

LA CIUDAD ([HTTP://WWW.LACAPITALMDP.COM/CATEGORIAS/LA-CIUDAD/](http://www.lacapitalmdp.com/categorias/la-ciudad/))

6 de December de 2014

 (<http://www.facebook.com/la.capital.mdp>)  (<https://twitter.com/lacapitalmdp>)  (<http://www.linkedin.com/company/lacapitalmdp>)  (<https://plus.google.com/115328162071421418964>)  (<https://www.youtube.com/channel/UCv0V1a-lacapitalmdp&lang=es>)

## Investigadores locales mejoran una herramienta de informática forense

Se trata de alumnos de la Universidad Fasta. Esta mejora permite que el análisis se realice en un 10% menos de tiempo en situaciones normales y hasta 5 veces más rápido en situaciones extremas.

En el marco de los proyectos de investigación y desarrollo de tecnología del Grupo de Informática Forense de la Universidad Fasta, se lograron mejoras sustantivas en el rendimiento de una de las herramientas más avanzadas de análisis forense de memoria en el mundo: Volatility.

Volatility es la herramienta líder en análisis forense de memoria a nivel mundial. Es de licencia GPL y cuenta con un equipo de desarrollo activo que la mantiene actualizada.

En agosto de 2014, se publicó el release 2.4 de Volatility y el equipo de investigación de Informática Forense de la Facultad de Ingeniería comenzó a utilizar la herramienta, detectando situaciones en las que su rendimiento era muy pobre. En un par de semanas de análisis de desempeño y pruebas, se lograron optimizar las funciones más costosas en términos de performance, bajando el tiempo de procesamiento de un caso testigo de 2 horas y media con el código original a solo 10 minutos con la versión mejorada por el ingeniero Bruno Constanzo.

A sugerencia de Michael Ligh, miembro del equipo de desarrollo de Volatility, las mejoras propuestas por el Grupo de Informática Forense (7 en total) fueron subidas al repositorio oficial en GitHub. Cuatro de esas mejoras están en fase de evaluación, una fue descartada y 2 ya fueron adoptadas e incluidas en el próximo release. Esta mejora permite que el análisis se realice en un 10% menos de tiempo en situaciones normales y hasta 5 veces más rápido en situaciones extremas.

La mejora de Volatility es muy importante y fue posible gracias al conocimiento desarrollado sobre forensia en memoria, especialmente a partir del proyecto final BIP-M "Búsqueda de Información de Procesos en Memoria", de los alumnos Gonzalo Ruiz de Angeli y Juan Ignacio Alberdi, dirigido por el Ing. Constanzo.

Esto pone en evidencia la calidad del trabajo de investigación del Grupo de Informática Forense de la Universidad y el nivel de "profundidad y eficiencia" de los proyectos finales de la carrera de Ingeniería en Informática, donde investigadores y alumnos logran optimizar el desempeño de una de las mejores herramientas del mundo en la temática.

Suplemento especial  
142° aniversario  
de Mar del Plata



DESCARGALO ACÁ

([http://www.lacapitalmdp.com/descargas/pdf/MDP\\_142\\_aniversario.pdf](http://www.lacapitalmdp.com/descargas/pdf/MDP_142_aniversario.pdf))