

# DDoS Filtering Tool

## A Design Paper

José Jair Santanna and Julik Keijer

University of Twente, the Netherlands  
j.j.santanna@utwente.nl, keijerjs@gmail.com  
<http://ddosdb.org/ddosfiltering>

## 1 Introduction

Process a large volume of data “at home”.

## 2 Collaborators Requirement

MAIN REQUIREMENTS:

- Facilitate the removal of any private information that can be potentially used for identifying either the collaborators or their clients;
- Generate a summary information of source IP addresses that were potentially involved in the attack;
- Use the summary information of source IP addresses to classify the attack type;
- Generate a summary of the attack;
- Generate a new network file with only the filtered IP addresses attack records.

ADDITIONAL REQUIREMENTS:

- Process the traffic at the collaborators’ infrastructure to avoid leak of information;
- Facilitated the deployment of the filtering tool;
- Speedup the loading process of visualizations;
- Create simple and meaningful visualizations;
- Have a dynamic (and manual) filtering interface;
- Highlight outliers.

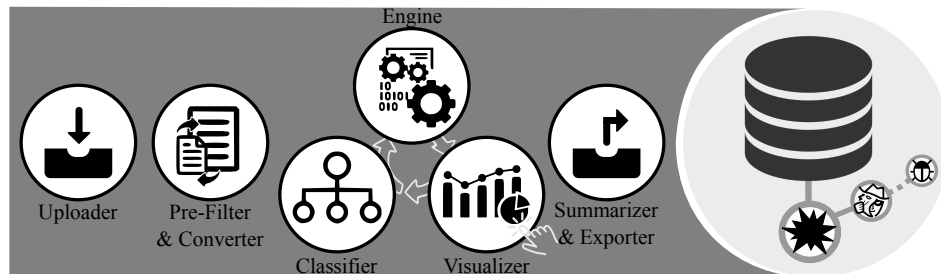
## 3 Tasks & Design Decisions

The achieve the majority of the requirements of collaborators we identify the following tasks:

1. Receive an uploaded network file that contains a DDoS attack (pcap[ng] or nfdump types);
2. Pre-filter the uploaded network file keeping only the ingress traffic;

3. Highlight the potential attack targets, i.e., the destination IP addresses that received more network traffic);
4. Highlight the IP protocol that generates more network traffic towards the highlighted destination IP address;
5. Present summarized information of source IPs that sent traffic using the highlighted IP protocol;
6. Highlight (and manually remove) the source IPs that does not follow an attack pattern (outliers);
7. Classify the set of remaining source IPs as a type of DDoS attack;
- \*8. Use the set of remaining source IPs to filter the pre-filtered traffic (output of step 2) towards identify multi-vector attacks;
9. Repeat steps 3, 4, 5 and 6 until the collaborator is satisfied about the remaining information;
10. Generate a new network attack file with only the remaining information;
11. Export the new network attack file and the summary of the attack to DDoSDB.

We decided to split the tasks in five main modules, depicted in Fig 1: (i) input, (ii) processing, (iii) visualization, (iv) classification, and (v) output. Additionally, we include an extra module named conversion to optimize the processing module. Each module is detailed in the further subsections.



**Fig. 1.** DDoS filtering tool modules.

### 3.1 Input Module

#### Requirements

#### Design decisions

### 3.2 Conversion & Prefiltering Module

#### Requirements

**Table 1.** Attack information shared by initiative.

	Information	Obtained	[?]	[?]	[?]	[?]	[?]
1	Start time	field	✓	✓			
2	Duration	field*	✓				
3	Bit rate (peak)	field*	✓				
4	Packet rate (peak)	field*					
5	# Src. IPs	field*					
6	# restricted Src. IPs	enrich					
7	# Src. IPs with fragm.	field					
8	Src. port (interval)	field	✓				
9	Dst. port (interval)	field	✓	✓			✓
10	Attack type	heuristic	✓	✓	✓		✓
11	+Spoofed attack type?	heuristic					
12	+Fragmented attack type?	heuristic					
13	+Reflected attack type?	heuristic					
14	Attack responsible (blame)	manual					
15	Dst. IP	field			✓		
16	Dst. IP country	enrich	✓	✓	✓	✓	
17	Dst. IP City	enrich		✓			
18	Dst. IP ASN	enrich		✓			
19	Src. IP	field		✓	✓		
20	Src. IP country	enrich	✓	✓	✓	✓	✓
21	Src. IP city	enrich		✓			
22	Src. IP ASN	enrich		✓			
23	Src. IP # total packets	field					
24	Src. IP # frag. packets	field					
25	Src. IP data rate	field*					
26	Src. IP packet rate	field*					
27	Src. IP restricted?	enrich					
28	Src. IP packet length	field					
29	Src. IP TTL	field					
30	Src. IP TCP flags	field					
31	Src. IP HTTP payload*	field					
32	Src. IP DNS query	field					
33	Src. IP open ports	enrich					

Design decisions

### 3.3 Processing and Visualization Module

Requirements

Design decisions

### **3.4 Classification Module**

#### **Requirements**

#### **Design decisions**

### **3.5 Output Module**

#### **Requirements**

#### **Design decisions** Web-based that performs offline filtering;

## **4 Preliminary results**