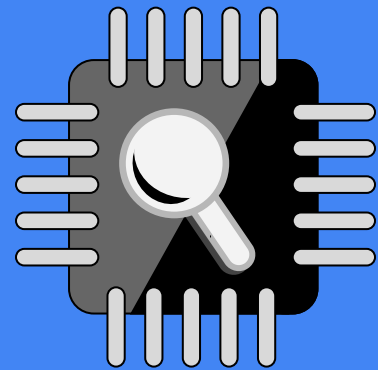


Rekall Agent - OSDFCon 2017

We will remember it for you wholesale!

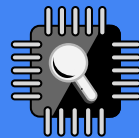
Michael Cohen

mic@rekall-innovations.com



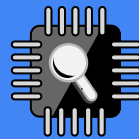
Rekall
Forensics

- Rekall is an open source project released under the GPL. It is not an official Google product, and does not necessarily reflect the views of Google.



Overview

- Why the Rekall Agent?
- Deployment: Rekall in the cloud!
- Authentication
- Flows
- Hunts
- Exporting data
- Post processing



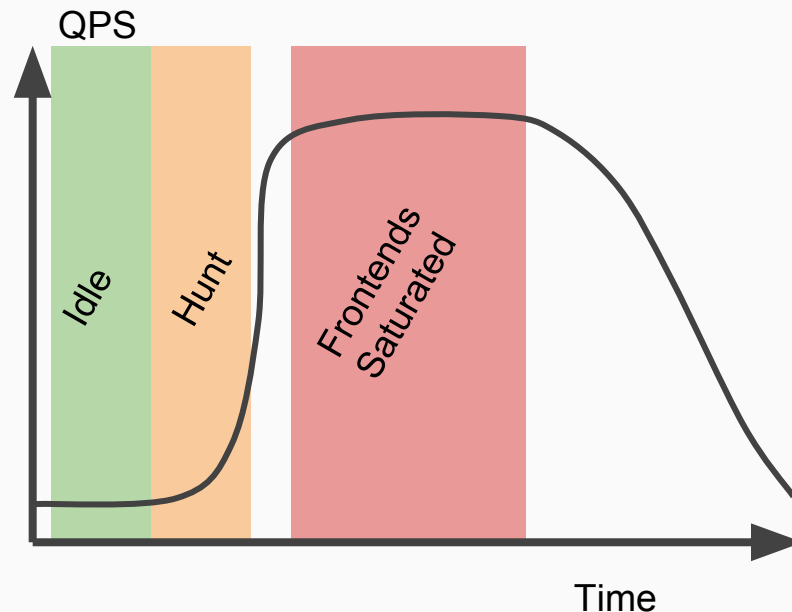
Why endpoint monitoring?

- An enterprise typically has a lot of endpoints (laptops, servers, cloud VMs).
 - Mix of operating systems, configurations and deployments.
 - Systems are not always accessible.
 - Dynamic changing environment.



Existing solutions

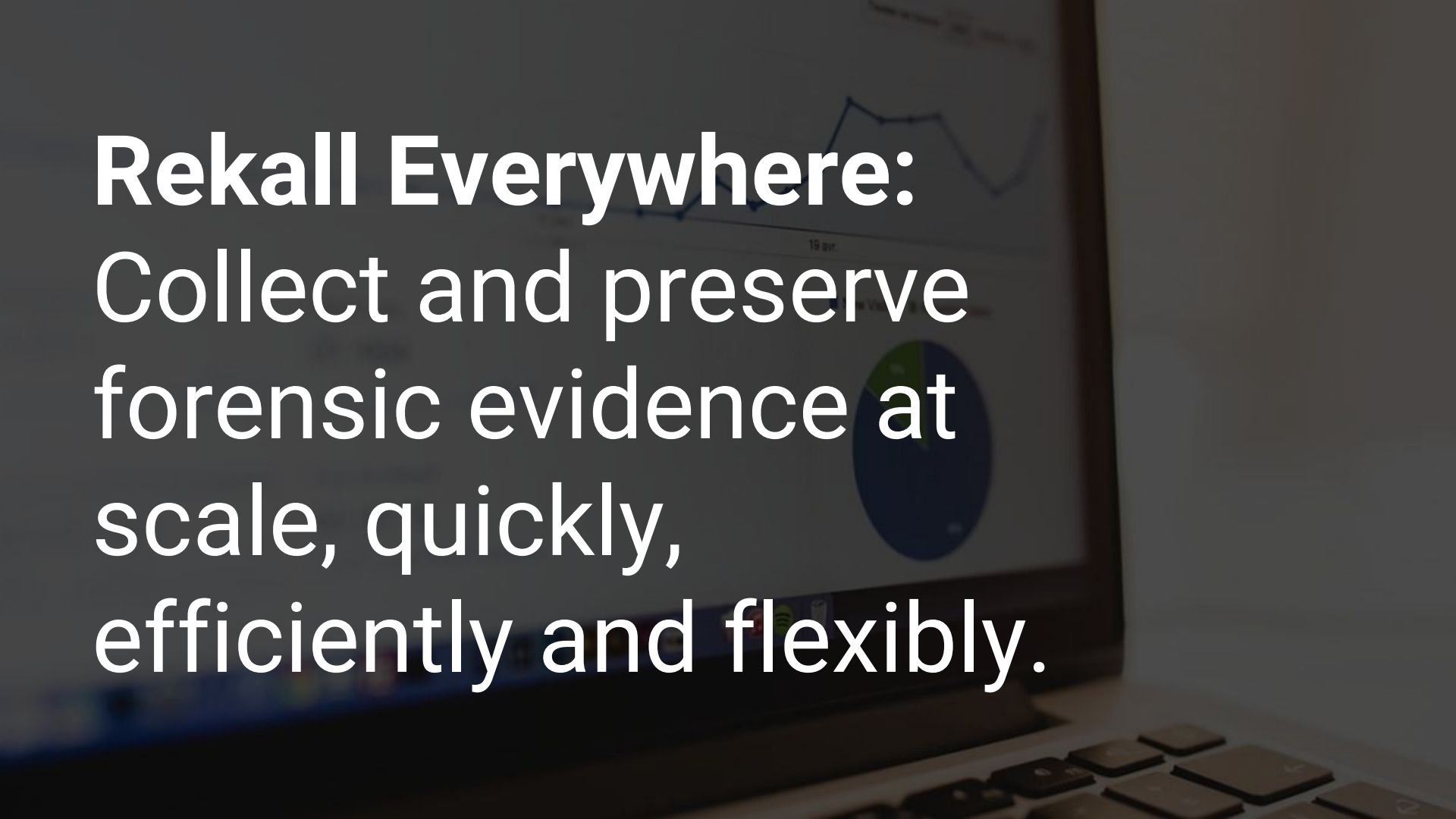
- Resource management.
 - System is idle much of the time.
 - But when something happens (e.g. a hunt) QPS load increases.
- Existing systems need to be provisioned in advance to handle maximal load.





Existing solutions

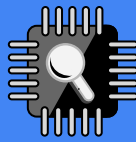
- Flexibility is important
 - Some existing solutions require code changes to be deployed server side or client side.
 - E.g. GRR requires python hacks to run arbitrary code.
 - In a dynamic, rapidly evolving incident we need to be able to get and filter data in creative ways.
 - Sometimes the framework does not provide flexible filtering requiring a lot of extra data to be transferred and the post-processed.



Rekall Everywhere:
Collect and preserve
forensic evidence at
scale, quickly,
efficiently and flexibly.



Use the Cloud!



Cloud technologies
provides automated
scaling.

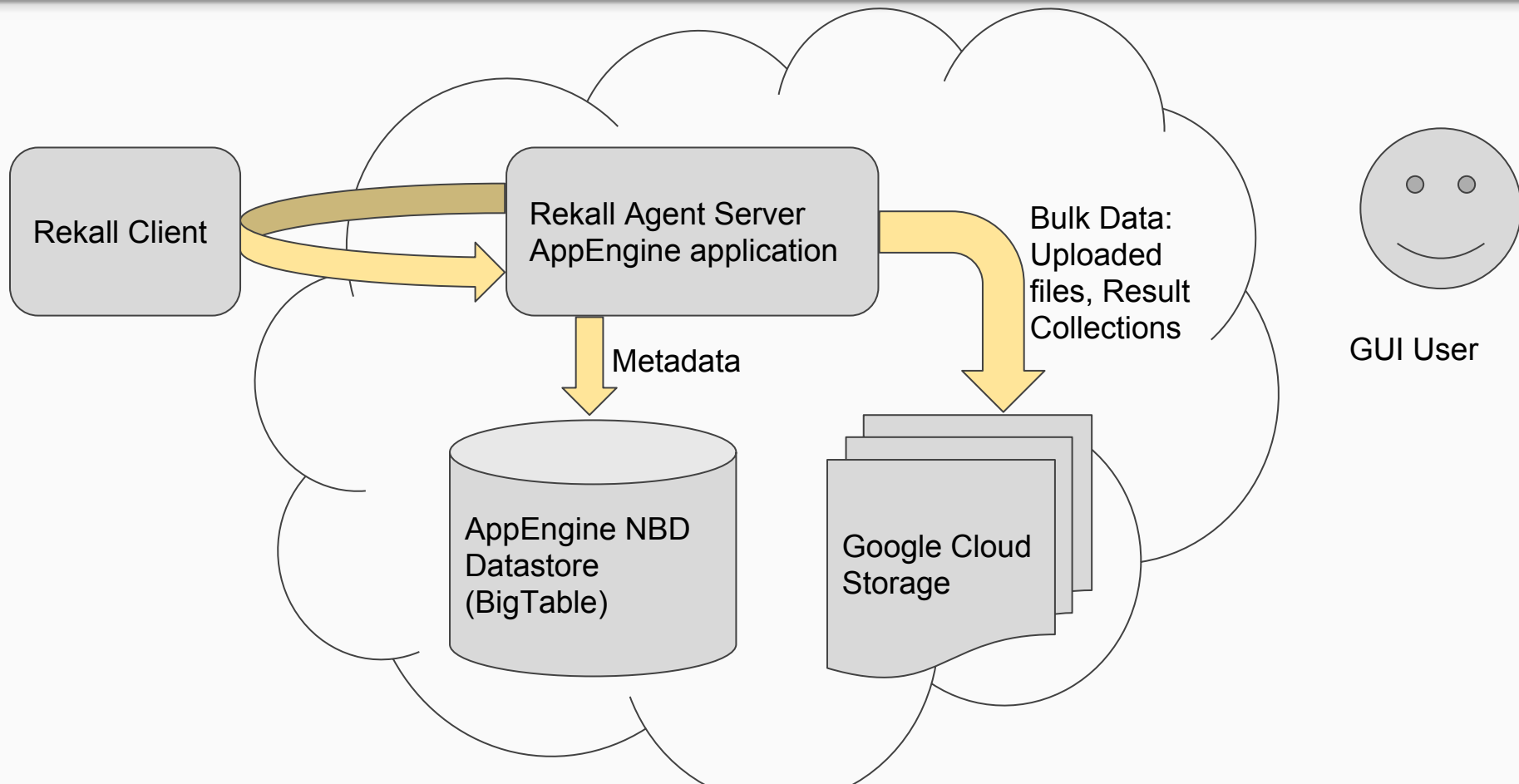
When things get busy, the
cloud takes care of scaling
up. When things are idle
the cloud scales down to
save on cost.

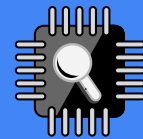


Why Rekall Agent?

- **Endpoint monitoring solution**
 - Rekall is already a sophisticated forensic analysis framework
 - Rekall Agent runs remote analysis at scale.
 - Collection system for results and files.
- **Strong Access controls and auditing.**
 - Role based access control mechanism
 - Peer approval process for gaining access to individual machine's data.
 - Strong auditing managed by the Google Cloud Platform.
- **Easily scalable**
 - The Google Cloud Platform (GCP) manages scaling on demand.

System overview





Deploying Rekall Agent

Create GCP project, push AppEngine app.

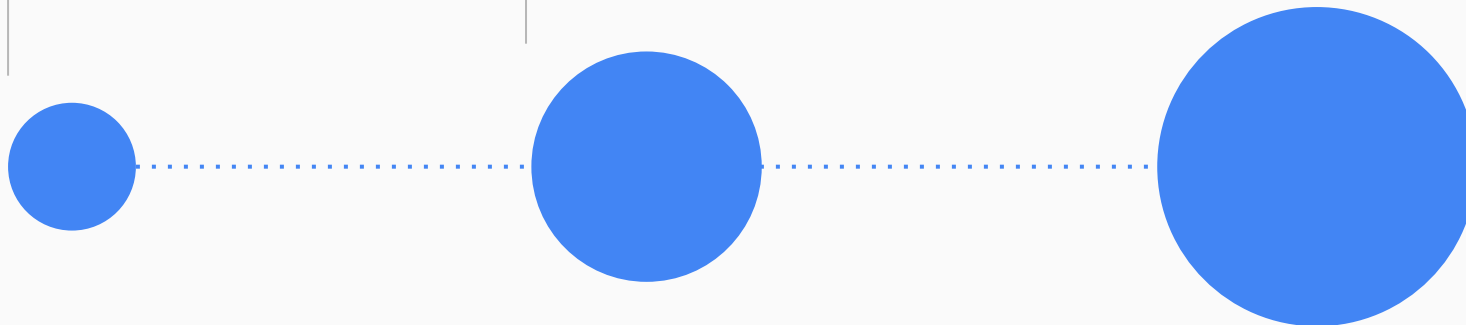
Step 1

Step 2

Configure App Engine app to allow users access.

Step 3

Create a client config for each OS and deploy client via software management tools.





Deployment - Server.

- Create a new project in the GCP console.
 - Give the project a unique name - the project will be served from <https://project-name.appspot.com>
 - Rekall Agent relies on SSL for communication security - GCP provides an SSL connection automatically.
- Get a working shell or spin up a virtual machine.
- Checkout the repository using git.
- Run the bootstrap script.
- Deploy the app
- Profit

Create a new project.


← → ↻ Secure | <https://console.cloud.google.com/projectcreate?previousPage=%2Fstorage%2Fbrowser%3Fproject%3Dfour> ☆




Google Cloud Platform




New Project

 You have 10 projects remaining in your quota. [Learn more.](#)

Project name 

dfrws2017-rekall

Your project ID will be dfrws2017-rekall  [Edit](#)

Create

Cancel

Browser

Transfer

Settings

Select

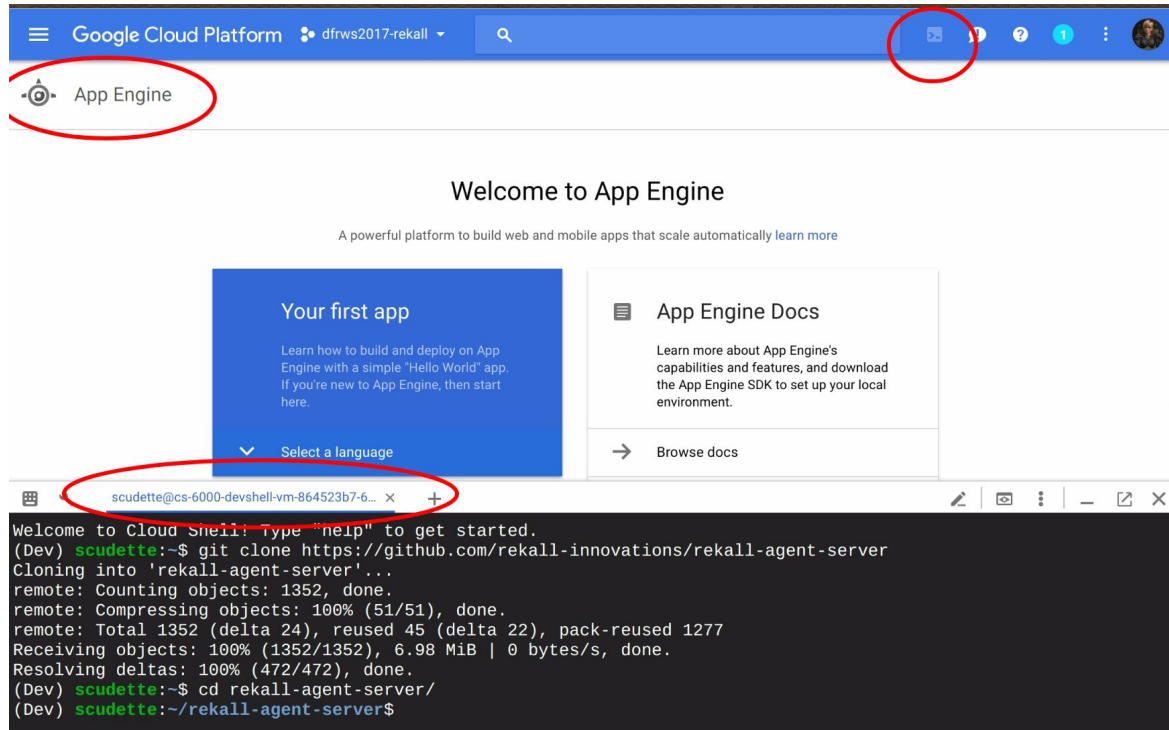
Search projects and folders

Recent All

Name	ID
 dfrws2017-rekall	dfrws2017-rekall
 Scudette	fourth-carport-147912
 Rekall Test Site	rekall-test-site
 dirrr	dirrr-158405
 Rekall	crypto-prism-89412

CANCEL OPEN

Cloning the Rekall repository for server deployment



The screenshot displays the Google Cloud Platform (GCP) console interface. At the top, the navigation bar shows "Google Cloud Platform" and a dropdown menu with "dfrws2017-rekall". A red circle highlights the user profile icon in the top right corner. Below the navigation bar, the "App Engine" service is selected, indicated by a red circle around its icon and label. The main content area displays a "Welcome to App Engine" message, followed by a description: "A powerful platform to build web and mobile apps that scale automatically". Below this, there are two main sections: "Your first app" and "App Engine Docs". The "Your first app" section includes a link to "Select a language" and a "Browse docs" button. The "App Engine Docs" section includes a link to "Learn more about App Engine's capabilities and features, and download the App Engine SDK to set up your local environment." At the bottom of the console, a terminal window is open, showing the command prompt "scudette@cs-6000-devshell-vm-864523b7-6...". The terminal output shows the command "git clone https://github.com/rekall-innovations/rekall-agent-server" being executed, followed by the cloning progress and the final directory structure.

Google Cloud Platform dfrws2017-rekall

App Engine

Welcome to App Engine

A powerful platform to build web and mobile apps that scale automatically [learn more](#)

Your first app

Learn how to build and deploy on App Engine with a simple "Hello World" app. If you're new to App Engine, then start here.

Select a language

App Engine Docs

Learn more about App Engine's capabilities and features, and download the App Engine SDK to set up your local environment.

Browse docs

scudette@cs-6000-devshell-vm-864523b7-6... x

```
Welcome to Cloud Shell: Type "help" to get started.
(Dev) scudette:~$ git clone https://github.com/rekall-innovations/rekall-agent-server
Cloning into 'rekall-agent-server'...
remote: Counting objects: 1352, done.
remote: Compressing objects: 100% (51/51), done.
remote: Total 1352 (delta 24), reused 45 (delta 22), pack-reused 1277
Receiving objects: 100% (1352/1352), 6.98 MiB | 0 bytes/s, done.
Resolving deltas: 100% (472/472), done.
(Dev) scudette:~$ cd rekall-agent-server/
(Dev) scudette:~/rekall-agent-server$
```



```
Welcome to Cloud Shell! Type "help" to get started.
(Dev) scudette:~$ git clone https://github.com/rekall-innovations/rekall-agent-server
Cloning into 'rekall-agent-server'...
remote: Counting objects: 1352, done.
remote: Compressing objects: 100% (51/51), done.
remote: Total 1352 (delta 24), reused 45 (delta 22), pack-reused 1277
Receiving objects: 100% (1352/1352), 6.98 MiB | 0 bytes/s, done.
Resolving deltas: 100% (472/472), done.
(Dev) scudette:~$ cd rekall-agent-server/
(Dev) scudette:~/rekall-agent-server$ ./bootstrap.sh
Collecting artifacts
  Downloading artifacts-20170806.tar.gz (58kB)
    100% |████████████████████████████████████████| 61kB 1.6MB/s
Collecting functools32
  Downloading functools32-3.2.3-2.zip
Collecting oauth2client==4.1.0
  Downloading oauth2client-4.1.0-py2.py3-none-any.whl (185kB)
    100% |████████████████████████████████████████| 194kB 3.1MB/s
Collecting humanize
  Downloading humanize-0.5.1.tar.gz
Collecting PyYAML>=3.11 (from artifacts)
  Downloading PyYAML-3.12.tar.gz (253kB)
    100% |████████████████████████████████████████| 256kB 2.7MB/s
Collecting httplib2>=0.9.1 (from oauth2client==4.1.0)
Collecting rsa>=3.1.4 (from oauth2client==4.1.0)
  Using cached rsa-3.4.2-py2.py3-none-any.whl
```

```
(Dev) scudette:~/rekall-agent-server$ gcloud app deploy app.yaml index.yaml
You are creating an app for project [dfrws2017-rekall].
WARNING: Creating an App Engine application for a project is irreversible and the region
cannot be changed. More information about regions is at
https://cloud.google.com/appengine/docs/locations.
```

Please choose the region where you want your App Engine application
located:

- [1] europe-west2 (supports standard and flexible)
- [2] us-east1 (supports standard and flexible)
- [3] us-east4 (supports standard and flexible)
- [4] asia-northeast1 (supports standard and flexible)
- [5] australia-southeast1 (supports standard and flexible)
- [6] us-central (supports standard and flexible)
- [7] europe-west3 (supports standard and flexible)
- [8] europe-west (supports standard and flexible)
- [9] cancel

Please enter your numeric choice: 6

Creating App Engine application in project [dfrws2017-rekall] and region [us-central]....done.
Services to deploy:

```
descriptor:    [/home/scudette/rekall-agent-server/app.yaml]
source:        [/home/scudette/rekall-agent-server]
target project: [dfrws2017-rekall]
target service: [default]
target version: [20170806t230849]
target url:     [https://dfrws2017-rekall.appspot.com]
```

Configurations to update:

```
descriptor:    [/home/scudette/rekall-agent-server/index.yaml]
type:          [datastore indexes]
target project: [dfrws2017-rekall]
```


Configurations to update:

```
descriptor:    [/home/scudette/rekall-agent-server/index.yaml]
type:          [datastore indexes]
target project: [dfrws2017-rekall]
```

Do you want to continue (Y/n)?

Beginning deployment of service [default]...
Some files were skipped. Pass `--verbosity=info` to see which ones.
You may also view the gcloud log file, found at
[/tmp/tmp.C25Ew73Fnc/logs/2017.08.06/23.07.59.356239.log].

= Uploading 862 files to Google Cloud Storage

====File upload done.

Updating service [default]...done.

Waiting for operation [apps/dfrws2017-rekall/operations/585e5e6e-6171-4694

.

Updating service [default]...done.

Deployed service [default] to [https://dfrws2017-rekall.appspot.com]

Updating config [index]...done.

Indexes are being rebuilt. This may take a moment.

You can stream logs from the command line by running:

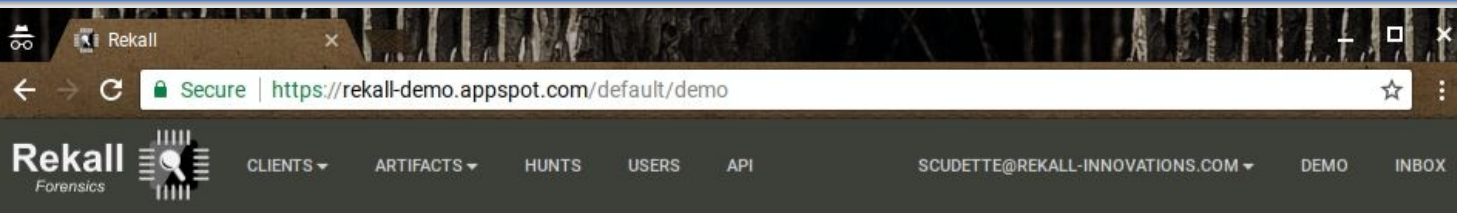
```
$ gcloud app logs tail -s default
```

To view your application in the web browser run:

```
$ gcloud app browse
```



Self Guided Demo



This is a demo application

The demo application is exactly the same as the fully installed application bar for the following restrictions:

- All data is visible to anyone who logs into this installation. Please do not input sensitive information into the app since it is visible to anyone. This includes your GMail user account which will also be visible to anyone.
- All data will be periodically wiped without warning. Please do not expect data to be retained.
- Anyone can fully interact with this demo installation. This means that anyone else can delete, modify or add any data, including remove data that you add. Please do not expect your data to be protected in any way.
- Please do not abuse the application. Abusers will be banned. Please remember that the application maintains detailed audit logging as well as request logs.
- If you find a problem or bug, please report it at support@rekall-forensic.com.

By using this application you acknowledge that you have read and understood these conditions. Press the below button and follow the login link.

MAKE ME ADMIN

There is a demo application you can use to play with The Rekall Agent Server.



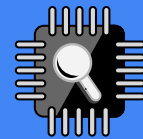
Access management

- Platform administrators:
 - Users with AppEngine admin level access.
 - No access control! Can do anything within the App, including update the application, push new code etc.
- Rekall Users
 - Rekall does not deal with user accounts/passwords - these are done by GCP.
 - Rekall users are given roles within the application.
 - Investigator - can issue new collection flows.
 - Examiner - Can view existing collections.
 - Hunter - Can propose hunts for the entire fleet.
 - Approver - Can approve collection flows and hunts.
 - Administrator - Can grant other users roles!



Deployment - Users

- Roles are assigned on resources (securable objects):
 - Clients
 - Hunts
 - The Application
- It is possible for a user to have different roles on different resources.
- Client/Hunt approval workflow essentially grants roles on Hunt/Client.
- When the user attempts to access a Client/Hunt for which they have no access:
 - Approval request is sent to Approver.
 - Once approval is granted, the user may access the Client.



Auditing

- Every Action a user makes is being audited.
- Users need the Auditor role to be able to see the audit log.



Deployment - Client

- Prepare a client configuration file.
 - Use the server provided one as a template
- On all clients install the Rekall package, and optionally the Rekall Agent package.
 - Most enterprises have their own software management solution.
 - Endpoint deployment and configuration is an exercise left to the reader.
- One can run the client manually to see the debugging messages.



Client capabilities

- Rekall Agent just runs regular Rekall plugins and collects their results on the server.
 - This means you can test potential plugin invocations in the regular Rekall Console.
 - The Rekall Agent server just manages collection storage and access controls. It does not further analysis by itself.
- Most useful Rekall plugins:
 - EFilter queries - allows for arbitrary combinations of plugins, filtering the output and retrieving only selected information.
 - OSQuery plugin - run the normal OSQuery binary and collect the results.
 - Can run memory analysis but this should not be first option - use API mode first.
- Rekall Agent implement resource limits (total CPU and CPU load).



Example EFilter queries.

Mactimes timeline output

```
select Hashes.md5,  
       Path,  
       Path.st_ino,  
       Path.st_mode,  
       Path.st_uid.uid,  
       Path.st_gid.gid,  
       Path.st_size,  
       timestamp(Path.st_atime) as a,  
       timestamp(Path.st_mtime) as m,  
       timestamp(Path.st_ctime) as c from hash(paths: (  
         select path from glob("/bin/*")  
       ).path.filename, hash: "md5")
```

PluginAction(Search)

LOGS

DATA

COPY

CSV

EXCEL

PDF

PRINT

Search:

md5	Path	st_ino	st_mode	uid	gid	st_size	a	m	c
004fd9b650f2d2dfcd3378ea6c99bb5c	/bin/vdir	5031	-rwxr-xr-x	0	0	118280	2015-03-14 15:47:04Z	2015-03-14 15:47:04Z	2017-10-02 20:19:30Z
0097b50c0ef76c8d68f67ad1abc4f2c0	/bin/dir	5005	-rwxr-xr-x	0	0	118280	2015-03-14 15:47:04Z	2015-03-14 15:47:04Z	2017-10-02 20:19:30Z
00f8323d4c1636f8b1202c018104672e	/bin/findmnt	5042	-rwxr-xr-x	0	0	45216	2015-03-29 22:34:08Z	2015-03-29 22:34:08Z	2017-10-02 20:19:30Z
03343bf5ba2365dcd37f58109121b827	/bin/netstat	5022	-rwxr-xr-x	0	0	120200	2014-11-08 18:09:08Z	2014-11-08 18:09:08Z	2017-10-02 20:19:30Z
0643adf77b207ac4284ebf6dcbbc42b3	/bin/grep	210	-rwxr-xr-x	0	0	202936	2015-02-14 01:27:29Z	2015-02-14 01:27:29Z	2017-10-02 20:19:30Z
08bc332b1d68296206d86d5bff1cb0e6	/bin/pidof	4973	lrwxrwxrwx	0	0	14	2015-04-06 18:44:32Z	2015-04-06 18:44:32Z	2017-10-02 20:19:30Z
0a5dfaab7900c415d246b58df5167932	/bin/lsblk	4962	-rwxr-xr-x	0	0	64552	2015-03-29 22:34:07Z	2015-03-29 22:34:07Z	2017-10-02 20:19:30Z
0b54c89ff07afe0b6a802b691d3553c	/bin/run-parts	262	-rwxr-xr-x	0	0	19312	2014-11-08 13:49:45Z	2014-11-08 13:49:45Z	2017-10-02 20:19:30Z
10a5a0be2ad3f47fff12daaf1c0256c5	/bin/bzexe	4966	-rwxr-xr-x	0	0	4877	2015-03-27 19:24:22Z	2015-03-27 19:24:22Z	2017-10-02 20:19:30Z
12ba858a706fce80095791f095ec382a	/bin/ps	5027	-rwxr-xr-x	0	0	93056	2015-03-06 21:13:12Z	2015-03-06 21:13:12Z	2017-10-02 20:19:30Z

Show entries

Showing 1 to 10 of 120 entries

PREVIOUS

1

2

3

4

5

12

NEXT

Find authorized_keys.

A user left the company and we want to see if their SSH keys are still installed somewhere:

```
select * from file_yara(paths: (  
    select path.filename.name  
        from glob("/home/*/ssh/authorized_keys")  
    ).name,  
    yara_expression: "rule r1 {strings: $a =  
\"T6qsh0WEh8pRvEKL/aZOBTKjr7d\" condition: any of them}")
```

Long running process from WebShell

A compromised webserver was found to contain a webshell. Which resource hungry processes were launched by the webshell?

```
select proc, proc.cpu_times.user from pslist() where  
proc.environ.HTTP_COOKIE =~ "WebShell-cwd"
```



Find out more!

The Rekall Agent White paper

<http://www.rekall-forensic.com/documentation-1/rekall-documentation/user-manual>

Rekall's home on Github <https://github.com/rekall-innovations>

Rekall's site <http://www.rekall-forensic.com/>

Mailing list rekall-discuss@googlegroups.com