ABOUT AGP

WHAT IS AN ARTIFACT?

Although there is no widely accepted definition of the term "digital forensic artifact", the Forensics Wiki provides this rather generalized definition:

An object of digital archaeological interest.

We have chosen to adopt MITRE's Cyber Observable eXpression (CybOX™) to represent digital forensic artifacts. CybOX is a standardized language for encoding and communicating high-fidelity information about cyber observables.

What is a cyber observable?

Cyber observables are events or stateful properties that occur, or may occur, in the operational cyber domain, such as the value of a registry key, deletion of a file, or the receipt of an http GET.

A MUCH NEEDED RESOURCE

Much work has been done in the area of digital forensic artifact discovery, however, results from past research projects are dispersed, and are not centralized in a location that can provide easy access for scientists and practitioners to identify and analyze artifacts quickly and efficiently. There is an immeasurable number of digital forensic artifacts today, and new artifacts are being created constantly leaving investigators “in the dark” when they come across an artifact that they have not seen before. This in turn slows down the investigative process or, even worse, could allow for evidence to be overlooked.

"Digital forensic laboratories are seeing an increase in demand while also seeing a significant increase in the amount of data received for each examination." (Casey, Katz, & Lewthwaite, 2013)

This calls for researchers to develop methods that increase the rate of forensic artifact acquisition and analysis.

ENTER AGP

AGP, or Artifact Genome Project, is an online system for uploading and viewing digital forensic artifacts. The project began in 2014 initiated by the University of New Haven and Purdue University's VACCINE, a US Department of Homeland Security Center of Excellence. We selected 19 cyber observables from MITRE's CybOX, representing what we believe to be the most prominent and common cyber observables. Users can upload artifacts they discover to the AGP website by filling out the applicable form. Artifacts can also be searched using keywords or any word that appears as part of the artifact.

It is our hope that through collaboration with universities, research institutions, and the rest of the cyber community we can continue to grow the AGP artifacts' database and educational modules into a more complete representation of all artifacts that may be discovered in the cyber domain. It is also our intention to provide this tool as a resource to support investigators, students, and the rest of the community in gaining an understanding of the artifacts they may find.

SATC: EDU: EXPANDING DIGITAL FORENSICS EDUCATION WITH ARTIFACT CURATION AND SCALABLE, ACCESSIBLE ARTIFACT EXERCISES - GRANT NO.1900210

Educational programs and resources have not kept up with digital forensics artifacts - which are the cornerstone of real-world investigations. The new additional tool introduced this year (2020) in the Artifact Genome Project (AGP) transforms and expands digital forensics education by focusing the community's attention to digital forensic artifacts. By leveraging past work on the AGP, users have the opportunity to use current digital forensic artifacts, or curate new ones to design scalable, self-paced, and open source online digital forensic exercises. New material under the SaTC: EDU is based upon work supported by the National Science Foundation under Grant No. 1900210. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

LEARN MORE FROM OUR POLICIES

PROJECT OBJECTIVES

- An educational platform for students to learn about digital forensic artifacts.
- An approach that allows instructors to implement self-paced, automatically assessed learning modules related to digital forensic artifacts into their courses.
- An online educational community made up of industry professionals, students, and instructors.
- Free access to the artifacts and instructional material for anyone vetted through the system.
- Catalyze the study of digital forensics artifacts over time.

There are four types of educational modules that can be created in AGP by filling out the applicable form. These are as follows, Learn AGP, Learn About Artifacts, Learn By Doing, and Scavenger Hunt. Similar to artifacts, these modules also require vetting by the AGP administrator before approval. Approved assignments can be searched using keywords or any word that appears as part of the educational module. Users are free to test their understanding of artifacts and digital forensics by taking these educational exercises. Similar to artifacts, a leaderboard is present to track users who have the highest scores when taking assignments.