Real Time Analytics of DNS packets using Apache STORM

Lightning talk

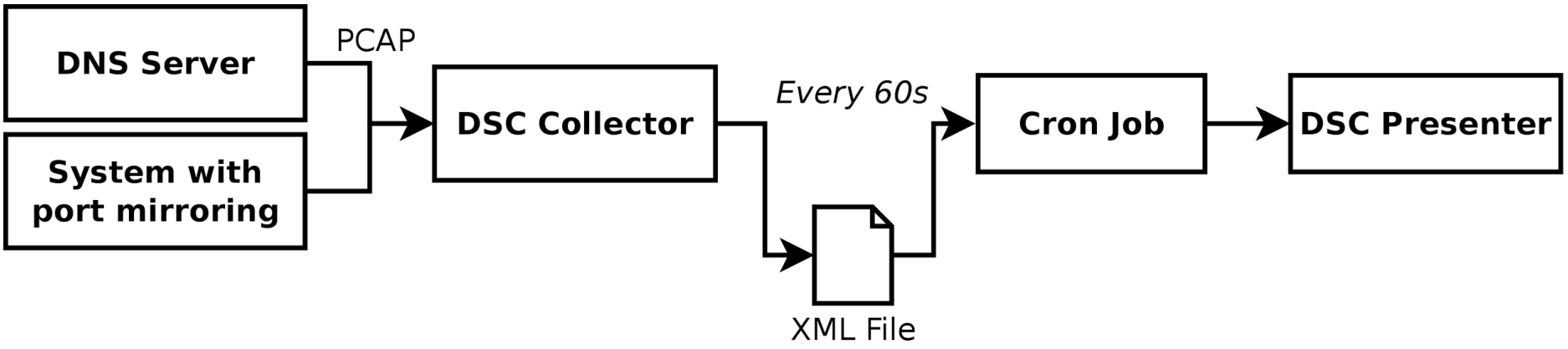
Francisco Cifuentes
francisco@niclabs.cl

State of the Art

BumbleBee

These are DSC presenters!

DSC: A DNS Statistics Collector



What's Apache Storm!?

"Apache Storm is a (…) distributed realtime computation system."

https://storm.apache.org/

What it is used for!?

“Storm has many use cases: realtime analytics, online machine learning, continuous computation, distributed RPC, ETL, and more…”

https://storm.apache.org/

What it is used for!?

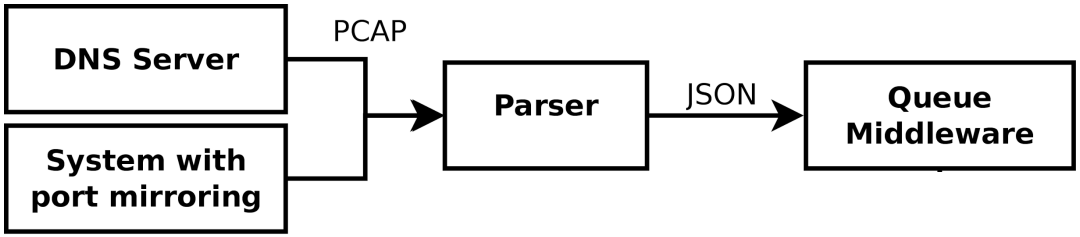
And many others...

What it is used for!?

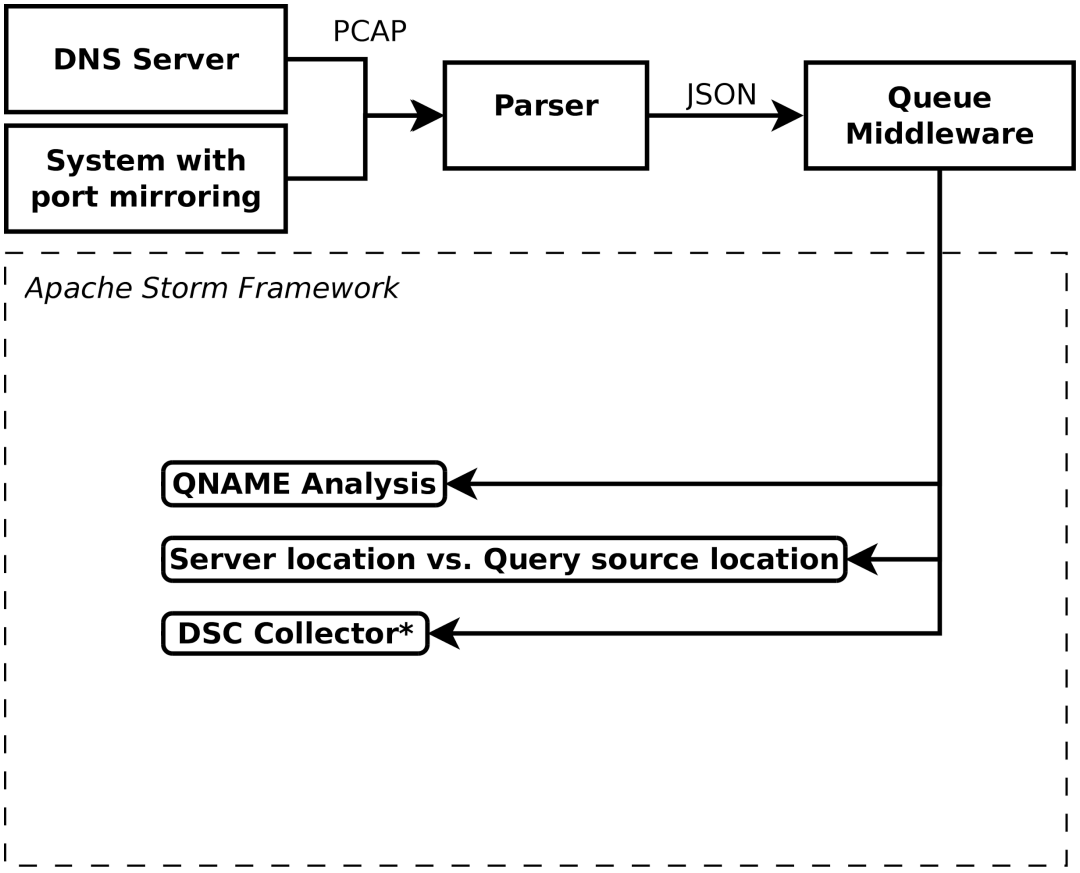
“One example is security monitoring where we are leveraging Storm to analyze the network telemetry data of our globally distributed infrastructure in order to detect and mitigate cyber attacks”

http://storm.apache.org/documentation/Powered-By.html

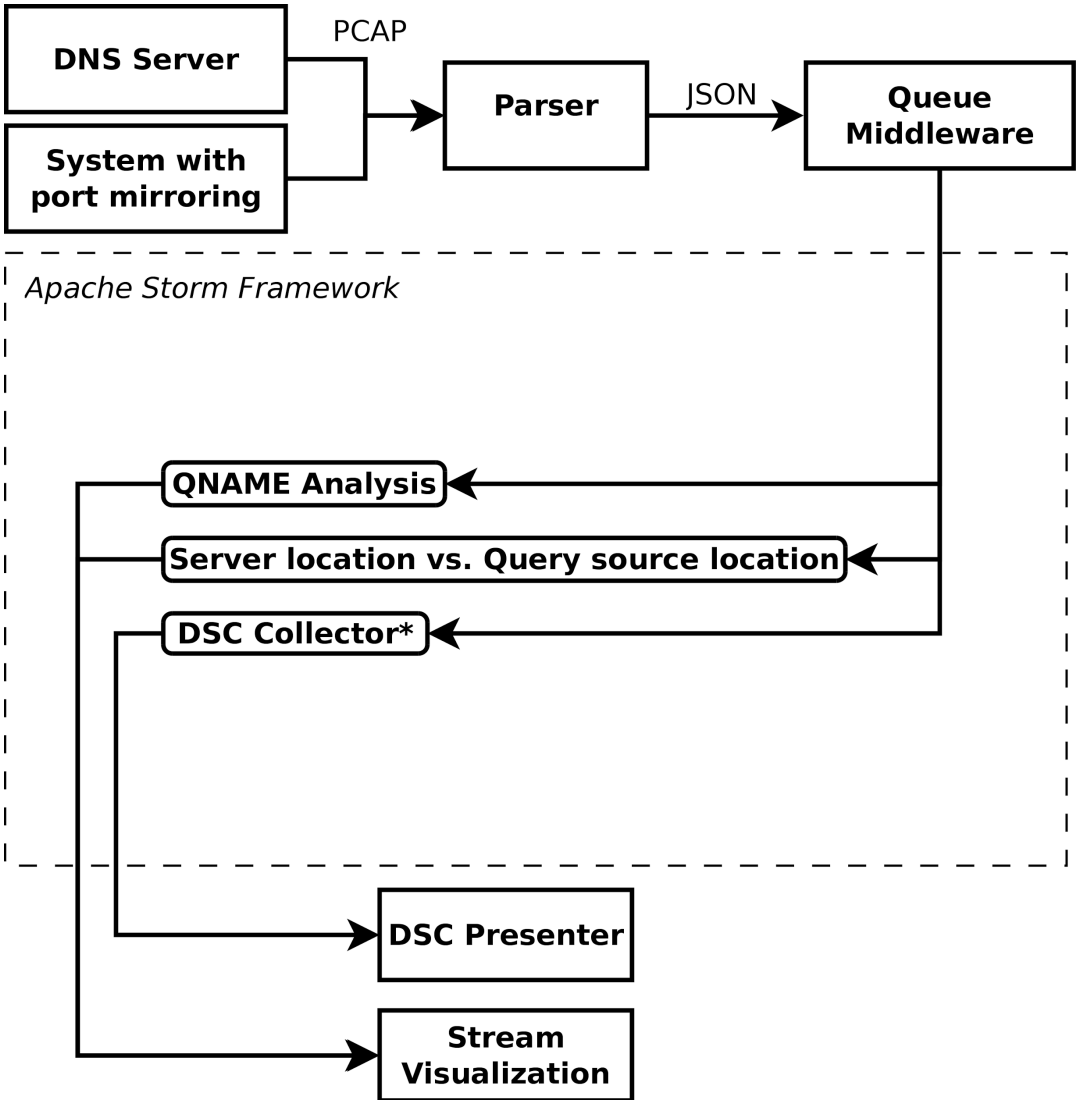
Proposed Architecture



Proposed Architecture



Proposed Architecture



Inspiration

emojitracker: realtime emoji use on twitter

682182092	510231506	310228658	291180060	265514148	217734221	214792959	206463404	204981578	202892724
190720918	188240449	166253133	150403243	144957659	98865958	96871814	95661514	94979231	87325730
84762525	81895524	80823368	77264443	70310643	68262692	67006918	63972895	63405448	60030272
58849703	57839238	56963214	56805644	56709218	55056998	54726346	54426735	53412310	52270809
51588095	51086591	49522011	48709125	48299574	47547304	45526816	43346308	42092947	41567318
41304209	41008226	39682797	38419048	37481035	37196347	35803227	35210976	34673468	32462028
31699021	31450788	31333565	29800902	29740452	29163728	28528718	28476550	26958181	26315903
24791764	24443931	23738159	23679518	23016477	22409341	22373303	22365316	22265170	21643462
21357601	20975413	20939432	20609303	20482218	20415539	19736566	19103166	18584122	18428489
18359568	18222633	18113898	17767851	17024825	16955540	16416171	14966286	14674883	14576565
14462397	14367148	13708465	13481506	13444434	13345653	13177368	13117552	12818016	12074500
11944513	11782259	11671876	11511973	11388156	11085191	10791147	10562097	10548510	10508874
10498875	10400482	10356395	10304498	10061666	10033611	9770096	9756582	9695215	9667585
9621791	9611301	9545558	9525743	9263185	9228379	9112377	9088960	8898958	8818676
8788692	8773498	8565514	8380752	8121308	7991140	7800381	7668300	7292781	7253755
7246275	7217272	7212098	7210377	7063625	7044714	7036246	7026229	7006373	6950208
6914490	6908741	6881880	6879372	6877677	6809689	6724757	6697997	6515685	6353757
6277043	6080973	6036068	6008864	5981023	5915603	5902928	5888225	5873236	5843741

Inspiration

Some choices reasons

- Why do we need real time analysis?
- Why Apache Storm?

What has been done

- DNS Packet Parser.
- Tested different topologies.

Suggestions / Ideas accepted!

Francisco Cifuentes

francisco@niclabs.cl

http://ratadns.niclabs.cl