

# DDoSDB

## Post-Mortem Analysis for Improving DDoS Attack Detection and Mitigation

José Jair Santanna  
University of Twente  
Netherlands  
j.j.santanna@utwente.nl

### ACM Reference Format:

José Jair Santanna. 2018. DDoSDB: Post-Mortem Analysis for Improving DDoS Attack Detection and Mitigation. In *Proceedings of ACM Conference (Conference'17)*. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

## 1 INTRODUCTION

## 2 POST-MORTEM DDOS ATTACK ANALYSIS

The goal of this section is to present how to extract only the attack vectors g

For a post-mortem analysis of the DDoS attack.

The workflow for collaborating with DDoSDB is composed of three modules: (1) the attack vector identification, (2) the attack vector extraction, and (3) the DDoS signature generation for specific technologies. In the attack vector identification module performs consecutive filters

and replacement of the victim's IP address

---

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

*Conference'17, July 2017, Washington, DC, USA*

© 2018 Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00

<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

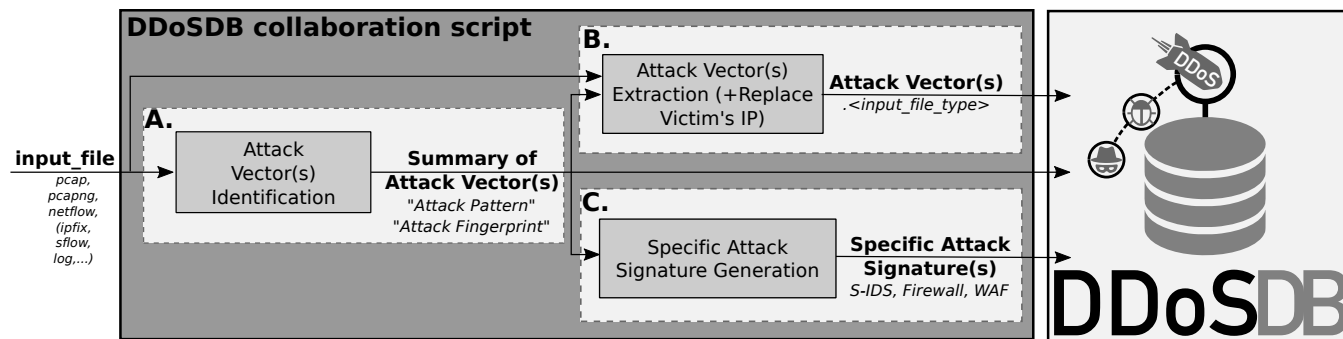


Figure 1: DDoSDB collaboration module