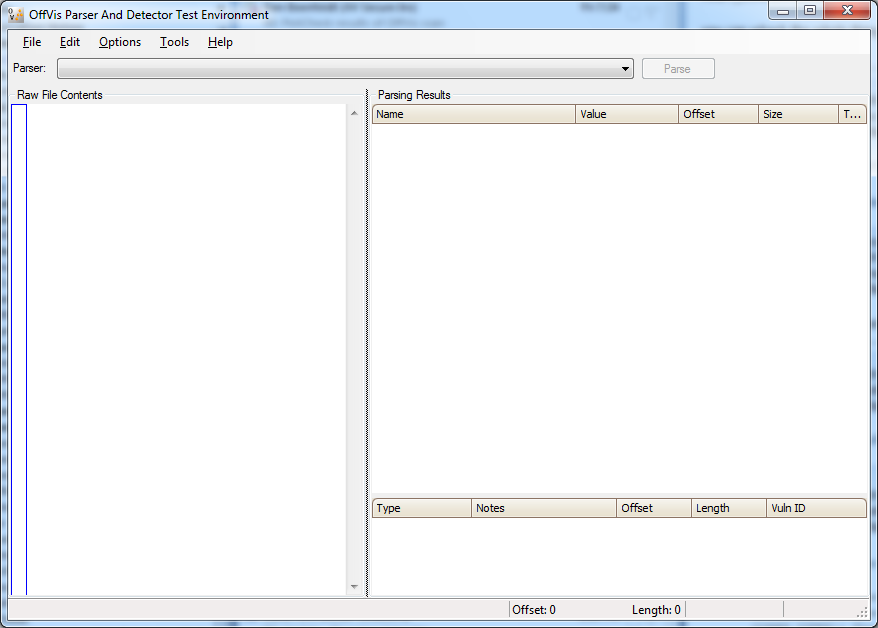
OffVis is an Office binary file format visualization tool.  We released it to help IT Pros, security researchers, and malware protection vendors better understand the binary file formats to deconstruct attacks and understand the vulnerabilities we fix for protection purposes.  It’s an easy GUI to use to generically browse around and show the bytes on disk (left half of screen) with the hierarchical view of the file as Office parses it (right half of screen).  It can also generically detect a handful of publicly-exploited vulnerabilities as it reads the file.

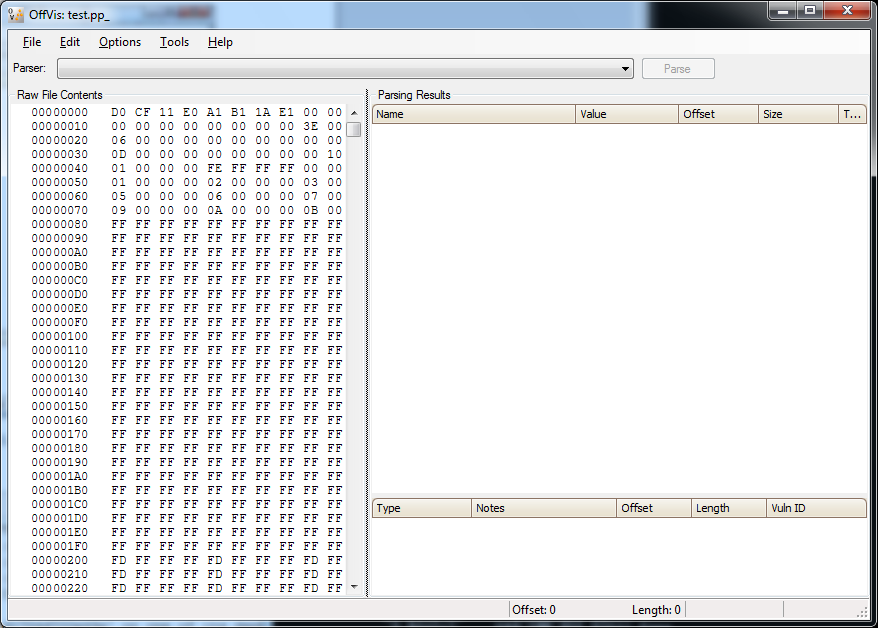
**Typical Usage**

1 - Extract the ZIP file contents to a directory

2 - Launch OffVis.exe. It will come up with a UI that looks like this:

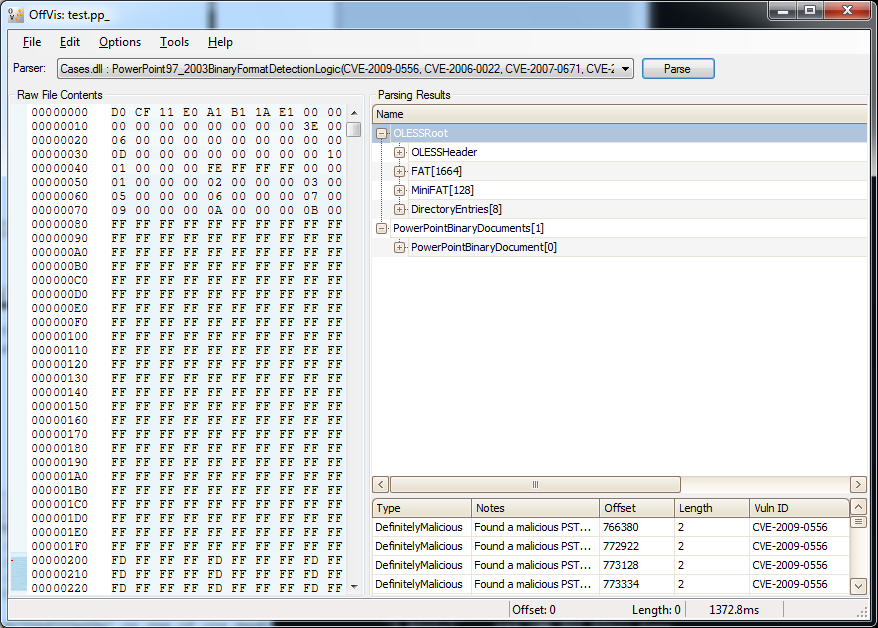


3 - Under File menu, click "Open Data File", open a DOC, XLS, or PPT file.

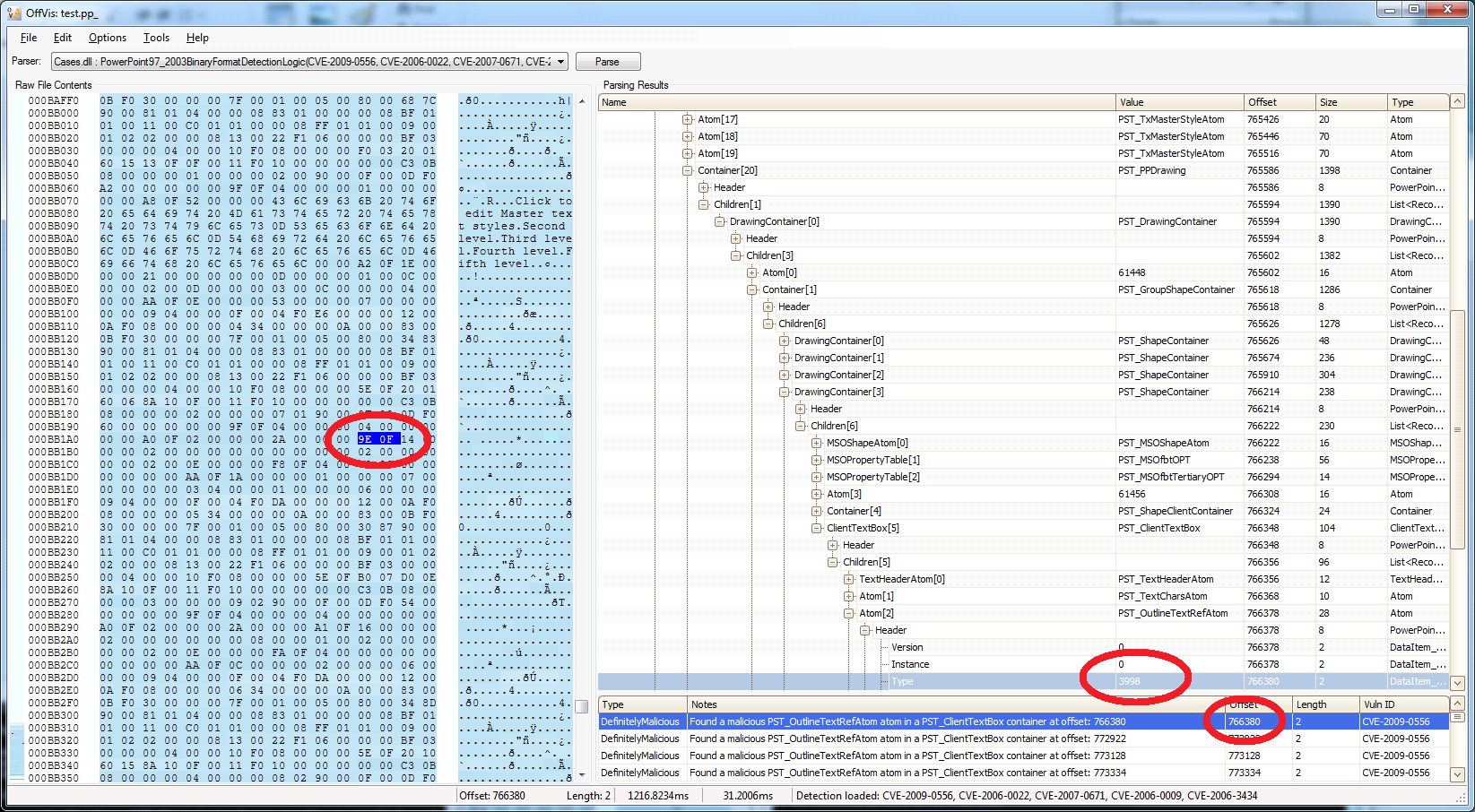


4 - Choose a "Parser" from the drop-down list. If you'd like to parse only at the OLESS layer, choose "Format Library.DLL: OLESSFormat". If you'd like to attempt to parse the file as an Excel, PowerPoint, or Word file, select one of those parsers.

5 - Click "Parse". (This may take a moment)



6 - You can double-click most any element on the right half of the screen and the hexview will highlight that value. The example above was a malicious file that attempts to exploit CVE-2009-0556. Double-clicking the "DefinitelyMalicious" row will highlight the element in the treeview in the upper right and also the exact value in the hex view on the left.



In the example above, a PST\_OutlineTextRefAtom starting at offset 766378 (hex BB1AA) has a "Type" in its header with value 3998 (hex 0xf9e). This triggers the detection logic for CVE-2009-0556.

Please send any questions to switech@microsoft.com. Thanks!

Microsoft Security Response Center - Engineering team