## Container Code Classification

Gao, Jeremy, Kostas, Ozan, Rahul

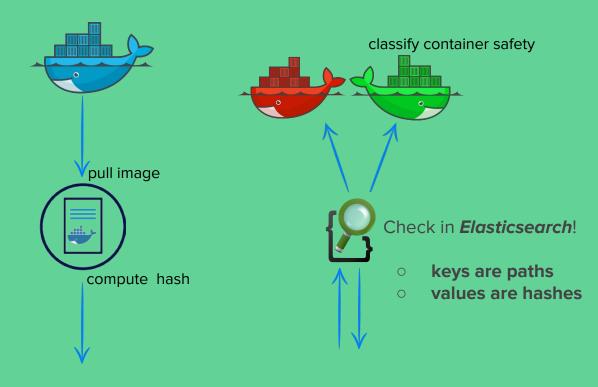
Mentor: Sastry S Duri (IBM Research)

#### Reminder:

1. Retrieve

2. Hash

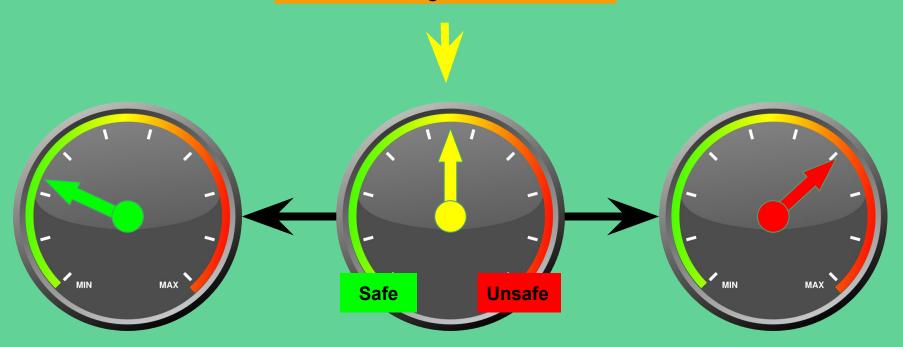
- 3. Compare
- 4. Classify



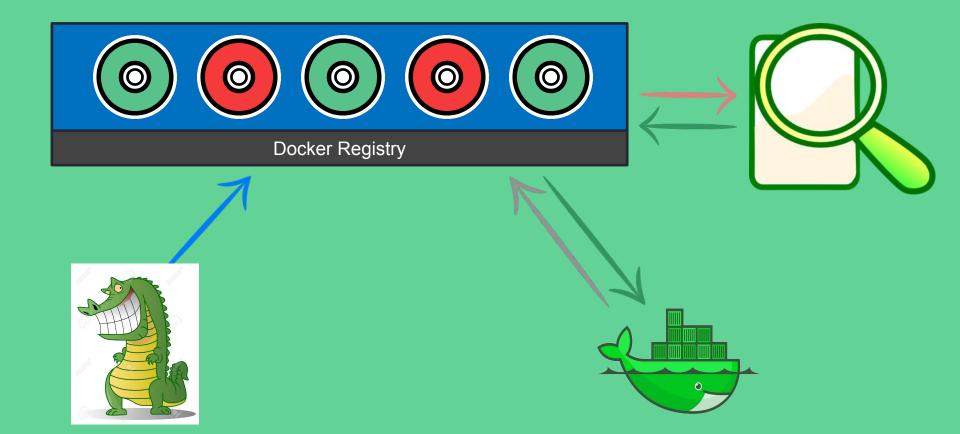
FAAAAAICAAARUAAAAAAAAAAAAAACEAAQQCAAAQAAkAAEAQAAJAAAgEAAgIIABIQA AAAAOEBAgAAABABAAAAAAAAEAgAAgAAACAIAAAEAAAAAAAABAAACAAAAAAGDAA AAAAAAAAgAABAAgAAAACQAAIAAAAAAAAAAAAAAAAAAAAAQAAAQAA QBAEAAKAACAAAAAAGDAAAAAAAA

# Classifying safety

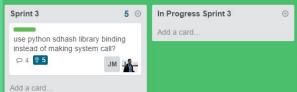
Docker Image or container



### Usecase 1: Suspicious Images



#### What we've done:



#### So Far (Sprint 3):

Implemented use case 1



Setup RabbitMQ to Queue hash tasks

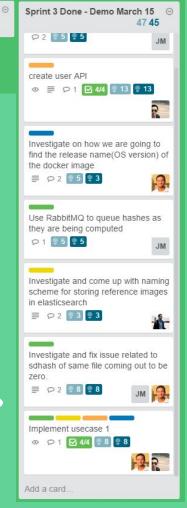


Implemented part of flask API for user

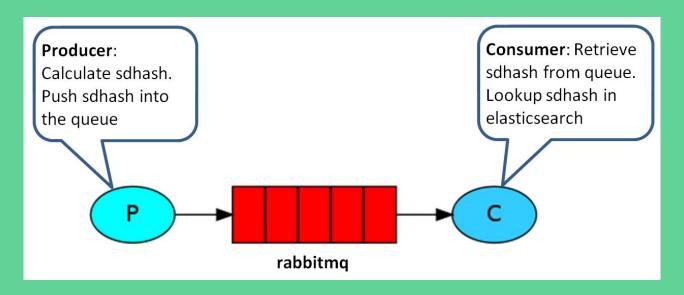


Integrated image push with hash-calculation



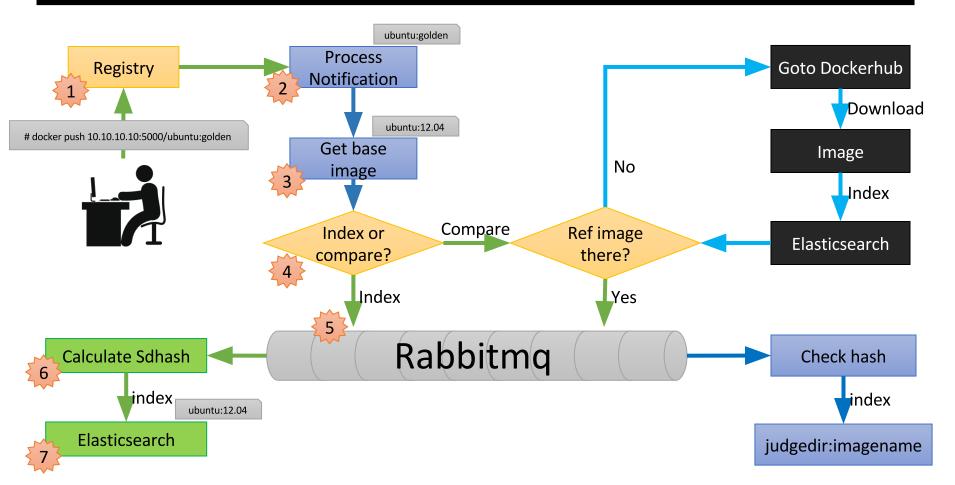


#### On RabbitMQ:

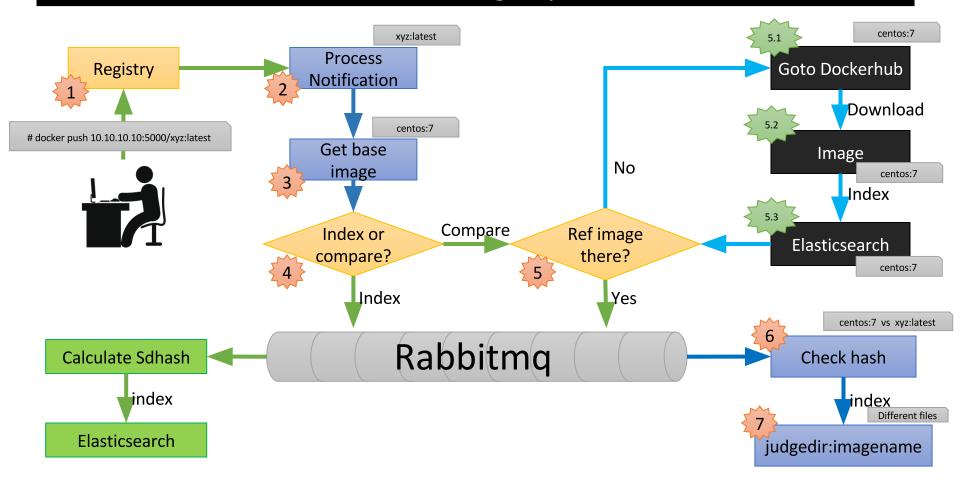


- Producer and consumer run in parallel
- There can be multiple producers and consumers for single queue
- RabbitMQ server can be hosted separately from producers and consumers

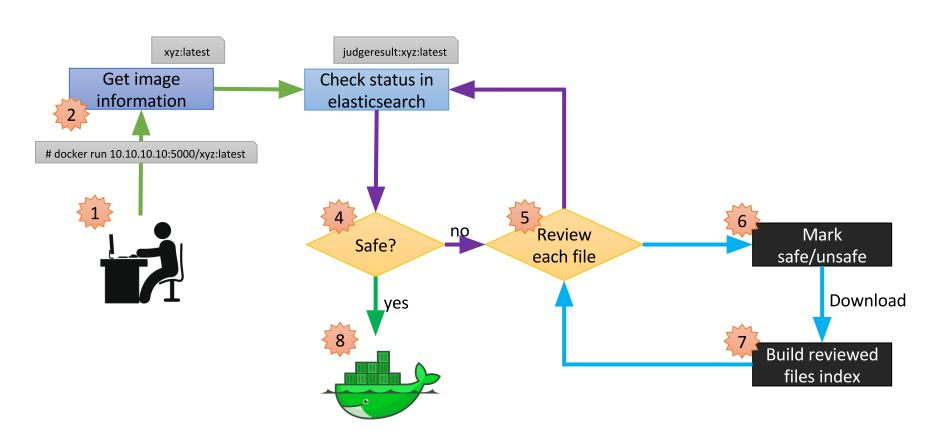
#### Flow for indexing an image



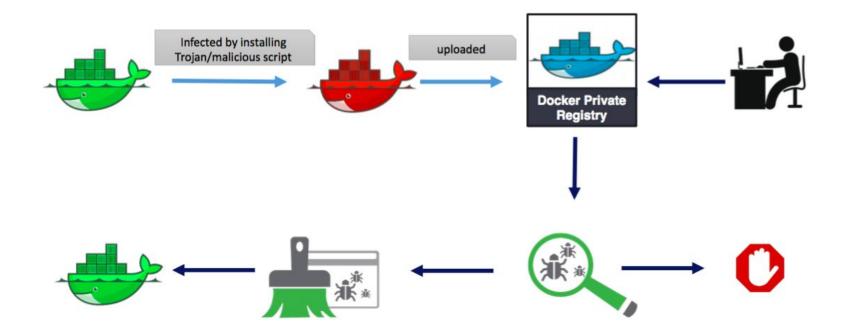
#### Flow for image upload



#### Flow for launching new container



#### Demo flow



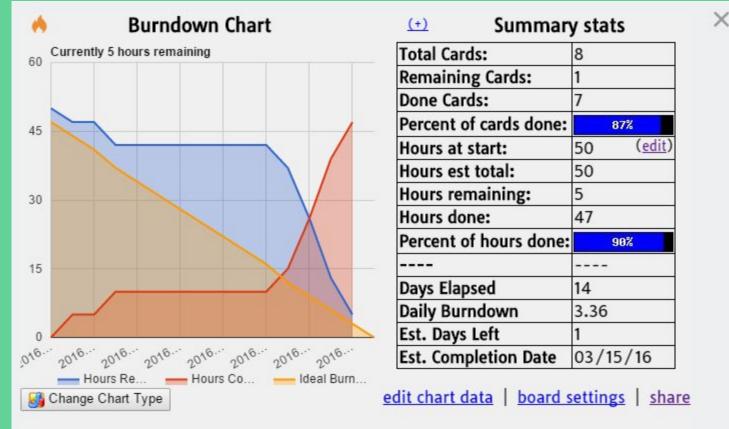
#### DEMO

```
1 121 2 4 5 6 7 c Tall 1 shouldbooms motion: "Pres, Solin, East about $45.55
                                                                    part at common man tricke to from a thickey of contact man - $2000 Clara ( French Lang Flacks PTS and the
 298x4.743x264936388**
                                                                         on squarkfilling
 convirus hayer - 1 ar#f16fa4253KeG75e9fx5q2279E36218cu7586432842c8
                                                                         * Resting on http://d.B.B.B.Sibbb/ (Press CTRLsC to quit)
 C1847744184-0809779*3
                                                                          metableMaterBase(27)
 Copyling Layer - 17, a stancistic 54157 Me Astheby 7876 to 986 to 57457 Frant
                                                                        $27, B. R. S. Cong. (25/Mary 2018. #81/94/51) "MET Jack. budge. mes/test. https://doi.org/10/
 171-2" ZWIL
 Coppley Layer - " a West attraction 24th characteristics
                                                                          mountable Market Black CETT
 C104F446c501c501c50163615
                                                                         9.39.38.11 - [15/may/2016 95:55:47] "NET /got_buller_res/test_lenge:latest
                     a" less 30+400xx4+g5+641+f3+42ctx00212x14454184740
 1971 11 2000
 (Stor PrintleSefeeber's
 our smoon ist unwritings as
penation kill corpora
18.18.18.7 - - [15/Mar/2810 18:82:28] "FOLT (Fail HTTS:1.1" 288 -
18:18.18.7 - (15:96-2916 10:82:28) 79057 (10:1 HTTP:3.1" 288 -
18:10:18:7 - [15:40=/2010 10:62:26] "FOST (NEXL HTTF/2:2" 200
18.10.10.7 - - [15:44ar/2016 10:82:20] "POST /test HTTP/1.1" 200
18.18.18.7 - 15.56a-/2016 10-82:28 "9057 /each HTTP/1.1" 288
11h/s80_04-Umax-gro/security/pex_dring.so match 1809.
                                                                                    membranical micker bay infected, reage 125, 18, 9, 145-3500 test, tour
ib/ski 64-linus-gnu/separity/pox.permit:so wotch 1985
librate 84-1 trus-grapher surfaty/per group as notice 1886
                                                                           ortogramme continue of ductor such 129.16.3 381: $200/text inspellatest
thright 64-lines greateneority/pure separatting motest 1889.
                                                                          he past refers to a repositiony (129.10.1.149 1888/test_inage)
hthrade, 64-first-graduresarity/pur, shells, so watch inth
                                                                          muta7228341 Newstree from infected image
(brail), 64-Etrus gru/secerity/pur, filter. so motch 100%
                                                                          TOTAL PROPERTY PROPERTY
                                                                          SECURITY MARKET From SECURITY
libratt, 64-finus-gen/security/pur_itress_se watch 1805
10/186,64-Cinus-Bray Security/Book_Mahistory, to match 1988
                                                                          HETSELTSRC Meaning from apparts.
                                                                          Inhabiteutt | Married from stores
Nibralis 64-11 run-grafeevantty/pum_rethonedir.su musch 1985
Sth/s88_64-Linux/gen/accortfy/pum_sorm.so match 2009
                                                                          atmosti aligenti alsažini 1937 luvimen kilkiniskokatarili n. kilak (2 hvist 79.1 a lainta Klarick
Through 64-Espain-genry Security details no models 1886
                                                                          #Feddize.wize: 1348
                                                                          hartaft jewe emblisht - $ []
Tib/x86_64-Tinus-gmu/plymouth/script_as match 1889
Sib/s80 84-Linux gravel amounts/renderers/drs. so eerch 2008
th/affi_64-Linux-gnu/plymouth/renderers/frame-buffer; sa match 1mm
$16/x86_64-Limux-grau/plymouth/revalences/vgs26fb.sn makin 108%
Tibristicapportor profile-tood moter 100%
Sthring Agestiert - job wetch 5000
```

Video: <a href="https://www.youtube.com/watch?v=srQAZGfY8Ec">https://www.youtube.com/watch?v=srQAZGfY8Ec</a>

## Next sprint

- Implement use case 2 (docker containers)
- Provide more API and web UI
- Modify "docker run" to check image status
- Alternatives to avoid shortcomings of sdhash
- Containerize our application deployment



If this Trello Board represents a Sprint or a Product Backlog, adding a start and end date will allow the x-axis to be more accurate and a desired-velocity line to be drawn.

Date Range: 2016-02-29 to 2016-03-15 Update

# Thank you & Q/A