University of New Haven

Artifact Genome Project (AGP) in Brief

Browser

AGP has been thoroughly tested using Google Chrome. Please note that some features may not work as well in other browsers; Firefox, Safari, etc.

Information Other Participants Will See & Leader Board

AGP is a crowd sourcing initiative. Therefore, your username and organization will be seen by other users accepted and enrolled in the AGP system on a visible leaderboard. Users that have not been enrolled and accepted cannot view this information. This leaderboard is used to show points that are given to contributing individuals and their respective organizations once their submitted artifacts have been submitted and vetted by AGP administrators.

AGP Membership Review Process

AGP contributors hail from a variety of backgrounds including academia, private, and public sector organizations. **Anyone may request access to AGP but not all applicants will get past the vetting process**.

Applicants are initially asked for their name, username, and e-mail during the application process. We ask that users to apply with a professional e-mail when possible and are encouraged to use a (first initial, last name, and number (if applicable), username style. i.e. bknieriem, or ibaggili1. The organization the applicant belongs to will either be determined via the e-mail address or by us contacting applicants on individual basis. Lastly, a professional work or government organization e-mail will expedite the application process.

This procedure helps prevent system contamination and assures that only experts, scientists, and professionals have access to this community initiative.

Administrators are not able to see user passwords in plain text due to encryption. Administrators capable of blocking user access and blacklisting user accounts in the event of account misuse. **User actions on the AGP system are logged for security reasons**; our goal is to create a curated artifact database that is usable by the forensics community at large.

AGP Artifact Collection Process

Artifacts may be submitted by any verified user. However, artifacts are not shown to other users until they are vetted and sanitized by an AGP analyst.

Note: When uploading potential sample artifacts like html files, SQLite databases, or other types of potential artifacts, make sure you use a sanitized dataset that does not hold any REAL evidence.

Artifacts are often collected from reviewing scholarly research or through professional work. It is of utmost importance that contributors attempt to fill as many of the fields as possible to create the most complete profile for each artifact. However, artifacts may be submitted with missing information and an analyst will decide if the profile is comprehensive enough to contribute to the live database. Contributors may find themselves working together to complete artifact profiles.

It is of note that there are two type of artifacts that people can tag within the artifacts themselves to create more granular artifacts for AGP users.

1. **SQLite Database Files:** Our analysis showed that many widely-adopted applications use SQLite database files for persistence. AGP will be able to render any SQLite database uploaded as a potential artifact with the following extensions: *.db, *.sqlite and *.sqlite3. Users can then tag columns, rows and tables in the database. For example, a SQLite database with a username column can have its column tagged with the word "username".
2. **Text Files:** Text files like html, code files, etc., also allow users to tag them. Uploaded text files with the following extensions are accepted text file artifacts: *.txt, *.html, *.xml, *.py, *.c, *.cpp, *.xsd, *.log, *.js, *.css. For example, variables in code, or hardcoded usernames and passwords may be tagged in uploaded text files.

We suggest the following process when attempting to add an artifact to AGP:

1. First, search the AGP database to see if the artifact exists. If it does and you believe it needs modification, please contact the AGP system administrators and we can examine/modify the artifact under question. If the artifact does not exist proceed to Step 2.
2. If the artifact does not exist in AGP create an artifact and choose the appropriate artifact type, fill out the form, and upload a file that contains a sanitized sample artifact should you have access to one, and submit the artifact.
3. The artifact will then go through the vetting process and will be received by an AGP analyst. The artifact may be accepted or returned for modification to the submitter.
4. Once an artifact is accepted points are assigned to the contributor and their respective organization; this will be reflected in the leaderboard.

AGP Artifact Review Process

Artifacts are categorized by state: Queued, Flagged, Updated, and Approved.

- **Queued** artifacts are awaiting attention from a qualitative analyst.
- **Flagged** artifacts may need to be revisited by another reviewer or contributor. If there is a lack of information, misinformation, or any circumstance that may inhibit reproducibility, an artifact may be flagged.
- **Updated** artifacts are flagged items that have been updated and require re-review. This indicates that they have been previously visited by an analyst and may only need minor updates to meet approval standards. Analysts may update and approve artifacts to completion themselves or request that the contributor spend more time on the artifact's profile.
- **Approved** artifacts have been completed and are now available for viewing by AGP members. They have a substantial level of profile completion and can be reproduced. Approved items are considered forensically relevant.