Online File Signature Database – Overview

April 2008

http://www.filesig.co.uk/

Introduction

The Online File Signature Database (OFSDB) is a bespoke database developed to maintain and improve the quality of File Identification Information[1]. The OFSDB requires that each member has their own username and password.

Database usage/modifications are automatically monitored and recorded in order to provide an audit log for all members to access. The audit log (or Changelog) can be reviewed by OFSDB members to track any changes made and to ensure data being entered by members is both valid and consistent.

The auditing process is reinforced by a Member Ratings system: all members can apply Positive, Negative or Neutral ratings relating to a particular entry. An overall rating is displayed with each entry allowing a visitor to quickly assess how effective a particular entry is to include any shortcomings or important comments on usage etc.

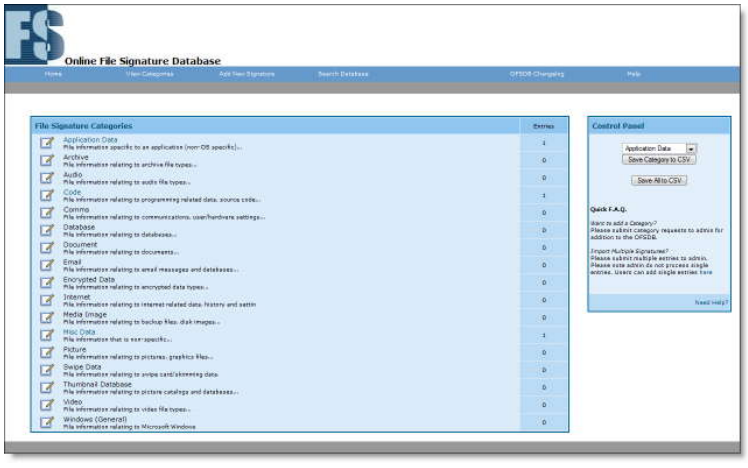
Overall database operations and functionality is controlled and maintained by site administrators. The database content is controlled and maintained by the membership.

Key Features

- Practitioner Access Only
- Members can add new content or edit existing content
- Automatic auditing, all modifications by members are recorded
- User rating system enabled
- Searchable
- Database can be exported to CSV format at any time

Categories Section

All information within the database is broken down into categories ranging from Applications Data to Operating Systems specific. Categories allow members to focus on specific needs, for example the identification of picture files. New categories can be added as and when required.

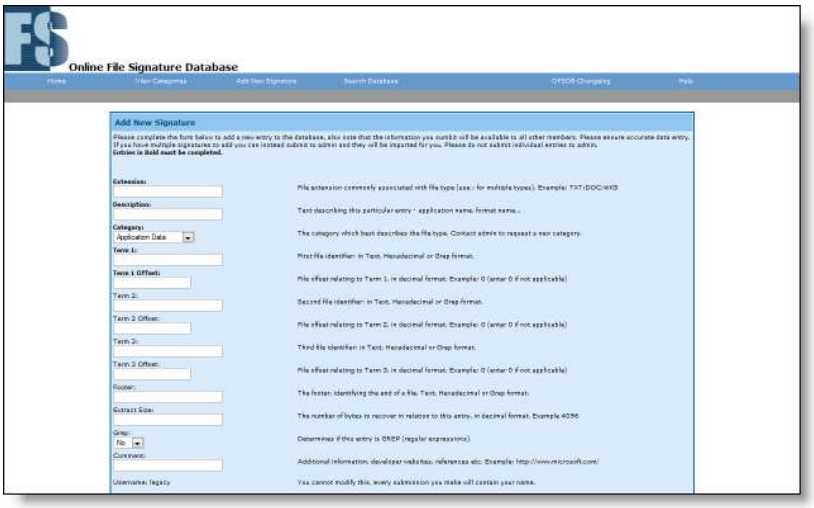


The option to save the database contents to CSV (comma separated value) format is available within this section. The export process can include all categories or specific categories.

[1] File identification information – a collective term used to describe elements of a given file for identification purposes and includes the terms File Header, Magic Number and File Signature.

Add Signature Section

This section allows members to add new information to the database. All additions are recorded within the changelog (covered later in this document). The add signature section contains thirteen fields (a minimum of 5 fields must be completed for successful entry).



The five required fields are:

1. Extension: file extension commonly associated with data type
2. Description: can include associated application name, format name etc
3. Category: chosen from existing categories or new requested category
4. Term 1: this would typically be the file header (magic number)
5. Term 1 Offset: the position within a file where Term 1 resides (starting from zero)

Additional Fields which can be completed, but not required include:

6. Term 2: additional search term
7. Term 2 Offset: the position within a file where Term 2 resides
8. Term 3: additional search term
9. Term 3 Offset: the position within a file where Term 3 resides
10. Footer: this is typically the end of the data/file
11. Extract Size: a numerical value, number of bytes to extract for data recovery
12. Grep: if a term is a regular expression this is specified here
13. Comment: any additional information, developer website, references etc

The information used to identify a file is referred to as a Term, three terms can be included per entry (this doe not include the footer). A term can be in any format including:

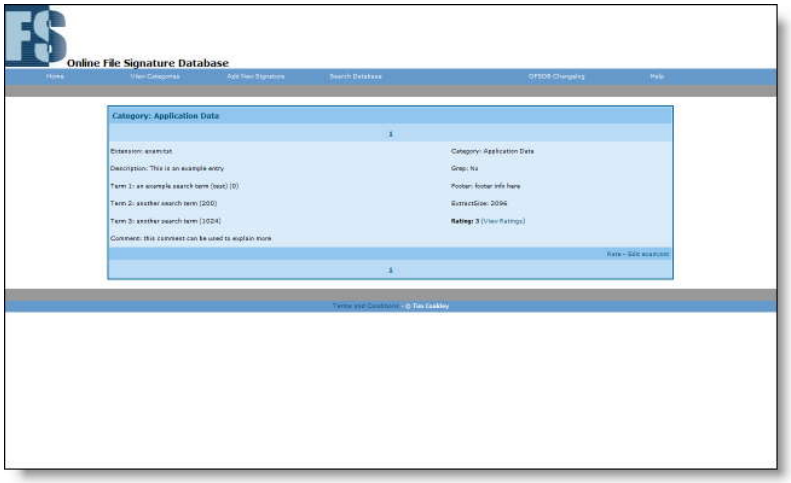
- Text (ASCII)
- Hexadecimal
- Regular Expression

Important Note:
The OFSDB does not conform to a particular format suitable for a given data recovery tool or forensic application. It is designed to be simple and flexible and acts as a central repository for the purposes of improving the quality and reliability of file identification information.

View Entry Section

All entries within the database can be viewed online. All information entered into an entry by member(s) is displayed and accessible by other members.

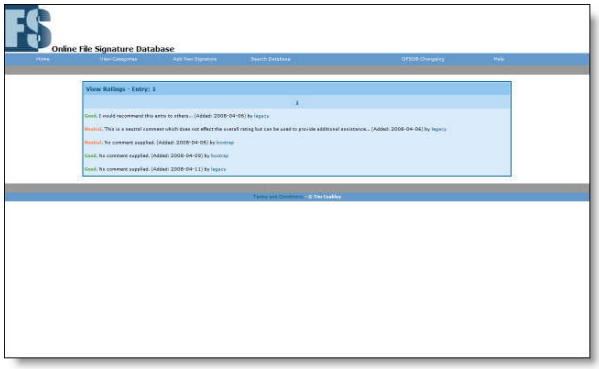
A member can edit and/or rate an entry from this section.



View Ratings Section

The rating section is one of the most important features of the database as it enables users to comment on an entry, rate the effectiveness of that entry and provide additional information. One of three ratings can be chose:

- Positive – a positive rating increases the overall rating by 1.
- Negative – a negative rating decreases the overall rating by 1.
- Neutral – a neutral rating doe not effect the overall rating however it provides additional 'comment space' allowing members to comment on particular issues relating to a particular entry.



Search Database Section

The database has a search facility so that members may search the content of the database for relevant entries. The search facility is capable of searching for the following fields:

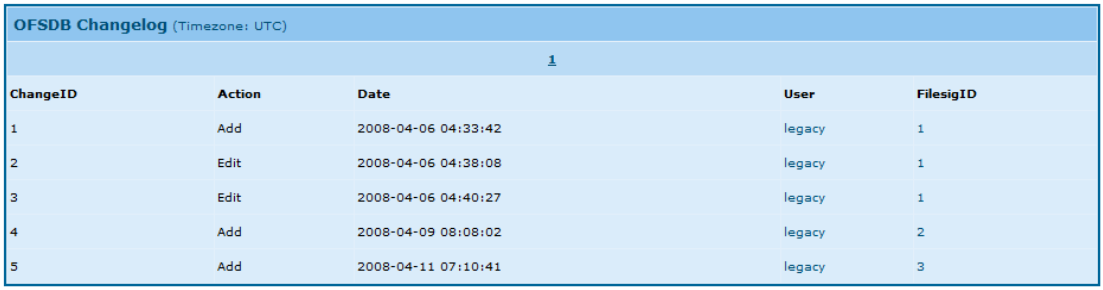
- Extension
- Description
- Category
- Term1
- Term2
- Term3
- Footer

Changelog Section

The changelog section is responsible for displaying activity recorded as the result of members adding or editing an entry. For example, when an entry has been edited a copy of that entry

is made along with date, time and username of member performing the edit. All changes and additions made by a member can be viewed in this section.

The changelog can assist members in identifying problems and any errors that have arisen. Members will know when an entry was changed, what was changed and why.



OFSDB Changelog (Timezone: UTC)

1

ChangeID	Action	Date	User	FilesigID
1	Add	2008-04-06 04:33:42	legacy	1
2	Edit	2008-04-06 04:38:08	legacy	1
3	Edit	2008-04-06 04:40:27	legacy	1
4	Add	2008-04-09 08:08:02	legacy	2
5	Add	2008-04-11 07:10:41	legacy	3

The above is a sample screenshot showing changelog entries.

Subscription Based Service

The OFSDB operates a yearly subscription based service, subscriptions pay toward ongoing bespoke development and upkeep of the resource including administrative tasks and responsibilities. The subscription also covers the cost of hosting (which is minimal in comparison to development but a cost none the less).

Small companies and units are welcome to subscribe under a single company/unit name.

A subscription can be in the name of an individual or a company. Please note that companies with 10 or more practitioners will need to contact support prior to purchase, it is not acceptable for multiple users to share one account in this instance.

Government organisations are welcome to sponsor this resource.

For more information or assistance please contact: info@filesig.co.uk

Acknowledgements

Clayton Hoskinson, for his assistance with this document.