CprE 491 - sdmay19-38

Android App Forensic Evidence Database

Weekly Report 3

09/26/2018 - 10/04/2018
Client: Neil Gong and Yong Guan
Faculty Advisors: Neil Gong and Yong Guan

Team Members:

Mitchell Kerr -- Tech Lead
Connor Kocolowski -- Report Lead
Emmett Kozlowski -- Meeting Scribe
Jacob Stair -- Testing Lead
Matthew Lawlor -- Meeting Facilitator

Past Week Accomplishments

- The ApkPure crawler is now able to collect descriptions, package names, reviews, previous versions, and the publish date and sha values of those versions.
- UpToDown web crawler is crawling across category web pages.
- Scrapy framework deemed to be too extraneous and unnecessary.
- MongoDB setup on VM
    - An initial instance of MongoDB was set up on our VM. This will allow us to now start creating a library to communicate with the database so we can start collecting and saving the data we are collecting.
- Initial Schema design
    - A first draft of how our data should be modeled in the database was created. In order to create this schema, research was required to understand how MongoDB works and what are the best practices are for modeling data in MongoDB.

Pending Issues

- Apks of previous versions are not being collected
    - There is an issue with the function to download the APK files
- Reviews will either be stored in the database or in the file path
    - There is a tremendous amount of data coming from the reviews and it may be best to store them on the file system. Still researching on these options.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Mitchell Kerr	Began implementing APKMirror crawler using beautifulsoup. Crawler can reach majority of app pages.	7	16
Connor Kocolowski	Worked on refining apkPure crawler to collect every version of an application along with the corresponding publish date and sha values	6	17
Emmett Kozlowski	Researched setting up MongoDB and set up initial Mongo instance. Also started on designing a schema for the database.	4	14
Jacob Stair	Researched benefits to using Scrapy framework. Worked on UpToDown web crawler. Crawler is now is crawling across category web pages.	7	17
Matthew Lawlor	Worked with Connor to finish ApkPure. Web crawler is now collecting descriptions, package names, and reviews. Working on getting our server synced with Cybox.	6	18

Plans for Coming Week

- Have a completed crawler as a baseline for following ones
    - Collect and display metadata from APKPure for approval from the client
- Have reliable communication with cybox
    - Look into setting up cyBox on the server to allow file system to be stored on the cloud
- Achieve more progress concerning upToDown and apkMirror web crawlers
    - Begin collecting metadata from these sites once all pages can be reached
- Create sketches for web application user interface
    - Ensure intuitive process for non-technical clients to be able to query database
- Create basic flask app to communicate with database
    - Create a flask app that can perform CRUD operations on the database.