REnigma is a software licensed by John Hopkins University that allows users to execute malware within a virtual machine and record and analyze its behavior so that its security threats can be thoroughly understood and prevented in a live situation. This software has many benefits; it offers a sandbox environment in which the full effects of a malware can be realized in order to be fully understood, it can also be done at the leisure of the researchers as the program logs all changes brought about from the viral program to be reviewed later, and it eliminates the need for manual reverse reengineering on the part of the researchers as the program can essentially be rewound to a specific point in time to allow for further testing. In practical use, the program can be utilized by security organizations to test and develop new preventive security measures and patch in existing security holes in any virtual environment so as to avoid future threats. It can also be used reactively to any new unexpected attacks in order to quickly patch the problem and develop solutions.