Dynamic analysis

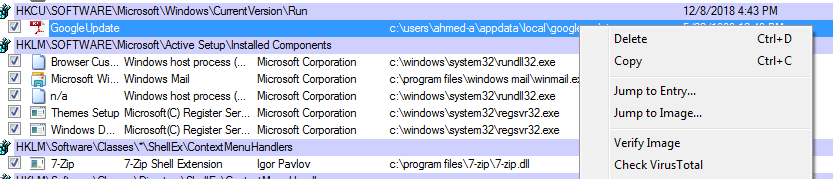
Autoruns: a tool that is capable to show a programs are configured to run during system bootup or login . Plus the tool can show the integrity levels showing by its colors. Red showing low integrity.

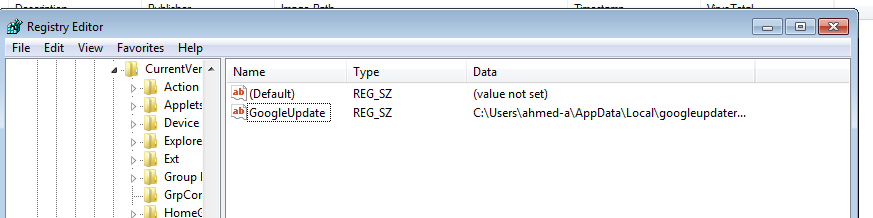
Malware file:

Shows the location of the file, when executing it created a executable process in that folder.

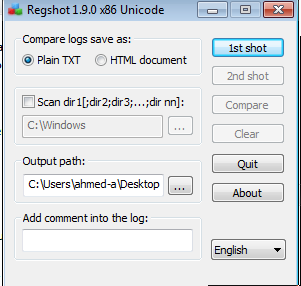
(GoogleUpdate). Plus the time which is incorrect.

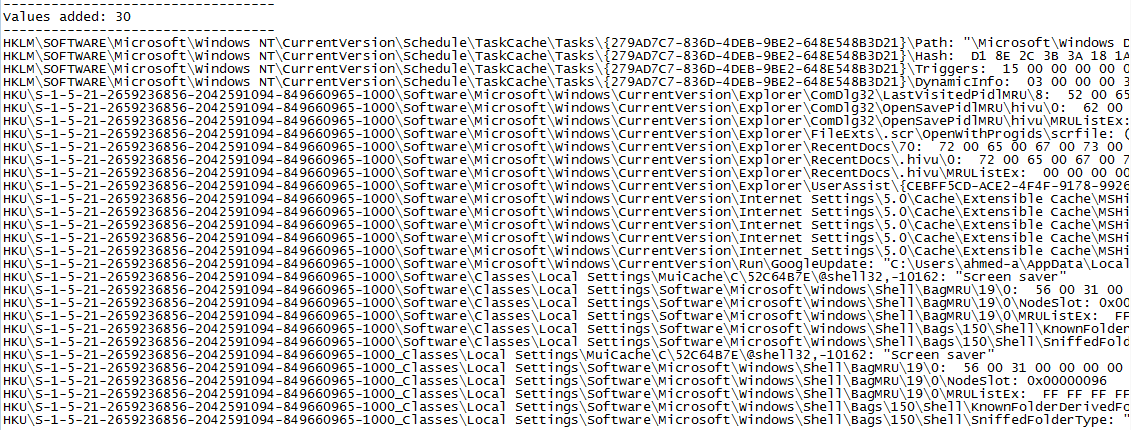
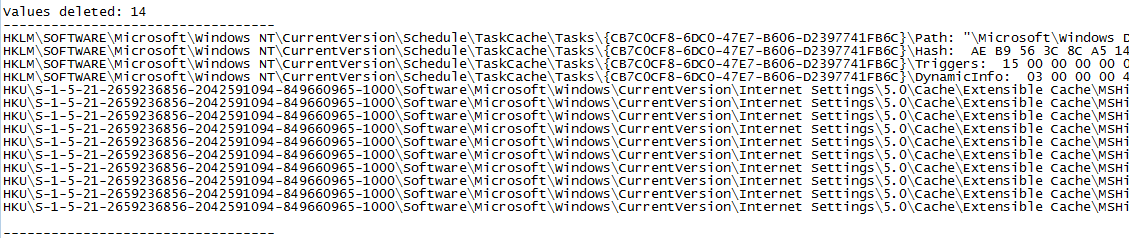
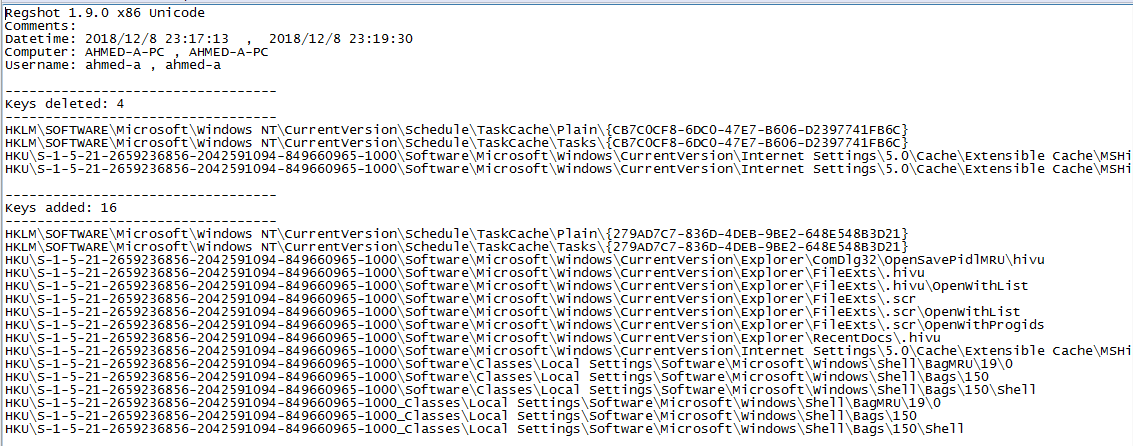


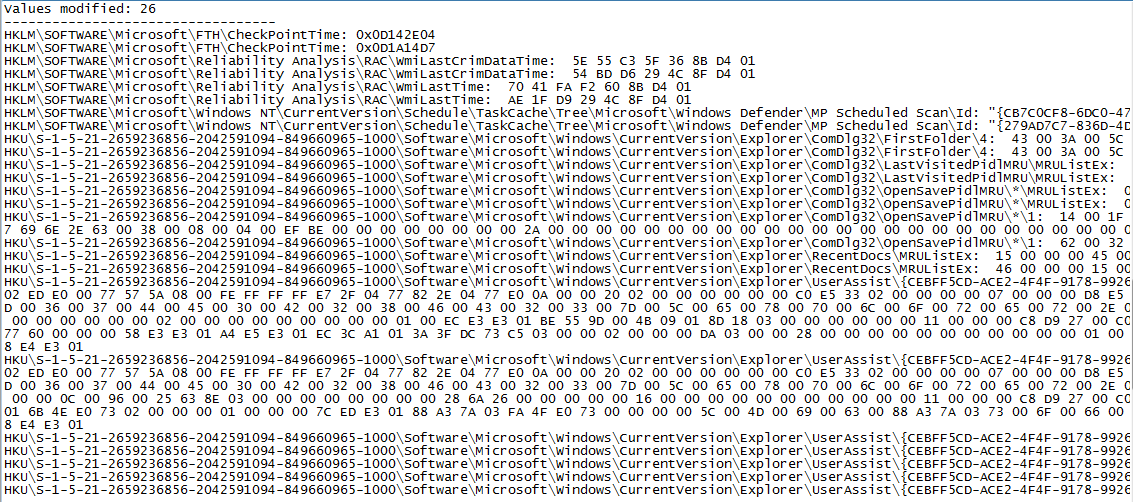
Options Autorun:  
  
  
  
Clicking Jump to Entry to delete the registrykey



Regshot tool: a tool that is takes a snapshop of your registry and then compare it with a secondone.

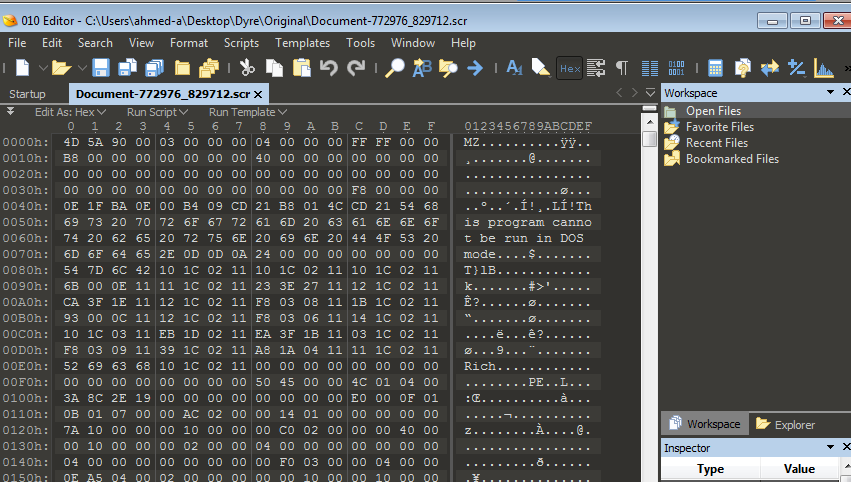


Description of add, delete, and modify registry keys.





010 editor: a tool that is a hexeditor



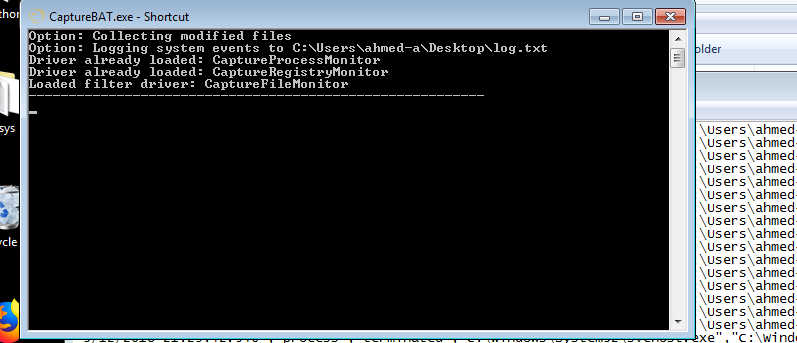
MZ file header which means its a dos executable



PE file header



Capturebat:



Using Capture-bate we were capable of creating a log file. The log file shows the time and operation of executable. As shown it was writing registry keys and starting up a process.

