**SOURCE OF MALWARE DETAILS AND BEHAVIOUR**

The ransomware locky malware family was extracted from <https://ransomwaretracker.abuse.ch/tracker/locky/>

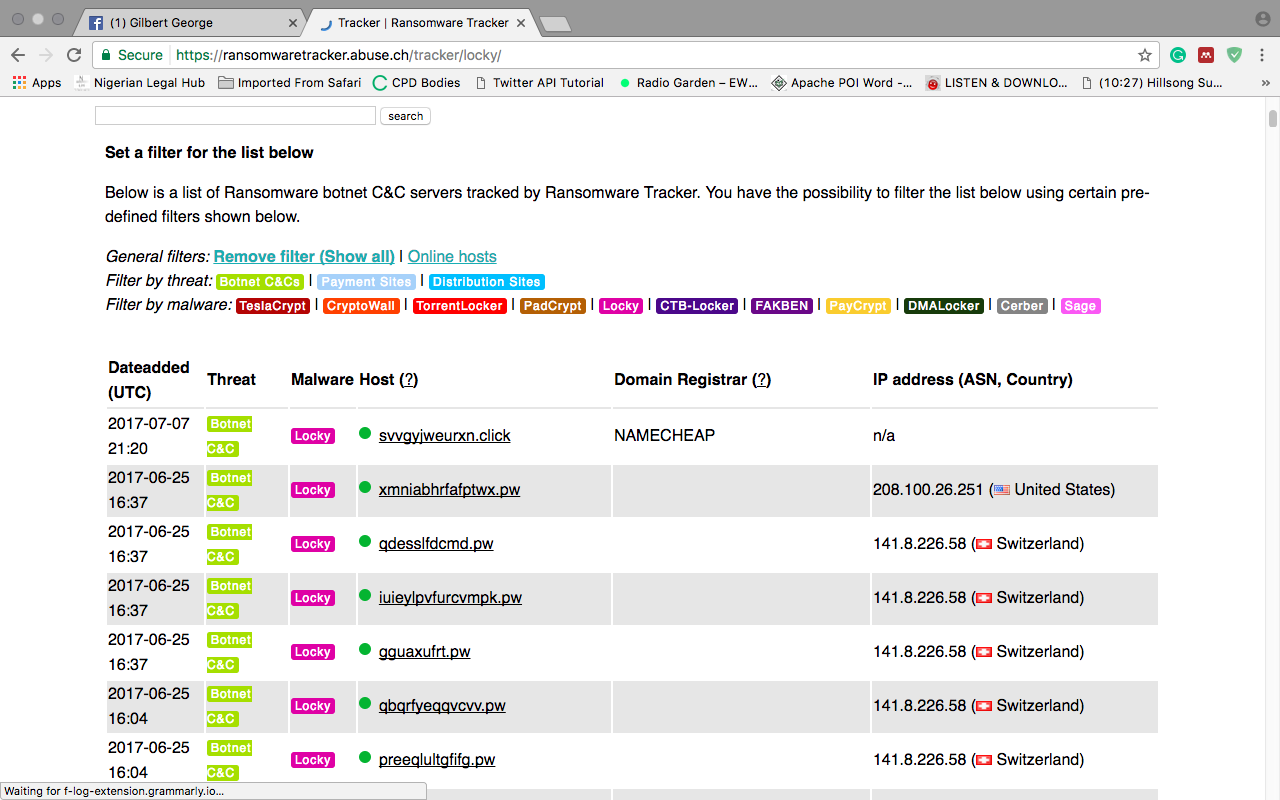
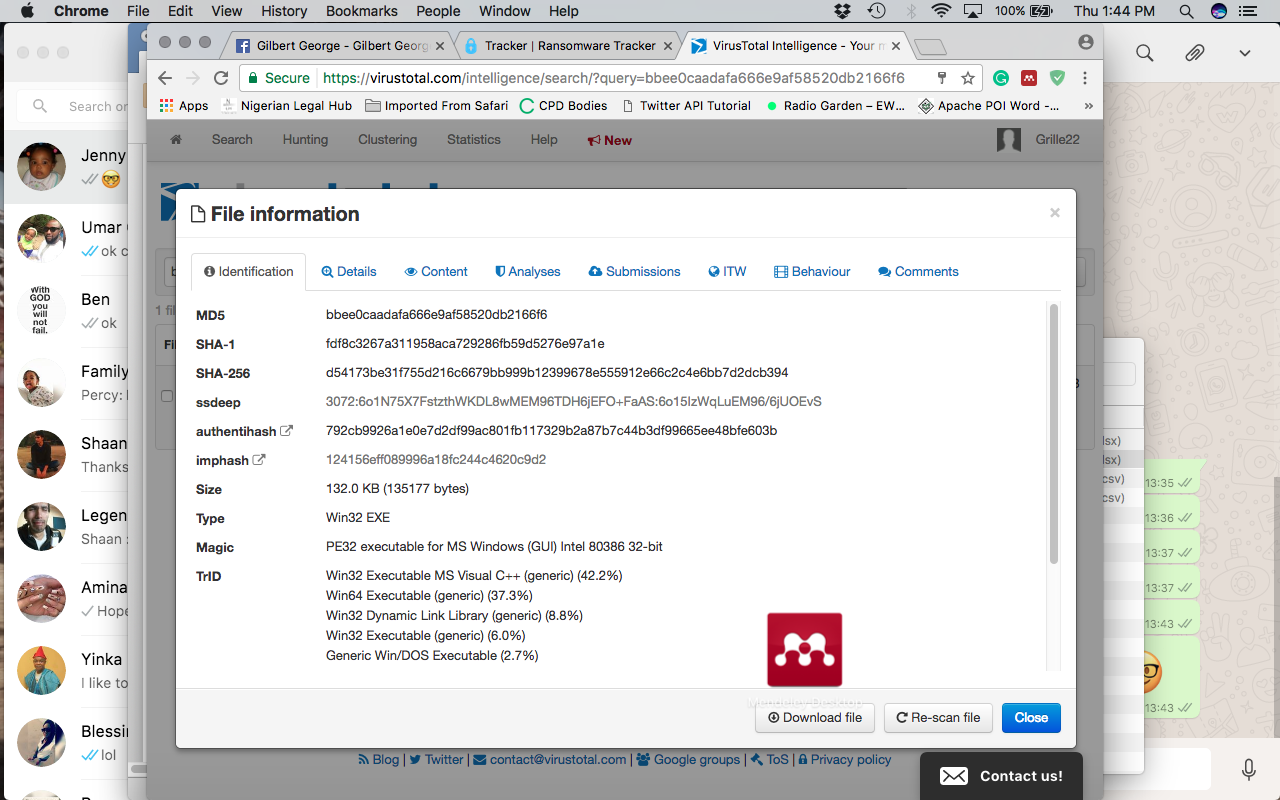
with bonet c&c and locky filter selected. Which brought up the latest bonet c&c locky ransomware registered in the virus total platform, which I used to download the 50 latest locky hashes.

Figure showing a screenshot of ransomware tracker platform



The behaviors are taken out from the Details, Content and Analysis attributes of the virus total intelligence platform. These are the list of attributes that composes the preprocessed data: Hash values, Strings, Portable Executable Sections, Portable execution Imports, Root Entry, document summary information and antivirus signatures.

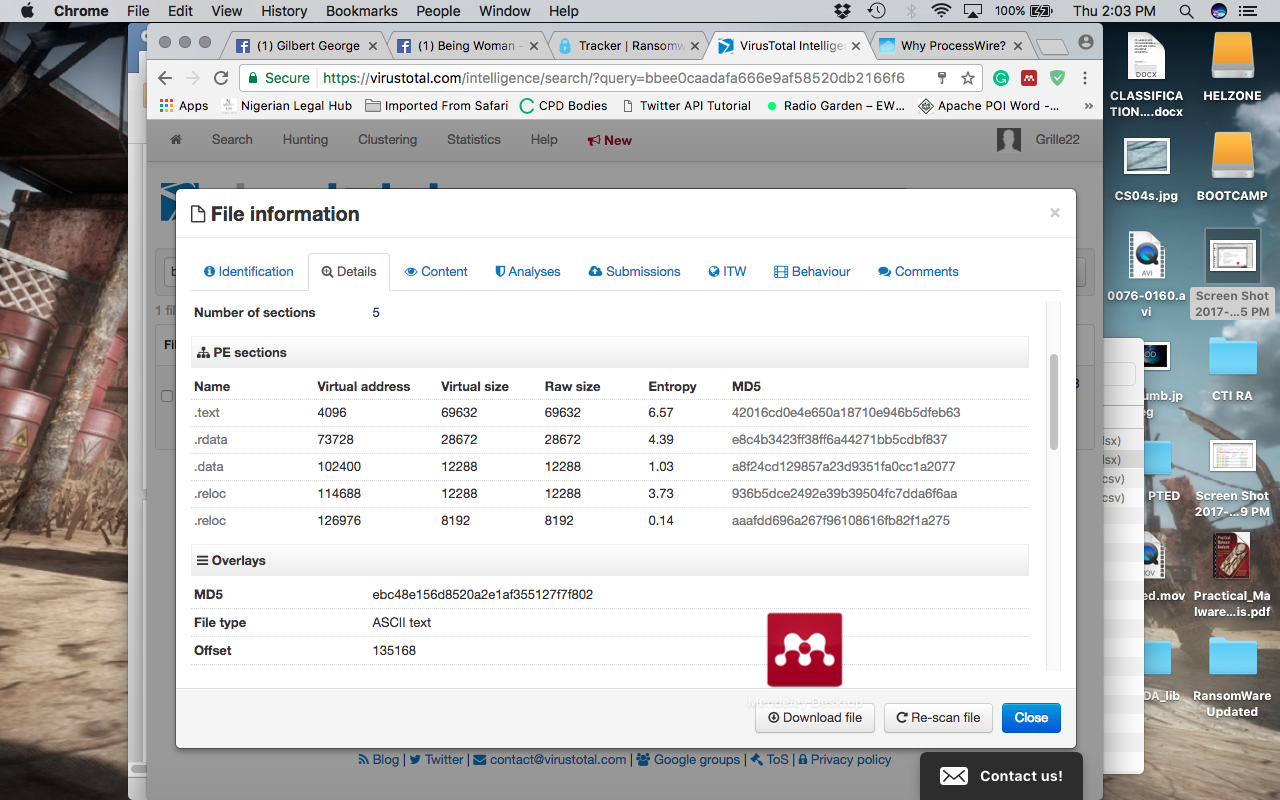
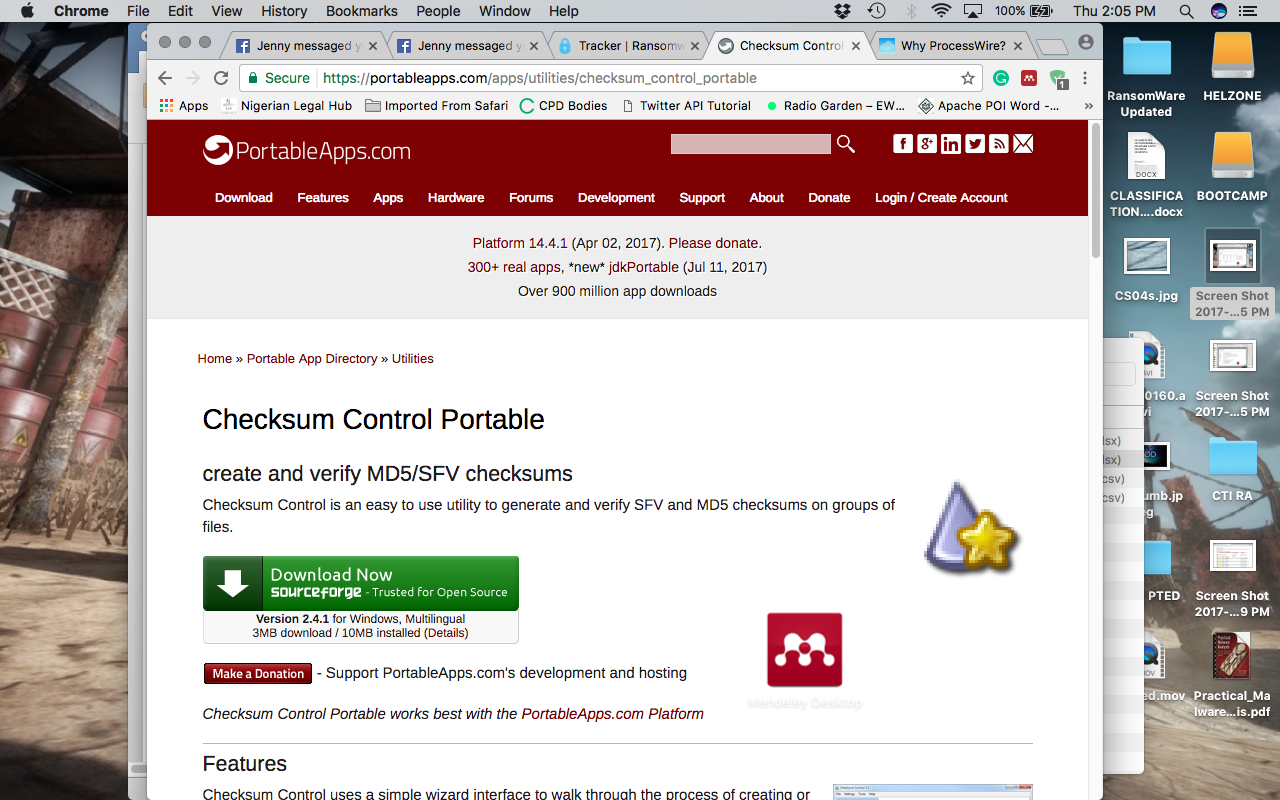


Figure Screenshot showing captured details of a malware hash

**SOURCE OF GOODWARE**

The 50 Benign ware of this project are collected from <https://portableapps.com/apps> 

The hashes were submitted on virus total intelligence to observe and collect their behavior.

In the code book folder are also excel and CSV files holding the preprocessed dataset for malware and benign wares.