**Research Journal**

**3rd December 2019**

What worked?

Got the dump file for LastPass process from the TaskManager. The dump file is in .DMP format. Its native to Windows. Then, used Volatility forensics tool to convert the .DMP file to .raw format. Specifically, imagecopy plugin for Volatility did the conversion

Why .raw?

Raw memory dump is the most commonly used memory dump format by modern analysis tools. Raw file formatted memory dumps do not contain headers, metadata, or magic values.

The raw format typically includes padding for any memory ranges that were intentionally skipped (i.e., device memory) or that could not be read by the acquisition tool, which helps maintain spatial integrity (relative offsets among data)1

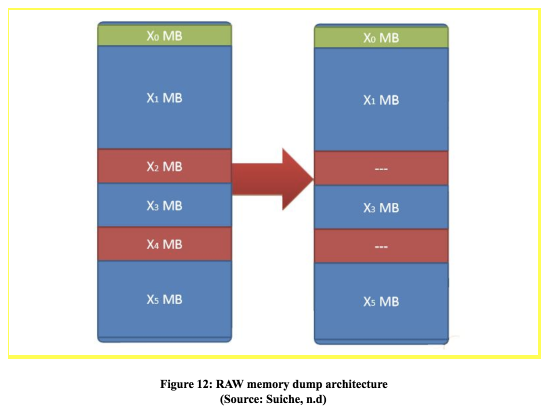
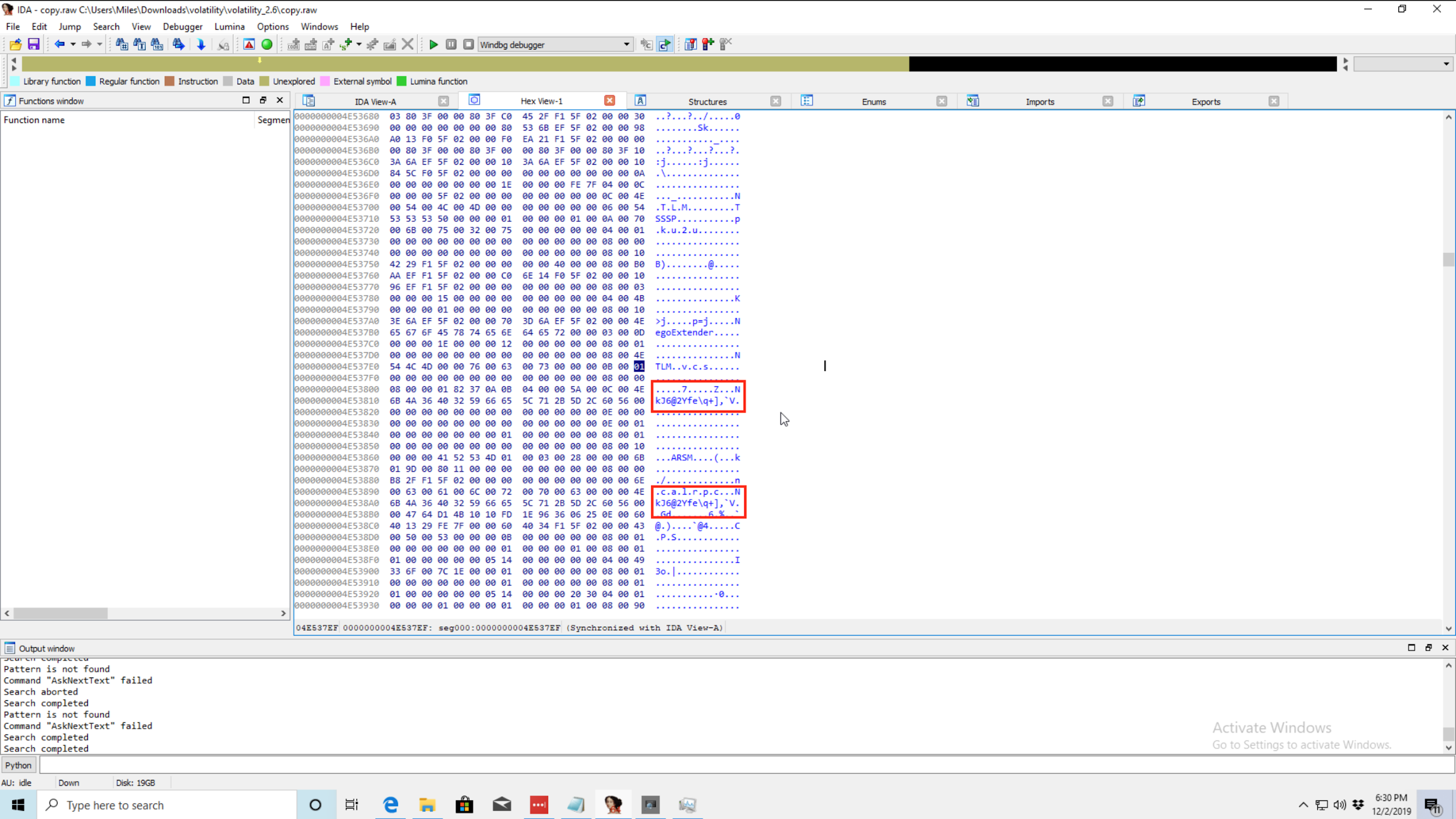


Image taken from https://articles.forensicfocus.com/2018/02/08/memory-dump-formats/

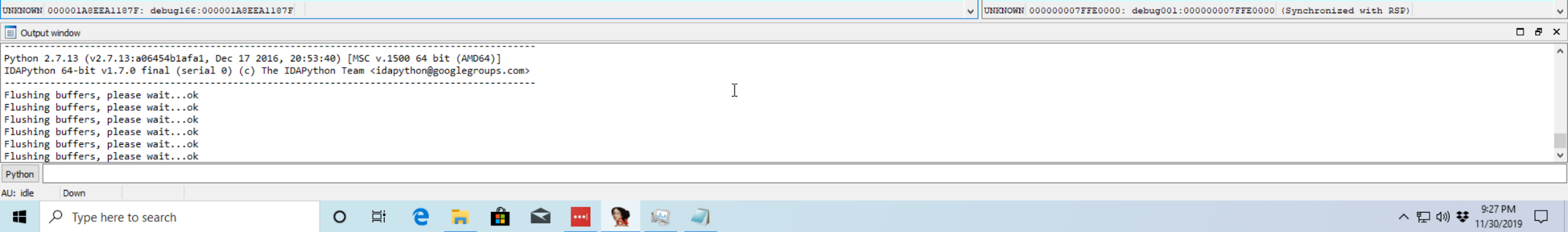
Use Interactive Disassembler Tool (IDA) to open the raw dump file of LastPass in the running state as a binary file. We get to see a hex-view of the memory along with the contents stored in it in ASCII format.

We searched for strings in the ASCII contents. We searched for substring of the master password and found it in memory in plaintext, more than once in quick succession.



This was the case when LastPass was in a “locked” state. That is, logged out of LastPass and created a dump file and looked at the memory in IDA. The master password was still present in the memory.

Attached WinDbg to LastPass to try understand the execution sequence and system calls made by LastPass for operations, we repeatedly see that LastPass is flushing buffers regularly but still the master password was present in clear text.



We did not find any saved passwords in memory in clear text.

What did not work?

Tried **mimikatz** tool to extract any clear text passwords from dump files of LastPass process.

References:

#### Courcier, S. (2018). *Memory Dump Formats*. *Forensic Focus - Articles*. Retrieved 3 December 2019, from https://articles.forensicfocus.com/2018/02/08/memory-dump-formats/