Fixity Workflow

Configuration

1. Download Fixity from the AVPreserve Website: https://www.avpreserve.com/avpsresources/tools/
2. From the main screen, Preferences > Email Settings
    a. SMTP Server: smtp.outlook.com
    b. Email Address: The email FROM which you want fixity alert emails to originate. This should be a generic departmental account where possible to maintain business continuity, e.g. uwmarchives@gmail.com. Note that departmental group accounts do not have traditional passwords and so generally are inappropriate for this purpose.
    c. Password: The password to email address in 1b
    d. Port: 587
    e. Encryption Method: TLS protocols
3. Click "Check Credentials" to send a test email, which will verify you've entered the settings correctly

Creating and running a project

1. From the main screen, File > New Project. Project name cannot contain spaces or special characters
2. Select one or more directories to scan for fixity. You can select multiple directories in case you want to scan some folders within a larger directory but not others
3. Enter one of more email addresses to which scan results should be SENT. This should usually be a department reflector/group account, such as askarch@uwm.edu for Archives.
4. Select when and how often you want to scan the directory
    a. Per advice of Mike Puissant in Library Systems, this frequency should be approximately once per 6 months.
5. Check "If missed, run on restart" to ensure the scan still happens if you're not in the office when you schedule it
6. Optionally, check "Email only upon warning or failure" to limit the amount of email you get from routine checks. Especially useful if you are checking a large number of collections or very frequently
7. File > Save settings to save the project
8. File > Run Now to run the fixity check for the first time (baseline check)

Receiving and interpreting Results

There are two sets of files created as the result of Fixity's check: the **Reports** and the **History**. Both files are saved as TSV files.

Reports

Once a check has finished running, the email that is sent will link to the report file for that check. Otherwise you can find them in your fixity directory under /reports/ .

1. The first few lines of the file are summary information, which tell you how many of each "category" of file there are in the check:
    a. "Confirmed" files are in the same location as the previous check, and content has not changed.
    b. "Moved or Renamed" files are either in a different location or have been renamed since last check, but the content is substantially the same based on the checksum.
    c. "New files" have been added to the collection since the last check.
    d. "Changed files" have changed content (based on the checksum) since the last check.
    e. "Removed files" were not found by Fixity in the expected or any other location.
2. For the first report run on a collection, all files should read as "New".
3. For subsequent reports, make note of any files in statuses b-e, above, and send list to Library Systems (libauto@uwm.edu) for restore as needed.
    a. In general, statuses of "Changed" and "Removed" are usually most serious from a file integrity standpoint.

History

The History files contain the raw checksums computed by Fixity, from which the program derives the reports by comparing one History File with another. In general, you will have no need to access this file, but it can be useful for comparing checksums independently with another tool, if necessary for particularly valuable files. The History files can be found in your Fixity directory under /history/.

1. The header of the History file indicates the directory against which Fixity was run, the time of the specific report, and the checksum algorithm used (Fixity defaults to SHA256, but MD5 is another common algorithm).
2. The list of files includes the checksum (in Hexadecimal notation) and the full path to the file to which it belongs. You can independently verify the fixity of a file by copying checksums from the same file from different history files to a 3rd party checksum comparison tool, such as Checksum Compare.