Experience Constructing the Artifact Genome Project (AGP): Managing the Domain's Knowledge One Artifact at a Time

* ˟ Cinthya Grajeda, *Laura Sanchez, Dr. Ibrahim Baggili, Devon Clark, & Dr. Frank Breitinger

*Graduate Researcher, UNHcFREG member
˟AGP Manager

Presenting @ DFRWS USA, Providence, Rhode Island, 2018

University of New Haven
Cyber Forensics Research & Education Group

UNHcFREG

Agenda

UNHcFREG

- Introduction
- Previous Work
- Impact (professional & academic)
- AGP System Design
- Vetting Process
- Data Usage and Analysis
- Demo
- Lessons Learned
- Future Work

AGP Explainer Video

Artifacts

- "Information or data created as a result of the use of an electronic device that shows past activity."
  - The Scientific Working Group on Digital Forensics (SWDGE), 2015
- Examples:
  - Registry keys
  - Logs
  - Headers

Artifacts – Continued

- Important to locate and decode
  - May indicate things that content itself may not, such as that a suspect did access a particular document or used a certain program to view an image
- Forensic tools serve to indicate that artifacts potentially exist
  - Do not contribute to establishing and maintaining artifact knowledge
  - Do not explicitly provide in-depth information about the makeup of artifacts

Related/Previous Work

- Forensic Artifact Analysis
  - Mobile Devices: Bader & Baggili (2010), Al Marzougy et al. (2012), Iqbal et al. (2013)
  - Supervisory Control and Data Acquisition (SCADA): Denton et al. (2017), Senthivel et al. (2017), Ahmed et al. (2017)
  - Smart Watches: Baggili et al. (2015), Ricci et al. (2016)
  - Cloud Storage Forensics: Hale (2013), Quick and Choo (2014), Roussev and McCulley (2016), Roussev et al. (2016)
  - Drones: Clark et al. (2017)
  - Mobile & Desktop Applications: Al Mutawa et al. (2012), Walnycky et al. (2015), Zhang et al. (2017), Al Mutawa et al. (2011), Marrington et al. (2012)

Related/Previous Work – Continued

- Schemas and Ontologies
  - Cyber Observable Expression (CybOX): Barnum et al. (2012), Casey et al. (2015)
  - Structured Threat Information eXpression (STIX): Barnum (2014)
  - Digital Forensic Analysis eXpression (DFAX): Casey et al. (2015)
  - Unified Cyber Ontology (UCO): Syed (2015), Syed (2016)
- Attempts at an Artifact Database
  - ForensicArtifacts.com
  - *Artifact Exchange* (Magnet Forensics)

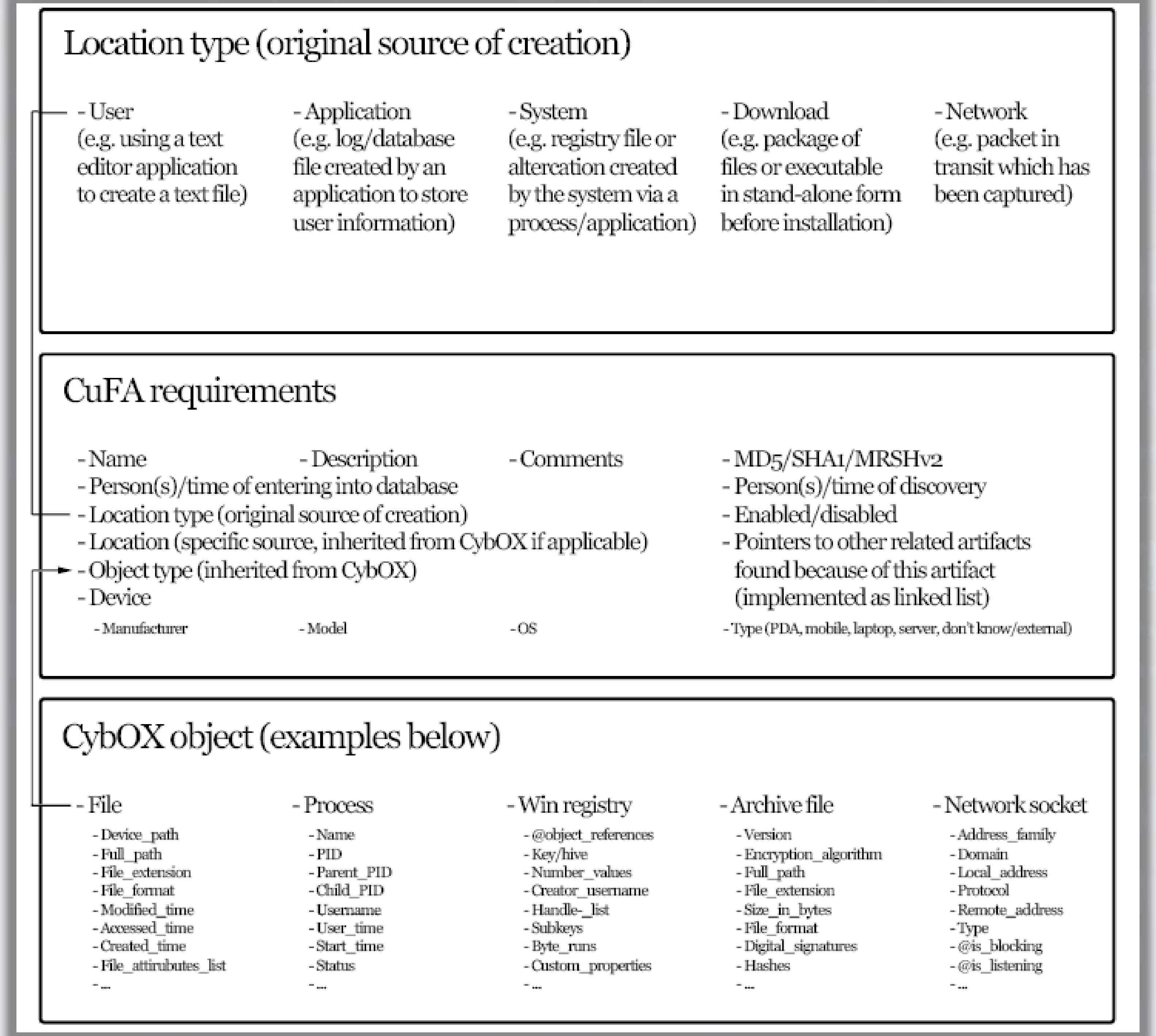
Curated Forensic Artifacts (CuFAs)

UNHcFREG

- Work from Harichandran et al. (2016)
  - Acknowledged the lack of a standardized definition and ontological model for artifacts and the challenges associated with this
- Results of this preliminary work:
  - A proposal of a more concrete and unified definition, as well as a new name: Curated (digital) Forensic Artifact (CuFA)
  - An ontological model was designed for the curation of artifacts- establishing a set of procedures and requirements for an object to be considered a CuFA
  - Presented a way to implement the ontology with CybOX to create an organized and searchable database

CuFA Model

Harichandran et al., 2016



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 altercation 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
  - Type (PDA, mobile, laptop, server, don't know/external)
- MD5/SHA1/MRSHv2
- Person(s)/time of discovery
- Enabled/disabled
- Pointers to other related artifacts found because of this artifact (implemented as linked list)

CybOX object (examples below)

- File
  - Device_path
  - Full_path
  - File_extension
  - File_format
  - Modified_time
  - Accessed_time
  - Created_time
  - File_attirubutes_list
  - ...
- Process
  - Name
  - PID
  - Parent_PID
  - Child_PID
  - Username
  - User_time
  - Start_time
  - Status
  - ...
- Win registry
  - @object_references
  - Key/hive
  - Number_values
  - Creator_username
  - Handle-_list
  - Subkeys
  - Byte_runs
  - Custom_properties
  - ...
- Archive file
  - Version
  - Encryption_algorithm
  - Full_path
  - File_extension
  - Size_in_bytes
  - File_format
  - Digital_signatures
  - Hashes
  - ...
- Network socket
  - Address_family
  - Domain
  - Local_address
  - Protocol
  - Remote_address
  - Type
  - @is_blocking
  - @is_listening
  - ...

AGP & Contributions

UNHcFREG

- Started in 2014, launched in 2017
- Crowd-sourcing initiative encouraging digital forensic professionals to share results relating to Curated Forensic Artifacts (CuFAs)
- Aspires to create a fundamental map of digital forensic artifacts
- Contributions
    - Largest vetted freely available digital forensics artifact platform
    - Primary implementation of CuFA
    - Catalyzes community-based artifact collection
    - Share design choices and lessons learned from building and maintaining

Professional Impact

- Make accessible various types of digital artifacts
  - Can search for artifacts one has not encountered before, saving time in an investigation

“A database of artifacts vetted by a community of examiner could prove useful in digital forensic investigations. As a Digital Forensic Examiner with the St. Louis County Police Department we are tasked with trudging through over a thousand pieces of evidence a year. If one of those pieces of evidences has artifacts we are searching for, it'd be very helpful to have a resource instead of finding it on our own. Additionally, if it is a new program with new artifacts that we find, to put that information out to the community and assist other examiners is very fulfilling.” Digital Forensic Examiner, St. Louis County Police Department

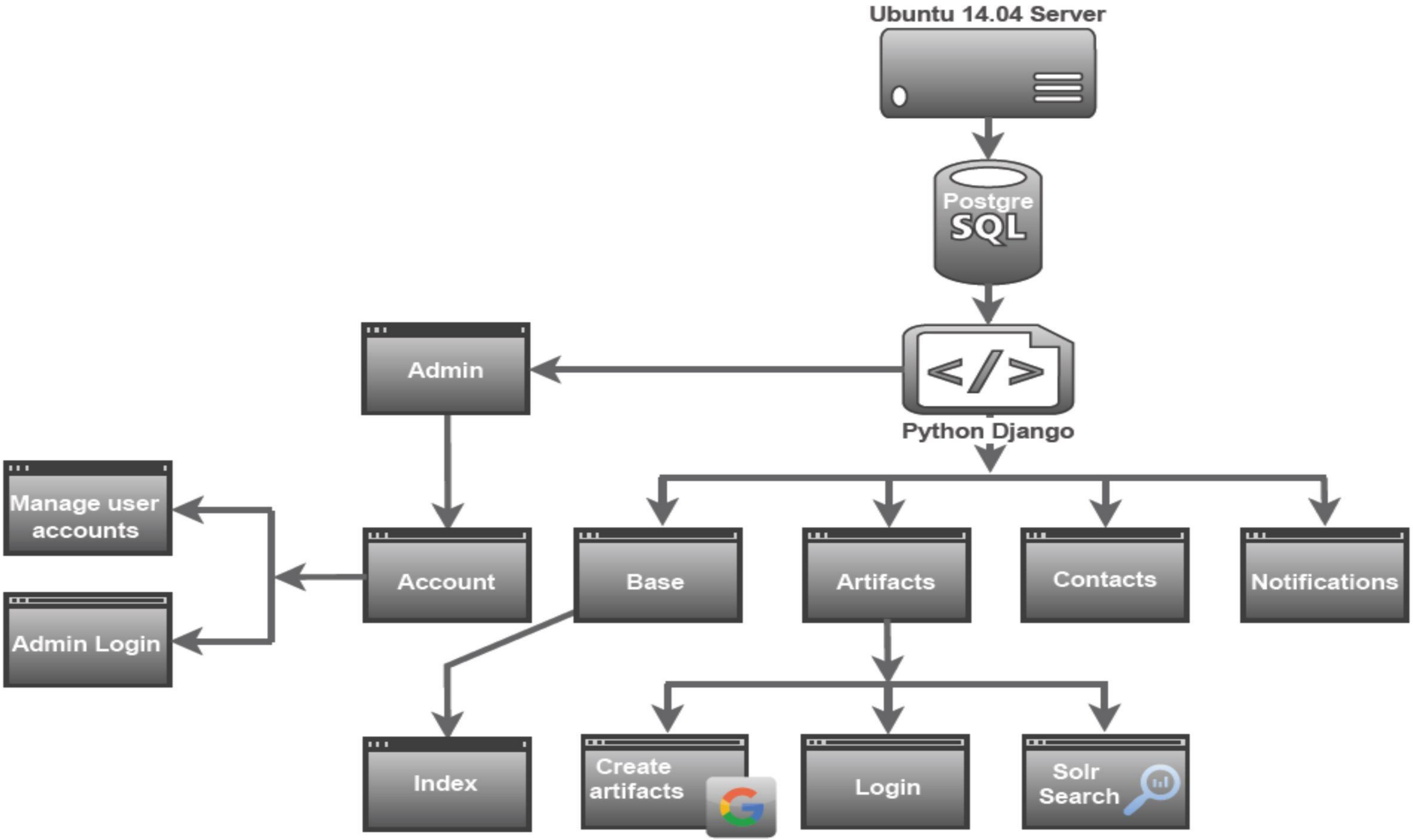
Professional Impact – Continued

- Allows practitioners to keep up-to-speed with new devices and applications
- Can be incorporated into scripts to be used with current tools
- Increase cooperation within the digital forensic community
  - Friendly competition
  - Tagging
  - Communication

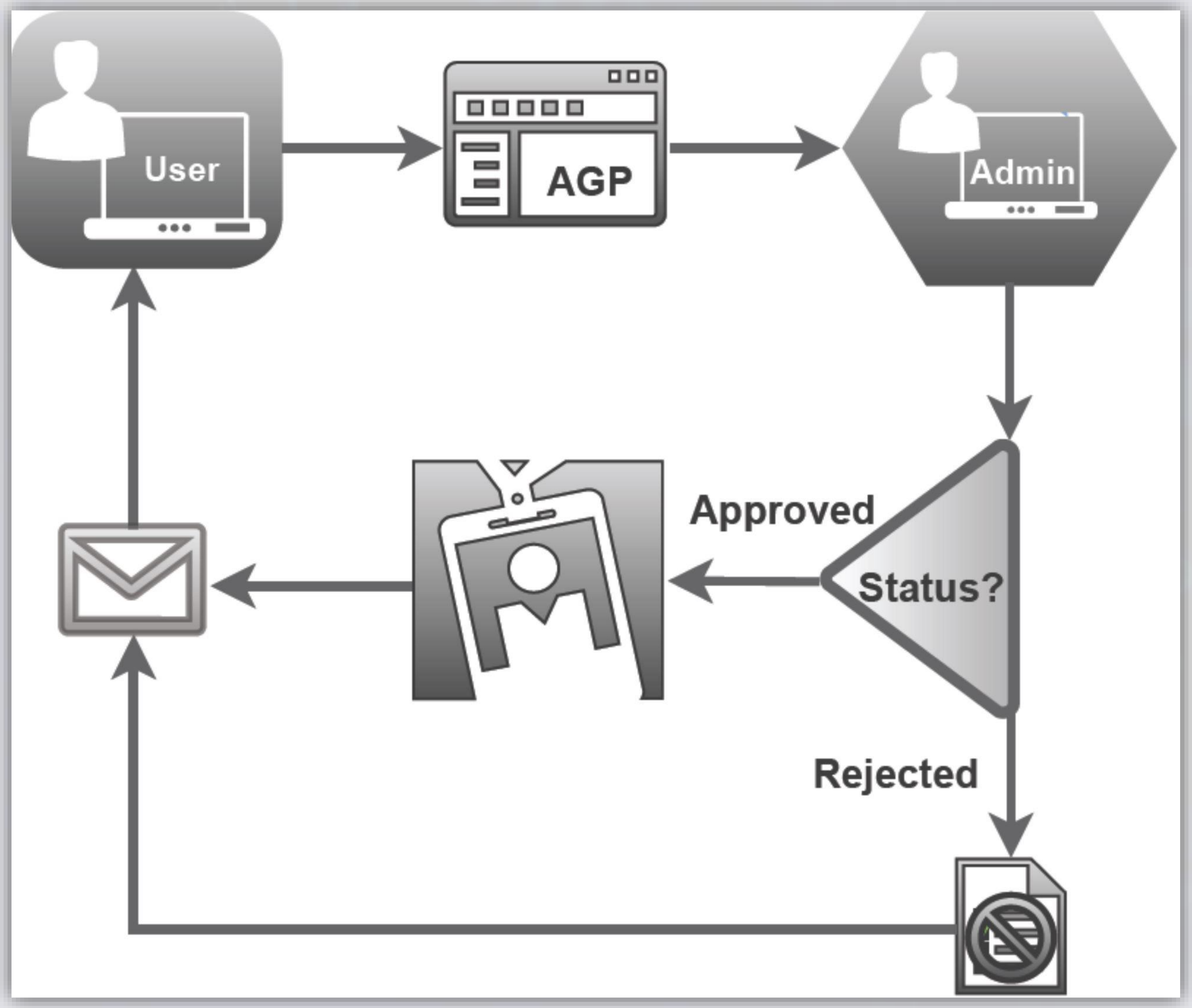
Academic Impact

- Students have been the main contributors of artifacts
  - UNH partnered with the University of Texas at San Antonio in the fall of 2017
  - AGP was implemented in a University of New Haven class in the fall of 2017, which helped surpass the 1000 artifact mark
  - Have conducted their own research to discover, sanitize, and upload new artifacts
  - For some it has provided a source of income while studying
- Provides hands-on experience and knowledge building
  - Better prepares them for a career in digital forensics by developing job-ready skills

AGP Architecture

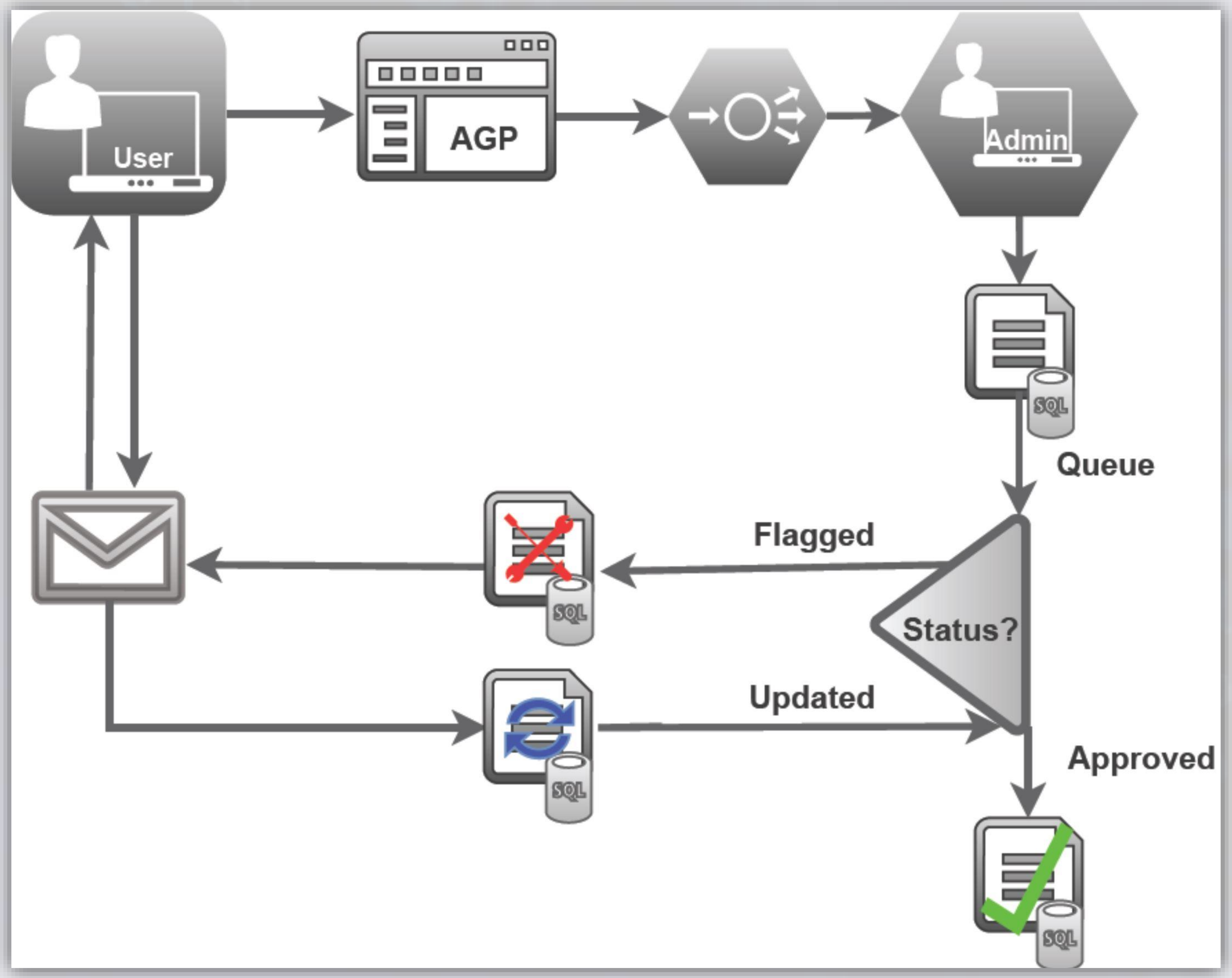

Ubuntu 14.04 Server
Postgre SQL
Python Django
Admin
Account
Manage user accounts
Admin Login
Base
Artifacts
Contacts
Notifications
Index
Create artifacts
Login
Solr Search

User Vetting Process



UNHcFREG

Artifact Vetting Process


User
AGP
Admin
SQL
Queue
Flagged
SQL
Status?
Updated
SQL
Approved
SQL

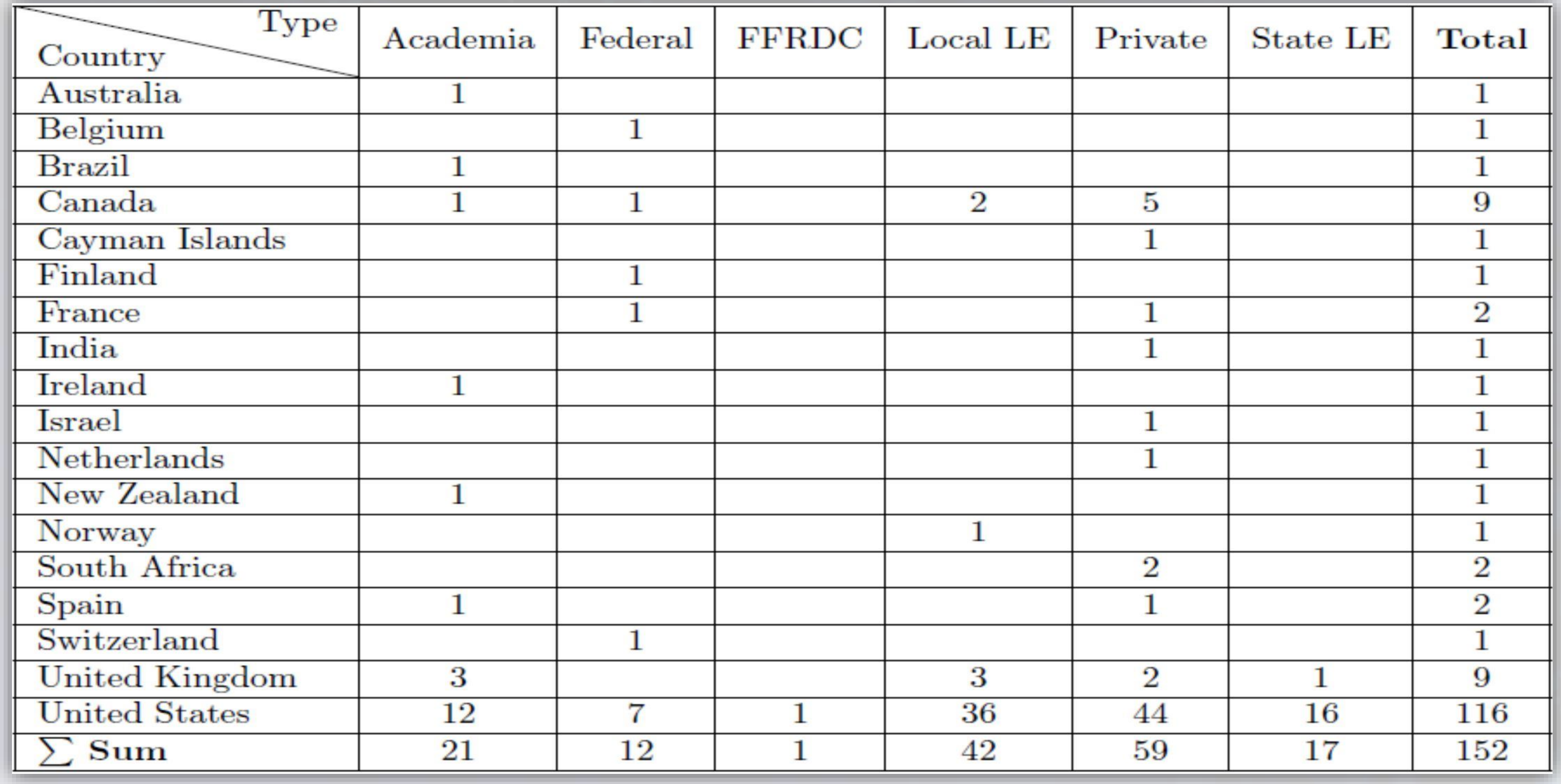
UNHcFREG

Data Usage & Analysis

User/System Statistics	
Vetted Users	193
Organizations	152
Countries	18
All system interactions	14,174
User, basic & advanced artifact search queries	2,734

Artifacts	
Sanitized artifacts	1,000
Devices	29
iOS	261
Android	238
Windows	284
MAC OS/Ubuntu	69/19

Data Usage & Analysis – Continued



Type Country	Academia	Federal	FFRDC	Local LE	Private	State LE	**Total**
Australia	1						1
Belgium		1					1
Brazil	1						1
Canada	1	1		2	5		9
Cayman Islands					1		1
Finland		1					1
France		1			1		2
India					1		1
Ireland	1						1
Israel					1		1
Netherlands					1		1
New Zealand	1						1
Norway				1			1
South Africa					2		2
Spain	1				1		2
Switzerland		1					1
United Kingdom	3			3	2	1	9
United States	12	7	1	36	44	16	116
∑ **Sum**	21	12	1	42	59	17	152

Data Usage & Analysis – Continued

- By tracking what users share and search for:
  - Helps understand:
    - What’s trending in terms of research and investigative interests
  - Helps create a fundamental archive of digital forensic artifacts
  - We could scientifically study artifacts overtime

Demo - AGP Website

https://agp.newhaven.edu/

Experience Creating AGP

UNHcFREG

- Practitioners want access to a curated artifacts platform
- Some digital forensic practitioners can be hesitant in sharing artifacts
- Academia is a good place for curating digital forensics artifacts

Future Work

- More collaborations with academic institutions
- Possibly hire more artifact diggers
- Add educational modules
- Develop forensic tool plugins that utilize AGP artifacts
- Explore mechanisms for automating artifact discovery

Acknowledgements

UNHcFREG

- This material is based upon work supported by the U.S. Department of Homeland Security under Award Number 2009-ST-061-CCI001-05 and the National Science Foundation under Grant No. 1565560. 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 or the Department of Homeland Security.
- Special thanks to:
- Developers:
  - Devon Clark, Jason Moore, and Kyle Anthony

Acknowledgements – Continued

- Pen-testers/Debugger:
  - Frank Breitinger, Matt Topor and Christopher Meffert/Cinthya Grajeda
- Artifact Collectors/Diggers
  - *University of New Haven (UNH)*: Brandon Knieriem, Cinthya Grajeda, Michael Mazzola, Ananya Yarramreddy, Chad Messam, Matt Topor, Xiaolu Zhang, Philip Levine, James Campbell, Samuel Perreault, Jason Thomas, Ibrahim Baggili and others.
  - *University of Texas at Sant Antonio (UTSA)*: Shalabh Saini
  - *Connecticut Center for Digital Investigations (CDI)*: Sgt. Corey Davis
  - *Teesside University*: Reece Bartle-Coates
  - *Wells Fargo*: Walker Johnson

Acknowledgements – Continued

- Article authors:
    - Cinthya Grajeda, Laura Sanchez, Ibrahim Baggili, Devon Clark, and Frank Breitinger
- Other support provided to AGP:
    - Sgt. Corey Davis (CDI) and Dr. Nicole Lang Beebe (UTSA)
- AGP Manager:
    - Cinthya Grajeda
- Google
    - For providing travel scholarships to Laura and Cinthya to present at DFRWS

Contact & Questions?

Cinthya Grajeda	cgraj1@unh.newhaven.edu
Laura Sanchez	lsanc3@unh.newhaven.edu
Ibrahim Baggili	ibaggili@newhaven.edu
AGP	agp@newhaven.edu

https://agp.newhaven.edu http://www.unhcfreg.com