Windows Investigation

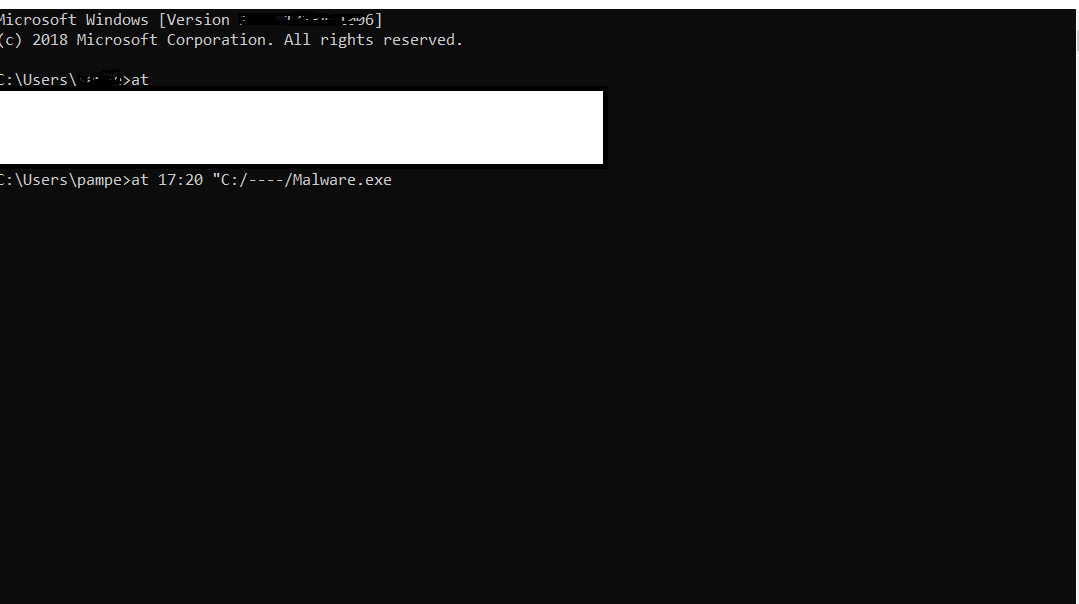
Andrew Maddox

University of Advancing Technology

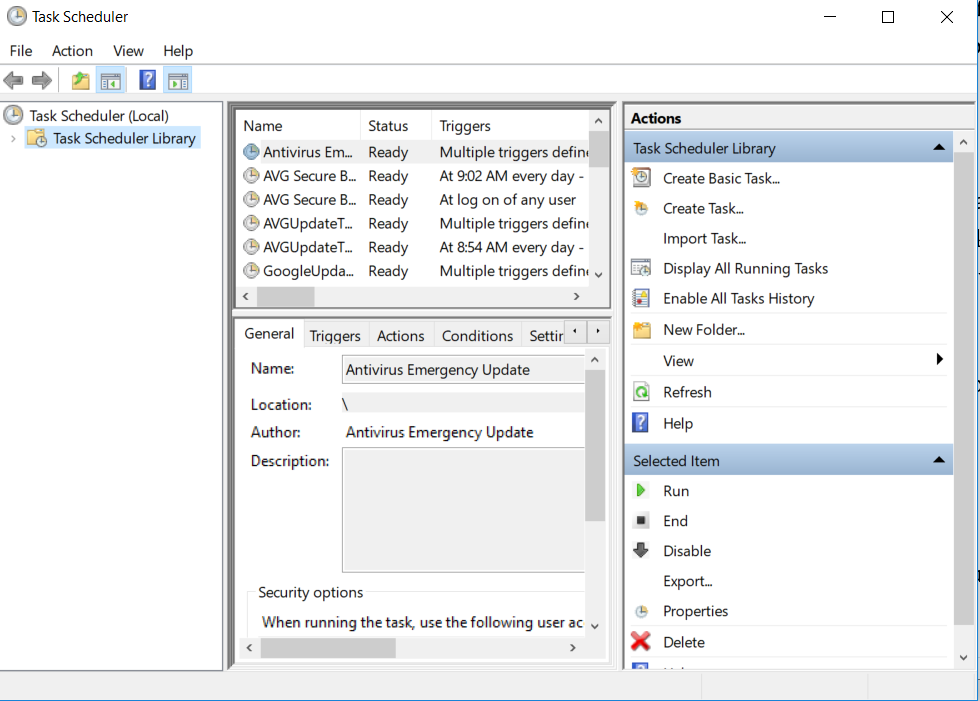
Windows Investigation

The first area of investigation is the Task Scheduler according to the book procedure. This shows the creation of a task in task scheduler. Creation of tasks can be done with at command and schtasks command. Tasks can also be accomplished through the GUI interface for task scheduler. The viewing of these files (Job Files) can be done through a hex editor or other means. A tool called Jamie Levy’s jobparser.py can be used also to achieve information of .job files. Analyzing .txt files involving scheduled tasks can be viewed but are encoded in Unicode.

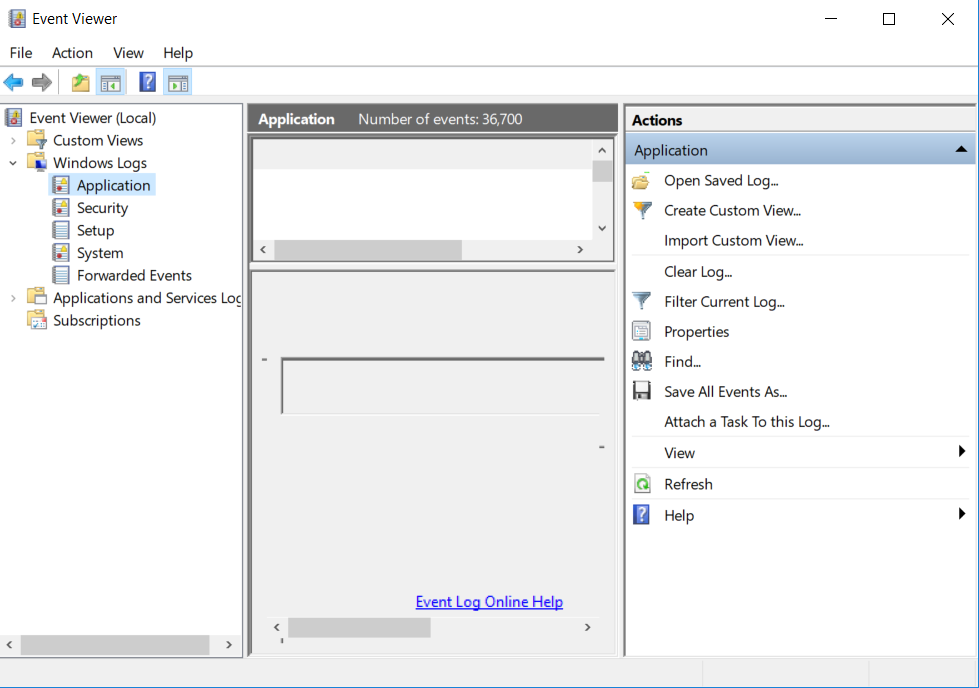
Example of creation of a task in command line user interface.



Example of Task Scheduler.

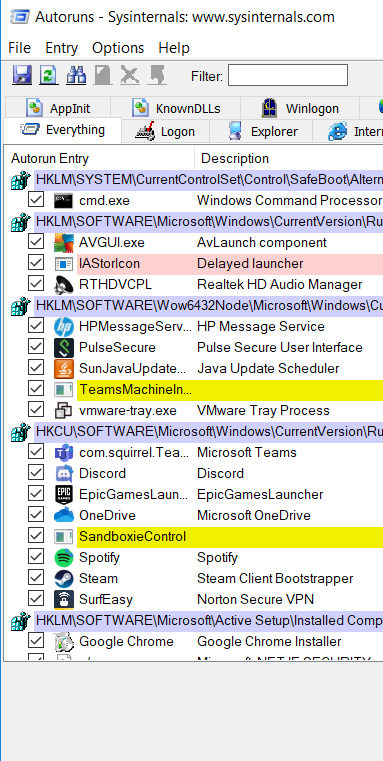


Example of Event Viewer.



Registry Analysis Tools

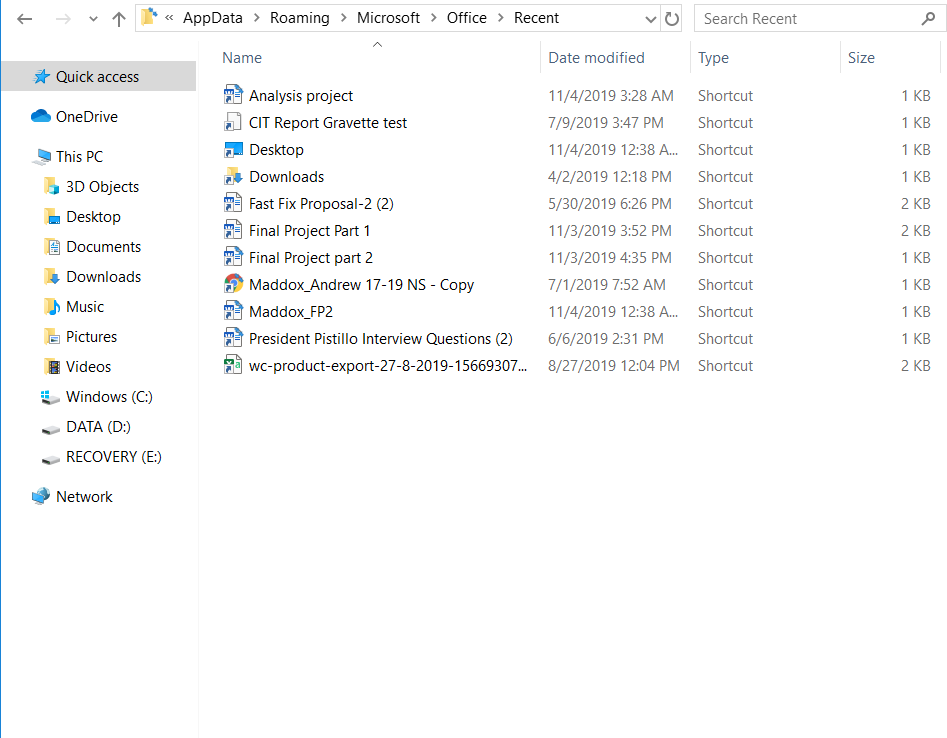
Autoruns is the tool that I will be using for the registry analysis tools section of this assignment. This tool was chosen because of the easy to use aspect, and the popularity support and features of the tool. Using autoruns to view the processes was very inciteful and thought provoking as these are not areas you commonly would search in. Nothing major of excitement was found on my personal machine but digging deeper and analyzing this area was definitely beneficial.



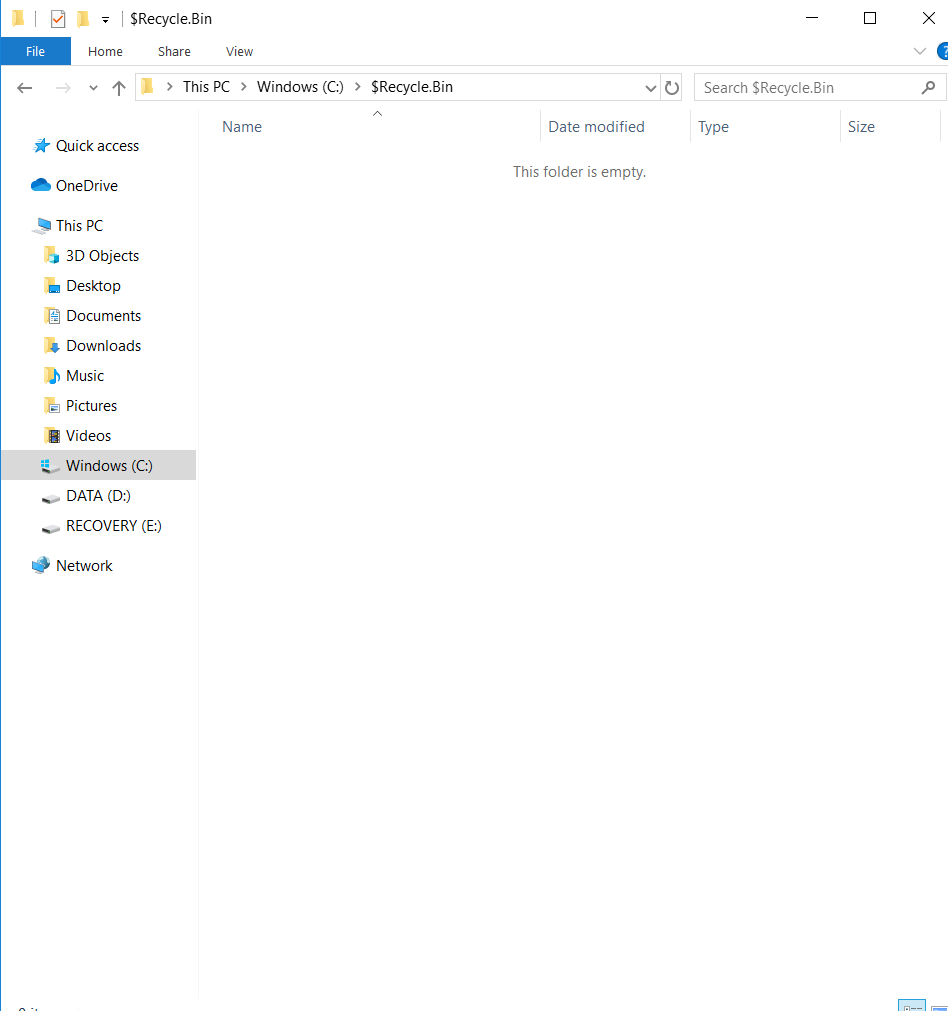
LNK Files and other artifacts

The recycling bin is a tool used in and comes with windows as a form of holding files before deletion. This has a hidden subdirectory and has specific user access. The metadata is held in a hidden file \Recycler\<SID>\INFO2

This is a picture showing the recent files in the %appdata%/appdata roaming Microsoft office recent section folder.

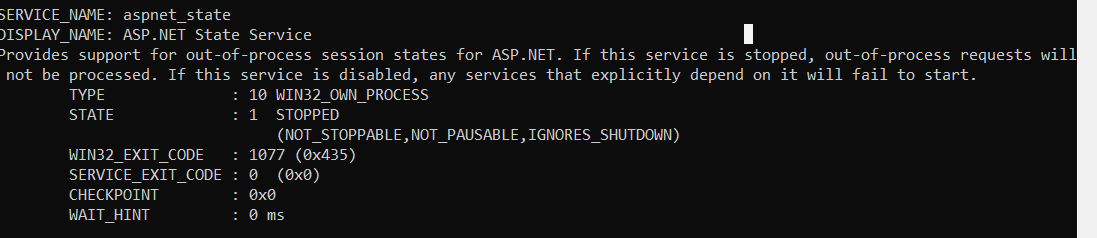
.

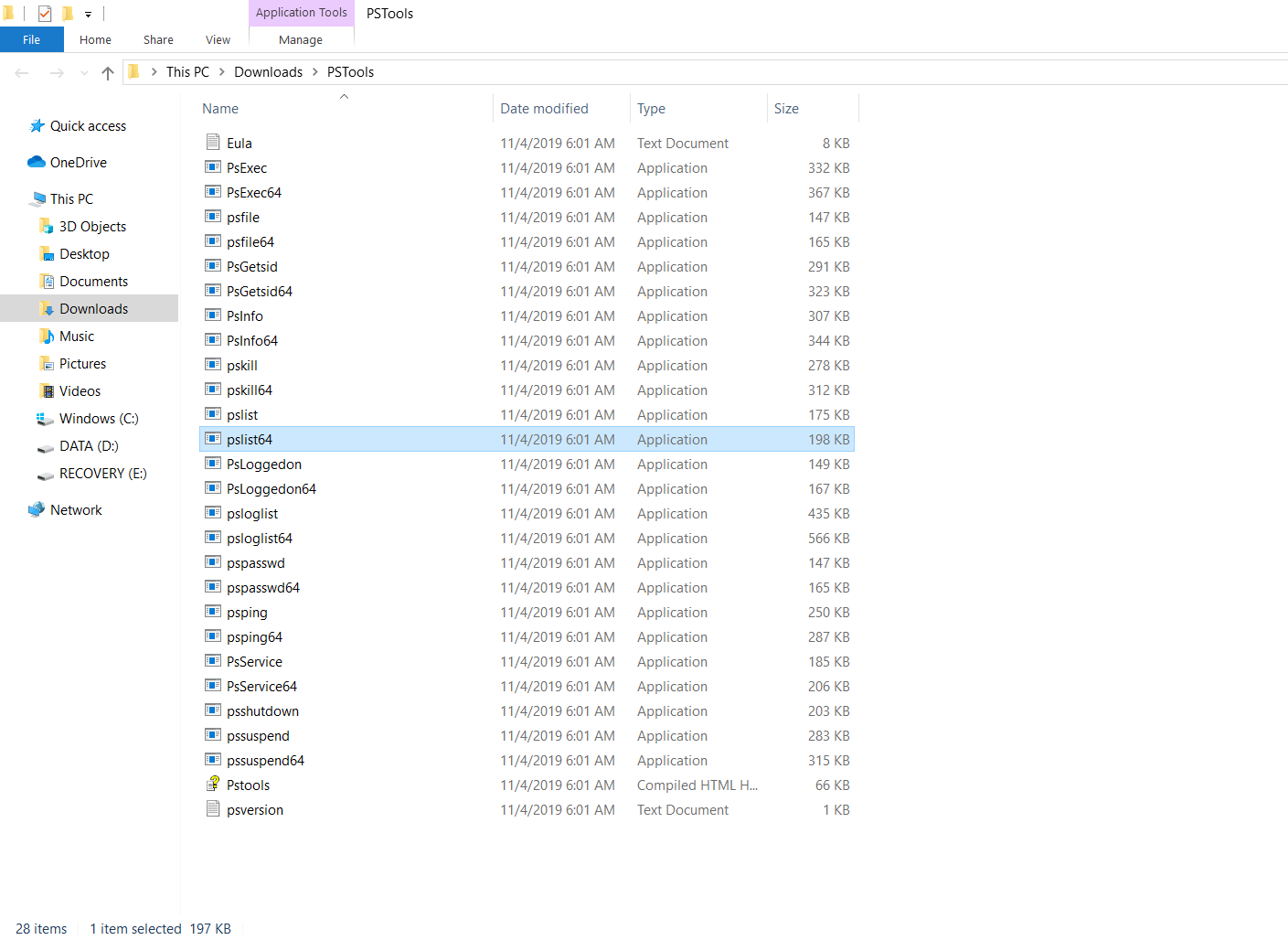
This is a picture of the recycle bin.



Memory Analysis

One of the tools that will also be used for Memory Analysis is pstools, pslist. Another interesting tool of interest that I investigated while using these tools was the psservice tool. This showed services running whether or not they could be stopped and information about the services themselves.





References

Incident Response & Computer Forensics, Third Edition Page 12-13