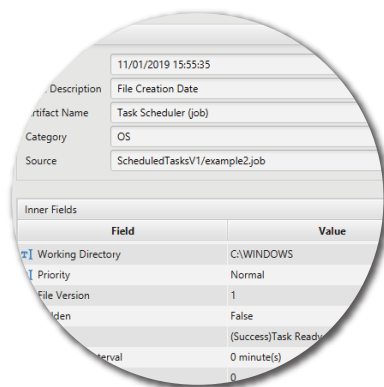
Metadata Parsing
Indexing for over 170 different file types

Content Indexing
File content indexing for over 170 different file types

Integrated File Viewer
Support for hundreds of file types including documents, multimedia and database files

Normalization
More normalized columns than currently available tools

Reporting
Generating 6 different types of detailed and normalized reports



FORENSAFE
SOFTWARE SOLUTIONS

575 Underhill Blvd.
Suite 209 Syosset,
NY 11791 USA

twitter.com/forensafe
linkedin.com/company/forensafe
www.forensafe.com