SaTC: EDU – Artifact Forensic Challenge

Ibrahim (Abe) Baggili, PI & Cinthya Grajeda, AGP Manager

*Interpol Digital Forensics Expert Group (DFEG) Conference*

*June 9, 2020*
Acknowledgements – AGP Team (active & non-active members)

Developers:
• Devon Clark, Jason Moore, and Kyle Anthony, Computer Science, MSc., Alumni.
• Shabana Akhtar Baig, Computer Science, MSc., Alumni.
• Bhavik Ashok Nahar, Cybersecurity & Networks, MSc.
• Krikor Herlopian, Computer Science, MSc.

Research Assistants:
• Andrew Mahr, Cybersecurity & Networks, BSc.
• Sophia Mateo, Cybersecurity & Networks, BSc.
• Meghan Cichon, Cybersecurity & Networks, BSc.
• Rogan Gopi, Cybersecurity & Networks, BSc.

Others:
• Laura Sanchez, Cybersecurity & Networks, MSc., Alumni.
• Tyler Balon, Computer Science, MSc.
• All the other University of New Haven students who were part of the artifact digging process
This materials is based upon work supported by the National Science Foundation under Grant Numbers 1565560 and 1900210, and the U.S. Department of Homeland Security under Award Number 2009-ST-061-CCI001-05. 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 and the U.S. Department of Homeland Security.
Scientific Publications

  • Link: https://www.sciencedirect.com/science/article/pii/S1742287616300366

  • Link: https://www.sciencedirect.com/science/article/pii/S1742287618302007
What is an Artifact?

Information or data created as a result of the use of an electronic device that shows past activity (SWGDE)

- Examples (Forensically relevant data)
  - Database that contains passwords, usernames etc.
  - Log files
  - Xml files that contain usage data
  - Etc.
Curated Forensic Artifact (CuFA)

Location type (original source of creation)

- User
  (e.g., using a text editor application to create a text file)
- Application
  (e.g., log/database file created by an application to store user information)
- System
  (e.g., registry file or alteration created by the system via a process/application)
- Download
  (e.g., package of files or executable in stand-alone form before installation)
- Network
  (e.g., packet in transit which has been captured)

CuFA requirements

- Name
- Description
- Comments
- Person(s)/time of entering into database
- Location type (original source of creation)
- Location (specific source, inherited from CybOX if applicable)
- Object type (inherited from CybOX)
- Device
  - Manufacturer
  - Model
  - OS
  - MD5/SHA1/MRSHv2
  - Person(s)/time of discovery
  - Enabled/disabled
  - Pointers to other related artifacts found because of this artifact (implemented as linked list)
  - Type (PDA, mobile, laptop, server, don't know/external)

CybOX object (examples below)

- File
  - Device_path
  - Full_path
  - File_extension
  - File_format
  - Modified_time
  - Accessed_time
  - Created_time
  - File_extensions_list
- Process
  - Name
  - PID
  - Parent_PID
  - Child_PID
  - Username
  - User_time
  - Start_time
  - Status
- Win registry
  - @object references
  - Key/value
  - Number_values
  - Creator_username
  - Handle_list
  - Subkeys
  - Date_runs
  - Custom_properties
- Archive file
  - Version
  - Encryption_algorithm
  - Full_path
  - File_extension
  - Size_in_bytes
  - Signature
  - Digital_signatures
  - Hashes
- Network socket
  - Address_family
  - Domain
  - Local_address
  - Protocol
  - Remote_address
  - Type
  - @file_blocking
  - @file_listening
Problem

- Many artifacts
- Many systems
- Many users
- Too much data
- All formatted differently
- Examiner overload
- Examiner backlogs
Enter AGP - Crowd Sourcing Video
<table>
<thead>
<tr>
<th>Artifact Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Artifact</td>
<td>Artifacts that take the form of a file with extensions such as .txt, .pdf,</td>
</tr>
<tr>
<td></td>
<td>.doc, .jpg, .mpeg, etc.</td>
</tr>
<tr>
<td>Windows Registry Artifact</td>
<td>Artifacts existing within the Windows Registry.</td>
</tr>
<tr>
<td>Process Artifact</td>
<td>Observe processes running on a machine.</td>
</tr>
<tr>
<td>Memory Artifact</td>
<td>Artifacts discovered through memory analysis.</td>
</tr>
<tr>
<td>SMS Message Artifact</td>
<td>A Short Message Service artifacts.</td>
</tr>
<tr>
<td>Account</td>
<td>Intended to characterize generic accounts.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>Intended to specify a cyber address.</td>
</tr>
<tr>
<td>Code</td>
<td>Artifacts composed of a body of computer code.</td>
</tr>
<tr>
<td>Disk</td>
<td>The Disk object is intended to characterize a disk drive.</td>
</tr>
<tr>
<td>Disk Partition</td>
<td>The Disk Partition object is intended to characterize a single partition of</td>
</tr>
<tr>
<td></td>
<td>a disk drive.</td>
</tr>
<tr>
<td>Email Message</td>
<td>Artifacts in the form of individual email messages.</td>
</tr>
<tr>
<td>Linux Package</td>
<td>The Linux Package object is intended to characterize a Linux software</td>
</tr>
<tr>
<td></td>
<td>package.</td>
</tr>
<tr>
<td>Network Packet</td>
<td>The Network Packet object provides the definition of a network packet based</td>
</tr>
<tr>
<td></td>
<td>on the TCP/IP model/Internet protocol suite.</td>
</tr>
<tr>
<td>Network Socket</td>
<td>Artifacts which take the form of network sockets.</td>
</tr>
<tr>
<td>User Account</td>
<td>The User_Account object is intended to characterize generic user accounts.</td>
</tr>
<tr>
<td>User Session</td>
<td>Artifacts in the form of observed user sessions.</td>
</tr>
<tr>
<td>Volume</td>
<td>The Volume object is intended to characterize generic drive volumes.</td>
</tr>
<tr>
<td>Windows Event Log</td>
<td>The Windows_Event_Log object is intended to characterize entries in the</td>
</tr>
<tr>
<td></td>
<td>Windows event log.</td>
</tr>
<tr>
<td>X509 Certificate</td>
<td>X509_Certificate object represents a public key certificate for use in a</td>
</tr>
<tr>
<td></td>
<td>public key infrastructure.</td>
</tr>
</tbody>
</table>
AGP by the numbers…

- AGP Launched 06/2017
- Over 280 Registered users
- Over 180 Organizations
- 28 Countries
- Over 1,100 Vetted artifacts
- Over 36,000 User interactions
Use case 1: Communicating over a large, connected cubicle
Use case 2: Peeping into some else’s cubicle on the network
Vet / check the work
What do your users get out of it?

• Lab knowledge management
  • If people leave, knowledge is left behind

• Improving education
  • Educational resources for examiners, educators, and students

• Improving communication
  • Investigators can communicate with other examiners

• Improving access to investigator resources

• Potential for automation in the future

• **IMPACT – SAVE LIVES, HELP EXAMINERS**
SaTC: EDU: Expanding Digital Forensics Education with Artifact Curation and Scalable, Accessible Artifact Exercises – 2020

- Transforms and expands digital forensics education.
- Focuses the community's attention to digital forensic artifacts.
- Uses current digital forensic artifacts, or curated new ones.
- Digital forensic exercises are scalable, self-paced, and open source.
Project Objectives

• An educational platform for students and professionals to learn about digital forensic artifacts.

• For instructors to implement it into their classrooms.
  • self-paced.
  • automatically graded by the system.

• To creates 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.

• To catalyze the study of digital forensics artifacts over time.
Educational Modules

• Currently, three types but more can be added.
  • Learn About Artifacts.
  • Learn By Doing.
  • Scavenger Hunt.

• Educational modules are vetted by the AGP administrator.

• Search for assignments using keywords or any word that appears as part of the educational module.

• Test your understanding of artifacts and digital forensics by taking these educational exercises.

• A leaderboard is present to track users' scores when taking assignments.
Artifact Educational Challenge

• One week to complete all exercises.

• In order to participate, register for an AGP account @ https://www.agpnewhaven.com. Open now to the public, go register.
  • Please, ensure you provide enough information in order to be vetted and be admitted to the site. Especially important, provide an organizational email address.
  • You will receive an email once your account has been vetted and approved.

• Limitations:
  • 1st time launching the modules to the public.
  • Tools are recommended in the exercises to answer some of the questions.
  • Some tools may need to be installed on your system. Use VM.
  • Complete survey.
Contact the AGP Team

• Send a message through the chat messaging system in AGP under Inbox tab, select a username:
  • Cgraj1 – AGP manager
  • Bhaviknahar19 – Developer
  • amahr1, bhaviknahar19, or Smate4 – Research assistants
  • If it’s a major issue, or if you prefer, use the contact page to send a message instead. Or,

• Email the admin at agp@newhaven.edu.
Future Collaborations

• Use AGP in your investigations
• Contribute assignments
• Use assignments in your training
• Use assignments in your classrooms
  • Automated grading!
• Contribute artifacts
• Reach out and add artifacts
• Add suggested artifacts
AGP Demo

• Artifacts
• Educational Modules