UAM Reto Silicon Valley: Episodio 1 - Hispasec

Descripción

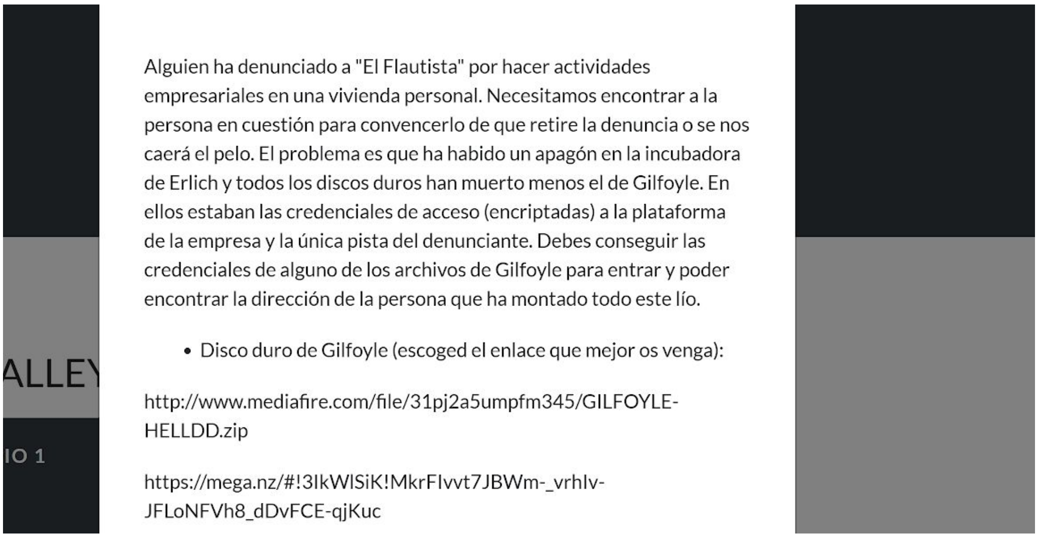
Nombre: UAM- Silicon Valley - Episodio 1 - (Related https://www.filmaffinity.com/es/film279751.html)
Fecha de liberación: 15 de septiembre de 2018
Autor: 1v4n https://unaalmes.hispasec.com/team/40
Puntuación: 200

Alguien ha denunciado a "El Flautista" por hacer actividades empresariales en una vivienda personal. Necesitamos encontrar a la persona en cuestión para convencerlo de que retire la denuncia o se nos caerá el pelo. El problema es que ha habido un apagón en la incubadora de Erlich y todos los discos duros han muerto menos el de Gilfoyle. En ellos estaban las credenciales de acceso (encriptadas) a la plataforma de la empresa y la única pista del denunciante. Debes conseguir las credenciales de alguno de los archivos de Gilfoyle para entrar y poder encontrar la dirección de la persona que ha montado todo este lío.

Disco duro de Gilfoyle (escoged el enlace que mejor os venga):
http://www.mediafire.com/file/31pj2a5umpfm345/GILFOYLE-HELLDD.zip

https://mega.nz/#!3IkWlSiK!MkrFIvvt7JBWm-_vrhIv-JFLoNFVh8_dDvFCE-qjKuc

Login: http://34.247.69.86/siliconvalley/episodio1/login.php

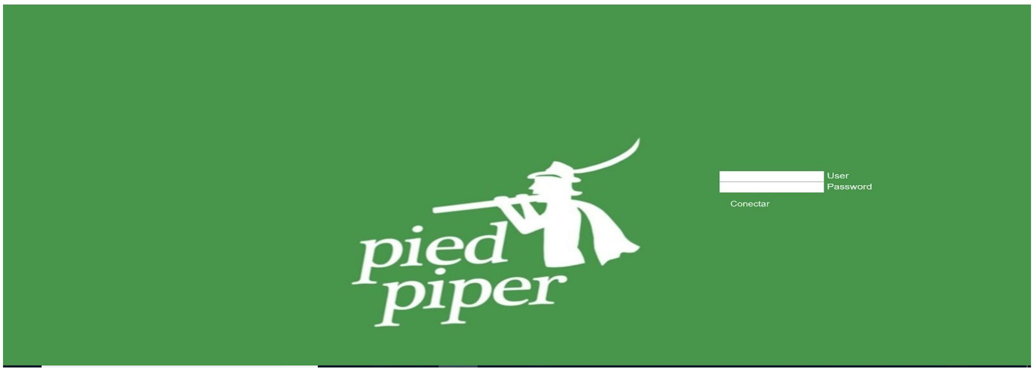


Alguien ha denunciado a "El Flautista" por hacer actividades empresariales en una vivienda personal. Necesitamos encontrar a la persona en cuestión para convencerlo de que retire la denuncia o se nos caerá el pelo. El problema es que ha habido un apagón en la incubadora de Erlich y todos los discos duros han muerto menos el de Gilfoyle. En ellos estaban las credenciales de acceso (encriptadas) a la plataforma de la empresa y la única pista del denunciante. Debes conseguir las credenciales de alguno de los archivos de Gilfoyle para entrar y poder encontrar la dirección de la persona que ha montado todo este lío.

- Disco duro de Gilfoyle (escoged el enlace que mejor os venga):

http://www.mediafire.com/file/31pj2a5umpfm345/GILFOYLE-HELLDD.zip

https://mega.nz/#!3IkWlSiK!MkrFIvvt7JBWm-_vrhIv-JFLoNFVh8_dDvFCE-qjKuc



Objetivo

Formato de la flag: UAM{md5}

Herramientas utilizadas

Versión 69.0.3497.100 (Build oficial) (64 bits) https://www.google.com/chrome/
megatools 1.10.2 - command line tools for Mega.nz https://github.com/megous/megatools
file-5.34
UnZip 6.00 ftp://ftp.info-zip.org/pub/infozip/
TestDisk 7.0, Data Recovery Utility, April 2015
curl 7.61.0
Volatility Foundation Volatility Framework 2.6
https://gchq.github.io/CyberChef
https://crackstation.net/
http://exif.regex.info/exif.cgi
https://www.google.es/maps

Resumen:

Comenzamos por visitar el reto y descargamos el archivo adjunto *con el Disco duro de Gilfoyle* utilizando la tool *megadl 'https://mega.nz/#!3IkWlSiK!MkrFIvvt7JBWm-_vrhIv-JFLoNFVh8_dDvFCE-qjKuc'*

```
root@kali:~/Desktop/uam/SiliconValley# megadl
'https://mega.nz/#!3IkWlSiK!MkrFIvvt7JBWm-_vrhIv-JFLoNFVh8_dDvFCE-qjKuc'
Downloaded GILFOYLE-HELLDD.zip
```

Procesado de archivo en formato desconocido

Pasamos a descomprimirlo con unzip y le realizamos un análisis

```
root@kali:~/Desktop/uam/SiliconValley# unzip GILFOYLE-HELLDD.zip
Archive:  GILFOYLE-HELLDD.zip
  inflating: GILFOYLE-HELLDD.raw
root@kali:~/Desktop/uam/SiliconValley# file GILFOYLE-HELLDD.raw
GILFOYLE-HELLDD.raw: data
root@kali:~/Desktop/uam/SiliconValley# root@kali:~/Desktop/uam/SiliconValley#
megadl 'https://mega.nz/#!3IkWlSiK!MkrFIvvt7JBWm-_vrhIv-JFLoNFVh8_dDvFCE-qjKuc'
bash: root@kali:~/Desktop/uam/SiliconValley#: No existe el fichero o el
directorio
root@kali:~/Desktop/uam/SiliconValley# Downloaded GILFOYLE-HELLDD.zip
bash: Downloaded: no se encontró la orden
root@kali:~/Desktop/uam/SiliconValley# root@kali:~/Desktop/uam/SiliconValley#
megadl 'https://mega.nz/#!3IkWlSiK!MkrFIvvt7JBWm-_vrhIv-JFLoNFVh8_dDvFCE-qjKuc'
bash: root@kali:~/Desktop/uam/SiliconValley#: No existe el fichero o el
directorio
root@kali:~/Desktop/uam/SiliconValley# Downloaded GILFOYLE-HELLDD.zip
bash: Downloaded: no se encontró la orden
root@kali:~/Desktop/uam/SiliconValley# testdisk /list GILFOYLE-HELLDD.raw
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
```

```
http://www.cgsecurity.org
Please wait...
Disk GILFOYLE-HELLDD.raw - 2147 MB / 2047 MiB - CHS 262 255 63
Sector size:512


Disk GILFOYLE-HELLDD.raw - 2147 MB / 2047 MiB - CHS 262 255 63
     Partition                  Start        End    Size in sectors

root@kali:~/Desktop/uam/SiliconValley#
```

Investigamos un poco y tenemos una referencia en la primera misión de los retos de UAM y en particular en una parte el writeup de https://donttouchmy.net/write-up-una-al-mes-mission001/ . Por lo tanto pasamos a utilizar Volatility:

```
root@kali:~/Desktop/uam/SiliconValley# volatility imageinfo -f GILFOYLE-HELLDD.raw
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
                Suggested  Profile(s)  :  Win7SP1x64,  Win7SP0x64,  Win2008R2SP0x64,
Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                                                  AS   Layer2   :   FileAddressSpace
(/root/Desktop/uam/SiliconValley/GILFOYLE-HELLDD.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800029f00a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800029f1d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2018-09-15 09:56:27 UTC+0000
     Image local date and time : 2018-09-15 11:56:27 +0200
root@kali:~/Desktop/uam/SiliconValley# volatility pslist --profile=Win2008R2SP1x64
-f GILFOYLE-HELLDD.raw
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess
Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------
------ ------------------------------ ------------------------------
0xfffffa80018ac040 System                  4      0     80      557 ------
0 2018-09-15 09:47:47 UTC+0000
0xfffffa8002101040 smss.exe              248      4      2       29 ------
0 2018-09-15 09:47:47 UTC+0000
0xfffffa80028c6b30 csrss.exe             324    316      9      411      0
0 2018-09-15 09:47:51 UTC+0000
0xfffffa80028df9e0 csrss.exe             372    364      9      342      1
0 2018-09-15 09:47:51 UTC+0000
0xfffffa80028ed060 wininit.exe           380    316      3       75      0
```

```
0 2018-09-15 09:47:51 UTC+0000
0xfffffa80028ee5e0 winlogon.exe               408     364      5       116       1
0 2018-09-15 09:47:52 UTC+0000
0xfffffa80028f1b30 services.exe               468     380      8       193       0
0 2018-09-15 09:47:52 UTC+0000
0xfffffa8002930430 lsass.exe                  476     380      8       718       0
0 2018-09-15 09:47:53 UTC+0000
0xfffffa800194bb30 lsm.exe                    484     380     10       144       0
0 2018-09-15 09:47:53 UTC+0000
0xfffffa800298e910 svchost.exe                572     468     10       349       0
0 2018-09-15 09:47:54 UTC+0000
0xfffffa80029a6060 VBoxService.ex             632     468     12       116       0
0 2018-09-15 09:47:55 UTC+0000
0xfffffa80029c2420 svchost.exe                696     468      7       285       0
0 2018-09-15 09:47:55 UTC+0000
0xfffffa8002a00b30 svchost.exe                784     468     22       573       0
0 2018-09-15 09:47:56 UTC+0000
0xfffffa8002a1bb30 svchost.exe                828     468     25       491       0
0 2018-09-15 09:47:56 UTC+0000
0xfffffa8002a22b30 svchost.exe                852     468     18       467       0
0 2018-09-15 09:47:56 UTC+0000
0xfffffa8002a286c0 svchost.exe                876     468     31       873       0
0 2018-09-15 09:47:56 UTC+0000
0xfffffa8002a6e060 svchost.exe               1012     468      5       110       0
0 2018-09-15 09:47:57 UTC+0000
0xfffffa8002abeb30 svchost.exe                532     468     14       379       0
0 2018-09-15 09:47:58 UTC+0000
0xfffffa8001f76720 spoolsv.exe               1120     468     13       269       0
0 2018-09-15 09:48:00 UTC+0000
0xfffffa8002b59b30 svchost.exe               1204     468     19       300       0
0 2018-09-15 09:48:01 UTC+0000
0xfffffa8002be15f0 svchost.exe               1324     468     19       273       0
0 2018-09-15 09:48:01 UTC+0000
0xfffffa8002d42b30 taskhost.exe              1804     468     10       255       1
0 2018-09-15 09:48:05 UTC+0000
0xfffffa8002d71300 dwm.exe                   1864     828      3        71       1
0 2018-09-15 09:48:05 UTC+0000
0xfffffa80019289e0 explorer.exe              1900    1852     34       922       1
0 2018-09-15 09:48:06 UTC+0000
0xfffffa8002e3b290 VBoxTray.exe              1376    1900     14       159       1
0 2018-09-15 09:48:08 UTC+0000
0xfffffa8002d24b30 soffice.exe               1756    1900      1        66       1
1 2018-09-15 09:48:13 UTC+0000
0xfffffa8002e8a9e0 SearchIndexer.            1160     468     11       611       0
0 2018-09-15 09:48:14 UTC+0000
0xfffffa8002ec4b30 wmpnetwk.exe              2008     468     13       415       0
0 2018-09-15 09:48:16 UTC+0000
0xfffffa8002f7fb30 svchost.exe               2236     468      8       346       0
0 2018-09-15 09:48:17 UTC+0000
0xfffffa8002fc7b30 soffice.bin               2340    1756     11       464       1
1 2018-09-15 09:48:18 UTC+0000
```

```
0xfffffa8003029b30 WmiPrvSE.exe           2516     572        7          113         0
0 2018-09-15 09:48:23 UTC+0000
0xfffffa8002f619e0 svchost.exe            2404     468       13          326         0
0 2018-09-15 09:50:03 UTC+0000
0xfffffa8002fc9b30 audiodg.exe            1856     784        5          127         0
0 2018-09-15 09:53:34 UTC+0000
0xfffffa8001d61b30 firefox.exe             956    3052        0 --------           1
0 2018-09-15 09:55:59 UTC+0000   2018-09-15 09:56:08 UTC+0000
0xfffffa8001d598b0 explorer.exe           2692     572       16          507         1
0 2018-09-15 09:55:59 UTC+0000
0xfffffa8001d67b30 WmiPrvSE.exe           2328     572        6          120         0
0 2018-09-15 09:56:02 UTC+0000
0xfffffa8001d2b060 DumpIt.exe             3596    2692        5           46         1
1 2018-09-15 09:56:18 UTC+0000
0xfffffa8001e1b060 conhost.exe            3608     372        2           51         1
0 2018-09-15 09:56:18 UTC+0000
0xfffffa80019de960 SearchProtocol         3824    1160        7          769 ------
0 2018-09-15 09:57:22 UTC+0000
0xfffffa8001d37060 SearchFilterHo         3852    1160        5           24 ------
0 2018-09-15 09:57:22 UTC+0000
```

Observamos que se estaba ejecutando un proceso que era soffice.exe y soffice.bin, que es el LibreOffice. Sospechamos de este proceso y pasamos a filescan con un grep:

```
root@kali:~/Desktop/uam/SiliconValley# volatility filescan
--profile=Win2008R2SP1x64 -f GILFOYLE-HELLDD.raw | grep odt
Volatility Foundation Volatility Framework 2.6
0x000000007fca5580      2      0 RW-rw-
\Device\HarddiskVolume2\Users\unaalmes\Desktop\.~lock.info.odt#
0x000000007fcabd50      1      1 RW-r--
\Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
```

Descubrimos un archivo llamado info.odt que nos arroja:

```
root@kali:~/Desktop/uam/SiliconValley# volatility --profile=Win2008R2SP1x64
dumpfiles -n -i -r \\.odt -f GILFOYLE-HELLDD.raw -D /root/Desktop/uam/
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0xfffffa8001aabd50   2340
\Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
root@kali:~/Desktop/uam/SiliconValley# apt-get install odt2txt
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  odt2txt
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 13,7 kB de archivos.
Se utilizarán 54,3 kB de espacio de disco adicional después de esta operación.
Des:1 http://kali.download/kali kali-rolling/main amd64 odt2txt amd64 0.5-1+b2
```

```
[13,7 kB]
Descargados 13,7 kB en 0s (30,2 kB/s)
Seleccionando el paquete odt2txt previamente no seleccionado.
(Leyendo la base de datos ... 437078 ficheros o directorios instalados
actualmente.)
Preparando para desempaquetar .../odt2txt_0.5-1+b2_amd64.deb ...
Desempaquetando odt2txt (0.5-1+b2) ...
Procesando disparadores para mime-support (3.61) ...
Configurando odt2txt (0.5-1+b2) ...
Procesando disparadores para man-db (2.8.4-2) ...
root@kali:~/Desktop/uam/SiliconValley# odt2txt
file.2340.0xfffffa8001acdf10.info.odt.dat --raw > info.odt
root@kali:~/Desktop/uam/SiliconValley# cat info.odt | python -c 'import
sys;import xml.dom.minidom;s=sys.stdin.read();print
xml.dom.minidom.parseString(s).toprettyxml()'
<?xml version="1.0" ?>
<office:document-content office:version="1.2"
xmlns:chart="urn:oasis:names:tc:opendocument:xmlns:chart:1.0"
xmlns:dc="http://purl.org/dc/elements/1.1/"
xmlns:dom="http://www.w3.org/2001/xml-events"
xmlns:dr3d="urn:oasis:names:tc:opendocument:xmlns:dr3d:1.0"
xmlns:draw="urn:oasis:names:tc:opendocument:xmlns:drawing:1.0"
xmlns:field="urn:openoffice:names:experimental:ooo-ms-interop:xmlns:field:1.0"
xmlns:fo="urn:oasis:names:tc:opendocument:xmlns:xsl-fo-compatible:1.0"
xmlns:form="urn:oasis:names:tc:opendocument:xmlns:form:1.0"
xmlns:grddl="http://www.w3.org/2003/g/data-view#"
xmlns:math="http://www.w3.org/1998/Math/MathML"
xmlns:meta="urn:oasis:names:tc:opendocument:xmlns:meta:1.0"
xmlns:number="urn:oasis:names:tc:opendocument:xmlns:datastyle:1.0"
xmlns:of="urn:oasis:names:tc:opendocument:xmlns:of:1.2"
xmlns:office="urn:oasis:names:tc:opendocument:xmlns:office:1.0"
xmlns:ooo="http://openoffice.org/2004/office"
xmlns:oooc="http://openoffice.org/2004/calc"
xmlns:ooow="http://openoffice.org/2004/writer"
xmlns:rpt="http://openoffice.org/2005/report"
xmlns:script="urn:oasis:names:tc:opendocument:xmlns:script:1.0"
xmlns:style="urn:oasis:names:tc:opendocument:xmlns:style:1.0"
xmlns:svg="urn:oasis:names:tc:opendocument:xmlns:svg-compatible:1.0"
xmlns:table="urn:oasis:names:tc:opendocument:xmlns:table:1.0"
xmlns:tableooo="http://openoffice.org/2009/table"
xmlns:text="urn:oasis:names:tc:opendocument:xmlns:text:1.0"
xmlns:textooo="http://openoffice.org/2013/office"
xmlns:xforms="http://www.w3.org/2002/xforms"
xmlns:xhtml="http://www.w3.org/1999/xhtml"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
	<office:scripts/>
	<office:font-face-decls>
		<style:font-face style:name="Mangal1" svg:font-family="Mangal"/>
```

```
                <style:font-face style:font-family-generic="roman"
style:font-pitch="variable" style:name="Times New Roman" svg:font-family="'Times
New Roman'"/>
                <style:font-face style:font-family-generic="swiss"
style:font-pitch="variable" style:name="Arial" svg:font-family="Arial"/>
                <style:font-face style:font-family-generic="system"
style:font-pitch="variable" style:name="Mangal" svg:font-family="Mangal"/>
                <style:font-face style:font-family-generic="system"
style:font-pitch="variable" style:name="Microsoft YaHei"
svg:font-family="'Microsoft YaHei'"/>
                <style:font-face style:font-family-generic="system"
style:font-pitch="variable" style:name="SimSun" svg:font-family="SimSun"/>
        </office:font-face-decls>
        <office:automatic-styles/>
        <office:body>
                <office:text text:use-soft-page-breaks="true">
                        <text:sequence-decls>
                                <text:sequence-decl text:display-outline-level="0"
text:name="Illustration"/>
                                <text:sequence-decl text:display-outline-level="0"
text:name="Table"/>
                                <text:sequence-decl text:display-outline-level="0"
text:name="Text"/>
                                <text:sequence-decl text:display-outline-level="0"
text:name="Drawing"/>
                        </text:sequence-decls>
                        <text:p text:style-name="Standard">

VGhlIG91dHB1dCBzaG93cyBlbGV2ZW4gc2VydmljZXMgcHJpbnRlZCBpbiB0aHJlZSB1bmlxdWUgdGlt
ZWZyYW1lcy4gVGhlIG1vc3QgcmVjZW50CnRpbWVmcmFtZSAoMTMwNzA3NTIwNykgdHJhbnNsYXRlcyB0
byAyMDExLTA2LTAzIDA0OjI2OjQ3IFVUQy4gQXQgdGhpcyB0aW1lLCB0aGUgTVJ4Q2xzIGFuZApNUnhO
ZXQgc2VydmljZXMgd2VyZSBlaXRoZXIgY3JlYXRlZCBvciBtb2RpZmllZC4gSXQgc2hvdWxkIGJlIGlt
bWVkaWF0ZWx5IHN1c3BpY2lvdXMgdGhhdApuZWl0aGVyIG9mIHRoZXNlIHNlcnZpY2VzIGlzIHZpc2li
bGUgaW4gdGhlIG91dHB1dCBvZiBzdmNzY2FuLiBUaGlzIGlzIGEgc3Ryb25nIGluZGljYXRvciB0aGF0
CnRoZSB0d28gc2VydmljZXMgYXJlIGhpZGRlbiAob3IgdGhleSB3ZXJlIHN0YXJ0ZWQgaW5hcHByb3By
aWF0ZWx5KTsgb3RoZXJ3aXNlLCB0aGUgU0NNCndvdWxkIGtub3cgYWJvdXQgdGhlbToKJCBweXRob24g
dm9sLnB5IC1mIHN0dXhuZXQudm1lbSAtLXByb2ZpbGU9V2luWFBTUDN4ODYgc3Zjc2Nhbgp8IGVncmVw
IC1pICcobXJ4bmV0fG1yeGNscyknClZvbGF0aWxpdHkgRm91bmRhdGlvbiBWb2xhdGlsaXR5IEZyYW1l
d29yayAyLjQKJApPbmUgd2F5IHRvIHZlcmlmeSB3aGV0aGVyIHRoZSBzZXJ2aWNlcyBhcmUgYWN0dWFs
bHkgcnVubmluZywgZGVzcGl0ZSB0aGUgZmFjdCB0aGF0CnRoZXJlIGFyZSBubyBfU0VSVklDRV9SRUNP
UkQgc3RydWN0dXJlcywgaW52b2x2ZXMgZmlyc3QgZGV0ZXJtaW5pbmcgdGhlIGFzc29jaWF0ZWQga2Vy
bmVsCm1vZHVsZS4gVGhlIHBhdGggaXMgc3RvcmVkIGluIHRoZSBJbWFnZVBhdGggdmFsdWUgb2YgdGhl
IGNvcnJlc3BvbmRpbmcgcmVnaXN0cnkga2V5LiBBcwp5b3UgY2FuIHNlZSBpbiB0aGUgZm9sbG93aW5n
IG91dHB1dCwgdGhlIG1vZHVsZSBpcyBtcnhuZXQuc3lzOgokIHB5dGhvbiB2b2wucHkgLWYgc3R1eG5l
dC52bWVtIC0tcHJvZmlsZT1XaW5YUFNQM3g4NiBwcmludGtleQotSyAnQ29udHJvbFNldDAwMVxTZXJ2
aWNlc1xNUnhOZXQnClZvbGF0aWxpdHkgRm91bmRhdGlvbiBWb2xhdGlsaXR5IEZyYW1ld29yayAyLjQK
TGVnZW5kOiAoUykgPSBTdGFibGUgKFYpID0gVm9sYXRpbGUKLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0t
LS0tLQpSZWdpc3RyeTogXERldmljZVxIYXJkZGlza1ZvbHVtZTFcV0lORE9XU1xzeXN0ZW0zMlxjb25m
aWdcc3lzdGVtCktleSBuYW1lOiBNUnhOZXQgKFMpCkxhc3QgdXBkYXRlZDogMjAxMS0wNi0wMyAwNDoy
Njo0NyBVVEMrMDAwMApTdWJrZXlzOgooVikgRW51bQpWYWx1ZXM6ClJFR19TWiBEZXNjcmlwdGlvbiA6
```

```
IChTKSBNUlhORVQKUkVHX1NaIERpc3BsYXlOYW1lIDogKFMpIE1SWE5FVApSRUdfRFdPUkQgRXJyb3JD
b250cm9sIDogKFMpIDAKUkVHX1NaIEdyb3VwIDogKFMpIE5ldHdvcmsKUkVHX1NaIEltYWdlUGF0aCA6
IChTKSBcPz9cQzpcV0lORE9XU1xzeXN0ZW0zMlxEcml2ZXJzXG1yeG5ldC5zeXMKUkVHX0RXT1JEIFN0
YXJ0IDogKFMpIDEKUkVHX0RXT1JEIFR5cGUgOiAoUykgMQpZb3UgY2FuIGNyb3NzLXJlZmVyZW5jZSB0
aGF0IG1vZHVsZSBuYW1lIHdpdGggdGhlIGN1cnJlbnRseSBsb2FkZWQga2VybmVsIG1vZHVsZXM6CiQg
cHl0aG9uIHZvbC5weSAtZiBzdHV4bmV0LnZtZW0gLS1wcm9maWxlPVdpblhQU1AzeDg2IG1vZHVsZXMK
fCBncmVwIG1yeG5ldC5zeXMKVm9sYXRpbGl0eSBGb3VuZGF0aW9uIFZvbGF0aWxpdHkgRnJhbWV3b3Jr
IDIuNAoweDgxYzJhNTMwIG1yeG5ldC5zeXMgMHhiMjFkODAwMCAweDMwMDAKXD8/XEM6XFdJTkRPV1Nc
c3lzdGVtMzJcRHJpdmVyc1xtcnhuZXQuc3lzVGhlIG91dHB1dCBzaG93cyBlbGV2ZW4gc2VydmljZXMg
cHJpbnRlZCBpbiB0aHJlZSB1bmlxdWUgdGltZWZyYW1lcy4gVGhlIG1vc3QgcmVjZW50CnRpbWVmcmFt
ZSAoMTMwNzA3NTIwNykgdHJhbnNsYXRlcyB0byAyMDExLTA2LTAzIDA0OjI2OjQ3IFVUQy4gQXQgdGhp
cyB0aW1lLCB0aGUgTVJ4Q2xzIGFuZApNUnhOZXQgc2VydmljZXMgd2VyZSBlaXRoZXIgY3JlYXRlZCBv
ciBtb2RpZmllZC4gSXQgc2hvdWxkIGJlIGltbWVkaWF0ZWx5IHN1c3BpY2lvdXMgdGhhdApuZWl0aGVy
IG9mIHRoZXNlIHNlcnZpY2VzIGlzIHZpc2libGUgaW4gdGhlIG91dHB1dCBvZiBzdmNzY2FuLiBUaGlz
IGlzIGEgc3Ryb25nIGluZGljYXRvciB0aGF0CnRoZSB0d28gc2VydmljZXMgYXJlIGhpZGRlbiAob3Ig
dGhleSB3ZXJlIHN0YXJ0ZWQgaW5hcHByb3ByaWF0ZWx5KTsgb3RoZXJ3aXNlLCB0aGUgU0NNCndvdWxk
IGtub3cgYWJvdXQgdGhlbToKJCBweXRob24gdm9sLnB5IC1mIHN0dXhuZXQudm1lbSAtLXByb2ZpbGU9
V2luWFBTUDN4ODYgc3Zjc2Nhbgp8IGVncmVwIC1pICcobXJ4bmV0fG1yeGNscyknClZvbGF0aWxpdHkg
Rm91bmRhdGlvbiBWb2xhdGlsaXR5IEZyYW1ld29yayAyLjQKJApPbmUgd2F5IHRvIHZlcmlmeSB3aGV0
aGVyIHRoZSBzZXJ2aWNlcyBhcmUgYWN0dWFsbHkgcnVubmluZywgZGVzcGl0ZSB0aGUgZmFjdCB0aGF0
CnRoZXJlIGFyZSBubyBfU0VSVklDRV9SRUNPUkQgc3RydWN0dXJlcywgaW52b2x2ZXMgZmlyc3QgZGV0
ZXJtaW5pbmcgdGhlIGFzc29jaWF0ZWQga2VybmVsCm1vZHVsZS4gVGhlIHBhdGggaXMgc3RvcmVkIGlu
IHRoZSBJbWFnZVBhdGggdmFsdWUgb2YgdGhlIGNvcnJlc3BvbmRpbmcgcmVnaXN0cnkga2V5LiBBcwp5
b3UgY2FuIHNlZSBpbiB0aGUgZm9sbG93aW5nIG91dHB1dCwgdGhlIG1vZHVsZSBpcyBtcnhuZXQuc3lz
OgokIHB
                                       <text:soft-page-break/>

5dGhvbiB2b2wucHkgLWYgc3R1eG5ldC52bWVtIC0tcHJvZmlsZT1XaW5YUFNQM3g4NiBwcmludGtleQo
tSyAnQ29udHJvbFNldDAwMVxTZXJ2aWNlc1xNUnhOZXQnClZvbGF0aWxpdHkgRm91bmRhdGlvbiBWb2x
hdGlsaXR5IEZyYW1ld29yayAyLjQKTGVnZW5kOiAoUykgPSBTdGFibGUgKFYpID0gVm9sYXRpbGUKLS0
tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLQpSZWdpc3RyeTogXERldmljZVxIYXJkZGlza1ZvbHVtZTF
cV0lORE9XU1xzeXN0ZW0zMlxjb25maWdcc3lzdGVtCktleSBuYW1lOiBNUnhOZXQgKFMpCkxhc3QgdXB
kYXRlZDogMjAxMS0wNi0wMyAwNDoyNjo0NyBVVEMrMDAwMApTdWJrZXlzOgooVikgRW51bQpWYWx1ZXM
6ClJFR19TWiBEZXNjcmlwdGlvbiA6IChTKSBNUlhORVQKUkVHX1NaIERpc3BsYXlOYW1lIDogKFMpIE1
SWE5FVApSRUdfRFdPUkQgRXJyb3JDb250cm9sIDogKFMpIDAKUkVHX1NaIEdyb3VwIDogKFMpIE5ldHd
vcmsKUkVHX1NaIEltYWdlUGF0aCA6IChTKSBcPz9cQzpcV0lORE9XU1xzeXN0ZW0zMlxEcml2ZXJzXG1
yeG5ldC5zeXMKUkVHX0RXT1JEIFN0YXJ0IDogKFMpIDEKUkVHX0RXT1JEIFR5cGUgOiAoUykgMQpZb3U
gY2FuIGNyb3NzLXJlZmVyZW5jZSB0aGF0IG1vZHVsZSBuYW1lIHdpdGggdGhlIGN1cnJlbnRseSBsb2F
kZWQga2VybmVsIG1vZHVsZXM6CiQgcHl0aG9uIHZvbC5weSAtZiBzdHV4bmV0LnZtZW0gLS1wcm9maWx
lPVdpblhQU1AzeDg2IG1vZHVsZXMKfCBncmVwIG1yeG5ldC5zeXMKVm9sYXRpbGl0eSBGb3VuZGF0aW9
uIFZvbGF0aWxpdHkgRnJhbWV3b3JrIDIuNAoweDgxYzJhNTMwIG1yeG5ldC5zeXMgMHhiMjFkODAwMCA
weDMwMDAKXD8/XEM6XFdJTkRPV1Ncc3lzdGVtMzJcRHJpdmVyc1xtcnhuZXQuc3lzVGhlIG91dHB1dCB
zaG93cyBlbGV2ZW4gc2VydmljZXMgcHJpbnRlZCBpbiB0aHJlZSB1bmlxdWUgdGltZWZyYW1lcy4gVGh
lIG1vc3QgcmVjZW50CnRpbWVmcmFtZSAoMTMwNzA3NTIwNykgdHJhbnNsYXRlcyB0byAyMDExLTA2LTA
zIDA0OjI2OjQ3IFVUQy4gQXQgdGhpcyB0aW1lLCB0aGUgTVJ4Q2xzIGFuZApNUnhOZXQgc2VydmljZXM
gd2VyZSBlaXRoZXIgY3JlYXRlZCBvciBtb2RpZmllZC4gSXQgc2hvdWxkIGJlIGltbWVkaWF0ZWx5IHN
1c3BpY2lvdXMgdGhhdApuZWl0aGVyIG9mIHRoZXNlIHNlcnZpY2VzIGlzIHZpc2libGUgaW4gdGhlIG9
1dHB1dCBvZiBzdmNzY2FuLiBUaGlzIGlzIGEgc3Ryb25nIGluZGljYXRvciB0aGF0CnRoZSB0d28gc2V
ydmljZXMgYXJlIGhpZGRlbiAob3IgdGhleSB3ZXJlIHN0YXJ0ZWQgaW5hcHByb3ByaWF0ZWx5KTsgb3R
oZXJ3aXNlLCB0aGUgU0NNCndvdWxkIGtub3cgYWJvdXQgdGhlbToKJCBweXRob24gdm9sLnB5IC1mIHN
```

```
0dXhuZXQudm1lbSAtLXByb2ZpbGU9V2luWFBTUDN4ODYgc3Zjc2Nhbgp8IGVncmVwIC1pICcobXJ4bmV
0fG1yeGNscyknClZvbGF0aWxpdHkgRm91bmRhdGlvbiBWb2xhdGlsaXR5IEZyYW1ld29yayAyLjQKJAp
PbmUgd2F5IHRvIHZlcmlmeSB3aGV0aGVyIHRoZSBzZXJ2aWNlcyBhcmUgYWN0dWFsbHkgcnVubmluZyw
gZGVzcGl0ZSB0aGUgZmFjdCB0aGF0CnRoZXJlIGFyZSBubyBfU0VSVklDRV9SRUNPUkQgc3RydWN0dXJ
lcywgaW52b2x2ZXMgZmlyc3QgZGV0ZXJtaW5pbmcgdGhlIGFzc29jaWF0ZWQga2VybmVsCm1vZHVsZS4
gVGhlIHBhdGggaXMgc3RvcmVkIGluIHRoZSBJbWFnZVBhdGggdmFsdWUgb2YgdGhlIGNvcnJlc3BvbmR
pbmcgcmVnaXN0cnkga2V5LiBBcwp5b3UgY2FuIHNlZSBpbiB0aGUgZm9sbG93aW5nIG91dHB1dCwgdGh
lIG1vZHVsZSBpcyBtcnhuZXQuc3lzOgokIHB5dGhvbiB2b2wucHkgLWYgc3R1eG5ldC52bWVtIC0tcHJ
vZmlsZT1XaW5YUFNQM3g4NiBwcmludGtleQotSyAnQ29udHJvbFNldDAwMVxTZXJ2aWNlc1xNUnhOZXQ
nClZvbGF0aWxpdHkgRm91bmRhdGlvbiBWb2xhdGlsaXR5IEZyYW1ld29yayAyLjQKTGVnZW5kOiAoUyk
gPSBTdGFibGUgKFYpID0gVm9sYXRpbGUKLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLQpSZWdpc3R
yeTogXERldmljZVxIYXJkZGlza1ZvbHVtZTFcV0lORE9XU1xzeXN0ZW0zMlxjb25maWdcc3lzd[44833
3920e12dc9fd9c5e8c30e6b1ea2]:[b3f894165d6166da47d52ffbf77b5d87]ZXQgKFMpCkxhc3Qgd
XBkYXRlZDogMjAxMS0wNi0wMyAwNDoyNjo0NyBVVEMrMDAwMApTdWJrZXlzOgooVikgRW51bQpWYWx1Z
XM6ClJFR19TWiBEZXNjcmlwdGlvbiA6IChTKSBNUlhORVQKUkVHX1NaIERpc3BsYXlOYW1lIDogKFMpI
E1SWE5FVApSRUdfRFdPUkQgRXJyb3JDb250cm9sIDogKFMpIDAKUkVHX1NaIEdyb3VwIDogKFMpIE5ld
HdvcmsKUkVHX1NaIEltYWdlUGF0aCA6IChTKSBcPz9cQzpcV0lORE9XU1xzeXN0ZW0zMlxEcml2ZXJzX
G1yeG5ldC5zeXMKUkVHX0RXT1JEIFN0YXJ0IDogKFMpIDEKUkVHX0RXT1JEIFR5cGUgOiAoUykgMQpZb
3UgY2FuIGNyb3NzLXJlZmVyZW5jZSB0aGF0IG1vZHVsZSBuYW1lIHdpdGggdGhlIGN1cnJlbnRseSBsb
2FkZWQga2VybmVsIG1vZHVsZXM6CiQgcHl0aG9uIHZvbC5weSAtZiBzdHV4bmV0LnZtZW0gLS1wcm9ma
WxlPVdpblhQU1AzeDg2IG1vZHVsZXMKfCBncmVwIG1yeG5ldC5zeXMKVm9sYXRpbGl0eSBGb3VuZGF0a
W9uIFZvbGF0aWxpdHkgRnJhbWV3b3JrIDIuNAoweDgxYzJhNTMwIG1yeG5ldC5zeXMgMHhiMjFkODAwM
CAweDMwMDAKXD8/XEM6XFdJTkRPV1Ncc3lzdGVtMzJcRHJpdmVyc1xtcnhuZXQuc3l
                        <text:soft-page-break/>

zVGhlIG91dHB1dCBzaG93cyBlbGV2ZW4gc2VydmljZXMgcHJpbnRlZCBpbiB0aHJlZSB1bmlxdWUgdGl
tZWZyYW1lcy4gVGhlIG1vc3QgcmVjZW50CnRpbWVmcmFtZSAoMTMwNzA3NTIwNykgdHJhbnNsYXRlcyB
0byAyMDExLTA2LTAzIDA0OjI2OjQ3IFVUQy4gQXQgdGhpcyB0aW1lLCB0aGUgTVJ4Q2xzIGFuZApNUnh
OZXQgc2VydmljZXMgd2VyZSBlaXRoZXIgY3JlYXRlZCBvciBtb2RpZmllZC4gSXQgc2hvdWxkIGJlIGl
tbWVkaWF0ZWx5IHN1c3BpY2lvdXMgdGhhdApuZWl0aGVyIG9mIHRoZXNlIHNlcnZpY2VzIGlzIHZpc2l
ibGUgaW4gdGhlIG91dHB1dCBvZiBzdmNzY2FuLiBUaGlzIGlzIGEgc3Ryb25nIGluZGljYXRvciB0aGF
0CnRoZSB0d28gc2VydmljZXMgYXJlIGhpZGRlbiAob3IgdGhleSB3ZXJlIHN0YXJ0ZWQgaW5hcHByb3B
yaWF0ZWx5KTsgb3RoZXJ3aXNlLCB0aGUgU0NNCndvdWxkIGtub3cgYWJvdXQgdGhlbToKJCBweXRob24
gdm9sLnB5IC1mIHN0dXhuZXQudm1lbSAtLXByb2ZpbGU9V2luWFBTUDN4ODYgc3Zjc2Nhbgp8IGVncmV
wIC1pICcobXJ4bmV0fG1yeGNscyknClZvbGF0aWxpdHkgRm91bmRhdGlvbiBWb2xhdGlsaXR5IEZyYW1
ld29yayAyLjQKJApPbmUgd2F5IHRvIHZlcmlmeSB3aGV0aGVyIHRoZSBzZXJ2aWNlcyBhcmUgYWN0dWF
sbHkgcnVubmluZywgZGVzcGl0ZSB0aGUgZmFjdCB0aGF0CnRoZXJlIGFyZSBubyBfU0VSVklDRV9SRUN
PUkQgc3RydWN0dXJlcywgaW52b2x2ZXMgZmlyc3QgZGV0ZXJtaW5pbmcgdGhlIGFzc29jaWF0ZWQga2V
ybmVsCm1vZHVsZS4gVGhlIHBhdGggaXMgc3RvcmVkIGluIHRoZSBJbWFnZVBhdGggdmFsdWUgb2YgdGh
lIGNvcnJlc3BvbmRpbmcgcmVnaXN0cnkga2V5LiBBcwp5b3UgY2FuIHNlZSBpbiB0aGUgZm9sbG93aW5
nIG91dHB1dCwgdGhlIG1vZHVsZSBpcyBtcnhuZXQuc3lzOgokIHB5dGhvbiB2b2wucHkgLWYgc3R1eG5
ldC52bWVtIC0tcHJvZmlsZT1XaW5YUFNQM3g4NiBwcmludGtleQotSyAnQ29udHJvbFNldDAwMVxTZXJ
2aWNlc1xNUnhOZXQnClZvbGF0aWxpdHkgRm91bmRhdGlvbiBWb2xhdGlsaXR5IEZyYW1ld29yayAyLjQ
KTGVnZW5kOiAoUykgPSBTdGFibGUgKFYpID0gVm9sYXRpbGUKLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0
tLS0tLQpSZWdpc3RyeTogXERldmljZVxIYXJkZGlza1ZvbHVtZTFcV0lORE9XU1xzeXN0ZW0zMlxjb25
maWdcc3lzdGVtCktleSBuYW1lOiBNUnhOZXQgKFMpCkxhc3QgdXBkYXRlZDogMjAxMS0wNi0wMyAwNDo
yNjo0NyBVVEMrMDAwMApTdWJrZXlzOgooVikgRW51bQpWYWx1ZXM6ClJFR19TWiBEZXNjcmlwdGlvbiA
6IChTKSBNUlhORVQKUkVHX1NaIERpc3BsYXlOYW1lIDogKFMpIE1SWE5FVApSRUdfRFdPUkQgRXJyb3J
Db250cm9sIDogKFMpIDAKUkVHX1NaIEdyb3VwIDogKFMpIE5ldHdvcmsKUkVHX1NaIEltYWdlUGF0aCA
6IChTKSBcPz9cQzpcV0lORE9XU1xzeXN0ZW0zMlxEcml2ZXJzXG1yeG5ldC5zeXMKUkVHX0RXT1JEIFN
```

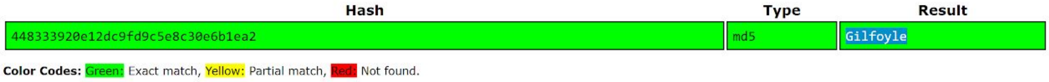
```
0YXJ0IDogKFMpIDEKUkVHX0RXT1JEIFR5cGUgOiAoUykgMQpZb3UgY2FuIGNyb3NzLXJlZmVyZW5jZSB
0aGF0IG1vZHVsZSBuYW1lIHdpdGggdGhlIGN1cnJlbnRseSBsb2FkZWQga2VybmVsIG1vZHVsZXM6CiQ
gcHl0aG9uIHZvbC5weSAtZiBzdHV4bmV0LnZtZW0gLS1wcm9maWxlPVdpblhQU1AzeDg2IG1vZHVsZXM
KfCBncmVwIG1yeG5ldC5zeXMKVm9sYXRpbGl0eSBGb3VuZGF0aW9uIFZvbGF0aWxpdHkgRnJhbWV3b3J
rIDIuNAoweDgxYzJhNTMwIG1yeG5ldC5zeXMgMHhiMjFkODAwMCAweDMwMDAKXD8/XEM6XFdJTkRPV1N
cc3lzdGVtMzJcRHJpdmVyc1xtcnhuZXQuc3lzVGhlIG91dHB1dCBzaG93cyBlbGV2ZW4gc2VydmljZXM
gcHJpbnRlZCBpbiB0aHJlZSB1bmlxdWUgdGltZWZyYW1lcy4gVGhlIG1vc3QgcmVjZW50CnRpbWVmcmF
tZSAoMTMwNzA3NTIwNykgdHJhbnNsYXRlcyB0byAyMDExLTA2LTAzIDA0OjI2OjQ3IFVUQy4gQXQgdGh
pcyB0aW1lLCB0aGUgTVJ4Q2xzIGFuZApNUnhOZXQgc2VydmljZXM
                   </text:p>
                   <text:p text:style-name="Standard">

gd2VyZSBlaXRoZXIgY3JlYXRlZCBvciBtb2RpZmllZC4gSXQgc2hvdWxkIGJlIGltbWVkaWF0ZWx5IHN
1c3BpY2lvdXMgdGhhdApuZWl0aGVyIG9mIHRoZXNlIHNlcnZpY2VzIGlzIHZpc2libGUgaW4gdGhlIG9
1dHB1dCBvZiBzdmNzY2FuLiBUaGlzIGlzIGEgc3Ryb25nIGluZGljYXRvciB0aGF0CnRoZSB0d28gc2V
ydmljZXMgYXJlIGhpZGRlbiAob3IgdGhleSB3ZXJlIHN0YXJ0ZWQgaW5hcHByb3ByaWF0ZWx5KTsgb3R
oZXJ3aXNlLCB0aGUgU0NNCndvdWxkIGtub3cgYWJvdXQgdGhlbToKJCBweXRob24gdm9sLnB5IC1mIHN
0dXhuZXQudm1lbSAtLXByb2ZpbGU9V2luWFBTUDN4ODYgc3Zjc2Nhbgp8IGVncmVwIC1pICcobXJ4bmV
0fG1yeGNscyknClZvbGF0aWxpdHkgRm91bmRhdGlvbiBWb2xhdGlsaXR5IEZyYW1ld29yayAyLjQKJAp
PbmUgd2F5IHRvIHZlcmlmeSB3aGV0aGVyIHRoZSBzZXJ2aWNlcyBhcmUgYWN0dWFsbHkgcnVubmluZyw
gZGVzcGl0ZSB0aGUgZmFjdCB0aGF0CnRoZXJlIGFyZSBubyBfU0VSVklDRV9SRUNPUkQgc3RydWN0dXJ
lcywgaW52b2x2ZXMgZmlyc3QgZGV0ZXJtaW5pbmcgdGhlIGFzc29jaWF0ZWQga2VybmVsCm1vZHVsZS4
gVGhlIHBhdGggaXMgc3RvcmVkIGluIHRoZSBJbWFnZVBhdGggdmFsdWUgb2YgdGhlIGNvcnJlc3BvbmR
pbmcgcmVnaXN0cnkga2V5LiBBcwp5b3UgY2FuIHNlZSBpbiB0aG
                         <text:soft-page-break/>

UgZm9sbG93aW5nIG91dHB1dCwgdGhlIG1vZHVsZSBpcyBtcnhuZXQuc3lzOgokIHB5dGhvbiB2b2wucH
kgLWYgc3R1eG5ldC52bWVtIC0tcHJvZmlsZT1XaW5YUFNQM3g4NiBwcmludGtleQotSyAnQ29udHJvbF
NldDAwMVxTZXJ2aWNlc1xNUnhOZXQnClZvbGF0aWxpdHkgRm91bmRhdGlvbiBWb2xhdGlsaXR5IEZyYW
1ld29yayAyLjQKTGVnZW5kOiAoUykgPSBTdGFibGUgKFYpID0gVm9sYXRpbGUKLS0tLS0tLS0tLS0tLS
0tLS0tLS0tLS0tLS0tLQpSZWdpc3RyeTogXERldmljZVxIYXJkZGlza1ZvbHVtZTFcV0lORE9XU1xzeX
N0ZW0zMlxjb25maWdcc3lzdGVtCktleSBuYW1lOiBNUnhOZXQgKFMpCkxhc3QgdXBkYXRlZDogMjAxMS
0wNi0wMyAwNDoyNjo0NyBVVEMrMDAwMApTdWJrZXlzOgooVikgRW51bQpWYWx1ZXM6ClJFR19TWiBEZX
NjcmlwdGlvbiA6IChTKSBNUlhORVQKUkVHX1NaIERpc3BsYXlOYW1lIDogKFMpIE1SWE5FVApSRUdfRF
dPUkQgRXJyb3JDb250cm9sIDogKFMpIDAKUkVHX1NaIEdyb3VwIDogKFMpIE5ldHdvcmsKUkVHX1NaIE
ltYWdlUGF0aCA6IChTKSBcPz9cQzpcV0lORE9XU1xzeXN0ZW0zMlxEcml2ZXJzXG1yeG5ldC5zeXMKUk
VHX0RXT1JEIFN0YXJ0IDogKFMpIDEKUkVHX0RXT1JEIFR5cGUgOiAoUykgMQpZb3UgY2FuIGNyb3NzLX
JlZmVyZW5jZSB0aGF0IG1vZHVsZSBuYW1lIHdpdGggdGhlIGN1cnJlbnRseSBsb2FkZWQga2VybmVsIG
1vZHVsZXM6CiQgcHl0aG9uIHZvbC5weSAtZiBzdHV4bmV0LnZtZW0gLS1wcm9maWxlPVdpblhQU1AzeD
g2IG1vZHVsZXMKfCBncmVwIG1yeG5ldC5zeXMKVm9sYXRpbGl0eSBGb3VuZGF0aW9uIFZvbGF0aWxpdH
kgRnJhbWV3b3JrIDIuNAoweDgxYzJhNTMwIG1yeG5ldC5zeXMgMHhiMjFkODAwMCAweDMwMDAKXD8/XE
M6XFdJTkRPV1Ncc3lzdGVtMzJcRHJpdmVyc1xtcnhuZXQuc3lz
                   </text:p>
             </office:text>
      </office:body>
</office:document-content>
```

Obtención de credenciales y acceso a la web

Vemos que existe parte del código en base64 hasta que encontramos 2 hash en formato md5 enmedio:

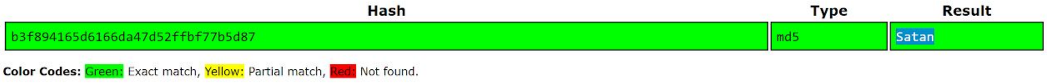
```
0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLQpSZWdpc3RyeTogXERldmljZVxIYXJkZGlza1ZvbHVtZT
FcV0lORE9XU1xzeXN0ZW0zMlxjb25maWdcc3lzd[448333920e12dc9fd9c5e8c30e6b1ea2]:[b3f89
4165d6166da47d52ffbf77b5d87]ZXQgKFMpCkxhc3QgdXBkYXRlZDogMjAxMS0wNi0wMyAwNDoyNjo0
NyBVVEMrMDAwMApTdWJrZ
```

Pasamos a crackear a través de la herramienta online que nos arroja la siguiente Gilfoyle y Satan



Hash	Type	Result
448333920e12dc9fd9c5e8c30e6b1ea2	md5	Gilfoyle

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



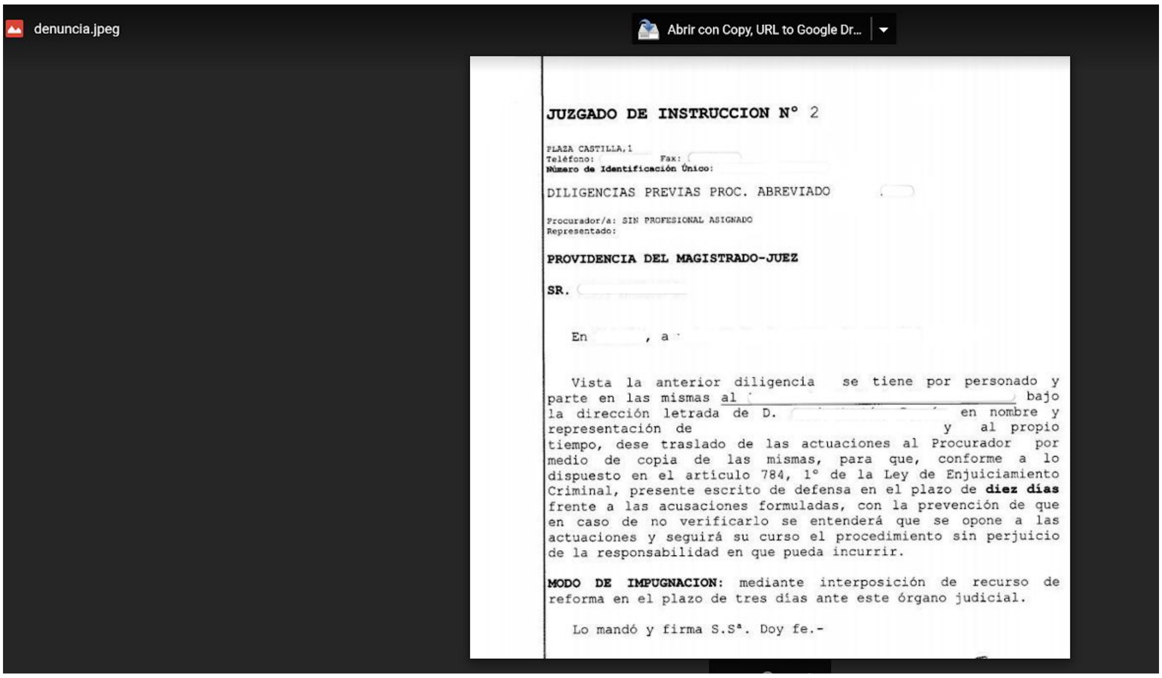
Hash	Type	Result
b3f894165d6166da47d52ffbf77b5d87	md5	Satan

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Con estas posibles credenciales visitamos la dirección http://34.247.69.86/siliconvalley/episodio1/login.php e introducimos como usuario a Gilfoley y password Satan y obtenemos el enlace con la providencia del juzgado:

```
Denuncia recibida:
https://drive.google.com/open?id=10iguWjRmx3mB0Y4g9iRrJOIXZ1HIJ_zC
```

Obtención de los metadatos y geolocalización



JUZGADO DE INSTRUCCION N° 2

PLAZA CASTILLA,1
Teléfono: Fax:
Número de Identificación Único:

DILIGENCIAS PREVIAS PROC. ABREVIADO

Procurador/a: SIN PROFESIONAL ASIGNADO
Representado:

PROVIDENCIA DEL MAGISTRADO-JUEZ

SR.

En , a

Vista la anterior diligencia se tiene por personado y parte en las mismas al bajo la dirección letrada de D. en nombre y representación de y al propio tiempo, dese traslado de las actuaciones al Procurador por medio de copia de las mismas, para que, conforme a lo dispuesto en el articulo 784, 1° de la Ley de Enjuiciamiento Criminal, presente escrito de defensa en el plazo de **diez días** frente a las acusaciones formuladas, con la prevención de que en caso de no verificarlo se entenderá que se opone a las actuaciones y seguirá su curso el procedimiento sin perjuicio de la responsabilidad en que pueda incurrir.

MODO DE IMPUGNACION: mediante interposición de recurso de reforma en el plazo de tres días ante este órgano judicial.

Lo mandó y firma S.Sª. Doy fe.-

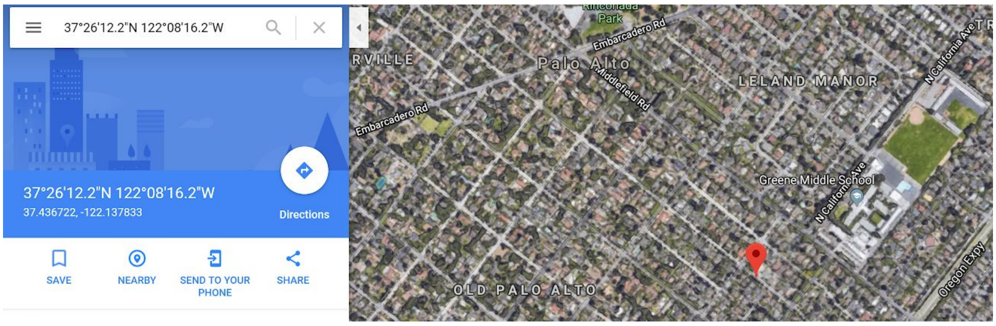
Lo descargamos y lo analizamos:

```
root@kali:~/Desktop/uam/SiliconValley# curl -L
"https://docs.google.com/uc?export=download&id=10iguWjRmx3mB0Y4g9iRrJOIXZ1HIJ_zC
" > output.jpeg
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   388    0   388    0     0    153      0 --:--:--  0:00:02 --:--:--   153
100  176k  100  176k    0     0  57628      0  0:00:03  0:00:03 --:--:-- 57628
root@kali:~/Desktop/uam/SiliconValley# file output.jpeg
output.jpeg: JPEG image data, JFIF standard 1.01, resolution (DPI), density
72x72, segment length 16, baseline, precision 8, 711x713, frames 3
```

```
root@kali:~/Desktop/uam/SiliconValley# exiftool output.jpeg
ExifTool Version Number         : 11.10
File Name                       : output.jpeg
Directory                       : .
File Size                       : 177 kB
File Modification Date/Time     : 2018:09:21 19:50:31+02:00
File Access Date/Time           : 2018:09:21 19:50:50+02:00
File Inode Change Date/Time     : 2018:09:21 19:50:31+02:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
XMP Toolkit                     : Image::ExifTool 11.10
Location                        : 37.436712, -122.137837
Profile CMM Type                : Little CMS
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2015:11:10 12:18:56
Profile File Signature          : acsp
Primary Platform                : Unknown (*nix)
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             :
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Little CMS
Profile ID                      : 0
Profile Description             : sRGB-elle-V2-srgbtrc.icc
Profile Copyright               : Copyright 2015, Elle Stone (website:
```

```
http://ninedegreesbelow.com/; email: ellestone@ninedegreesbelow.com). This ICC
profile is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported
License (https://creativecommons.org/licenses/by-sa/3.0/legalcode).
Media White Point               : 0.9642 1 0.82491
Chromatic Adaptation            : 1.04788 0.02292 -0.05022 0.02959 0.99048
-0.01707 -0.00925 0.01508 0.75168
Red Matrix Column               : 0.43604 0.22249 0.01392
Blue Matrix Column              : 0.14305 0.06061 0.71393
Green Matrix Column             : 0.38512 0.7169 0.09706
Red Tone Reproduction Curve     : (Binary data 8204 bytes, use -b option to
extract)
Green Tone Reproduction Curve   : (Binary data 8204 bytes, use -b option to
extract)
Blue Tone Reproduction Curve    : (Binary data 8204 bytes, use -b option to
extract)
Chromaticity Channels           : 3
Chromaticity Colorant           : Unknown (0)
Chromaticity Channel 1          : 0.64 0.33002
Chromaticity Channel 2          : 0.3 0.60001
Chromaticity Channel 3          : 0.15001 0.06
Image Width                     : 711
Image Height                    : 713
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 711x713
Megapixels                      : 0.507
```

En el apartado Location nos llama la atención la Geolocalización 37.436722, -122.137833 o 37°26'12.2"N 122°08'16.2"W

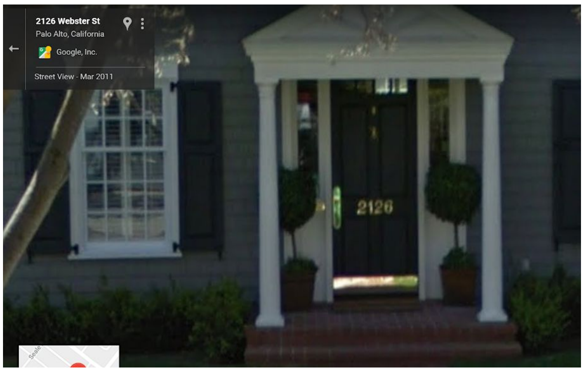


37°26'12.2"N 122°08'16.2"W

37°26'12.2"N 122°08'16.2"W

37.436722, -122.137833

Si nos acercamos más con herramienta de Street view observaremos el número de la puerta.



2126 Webster St

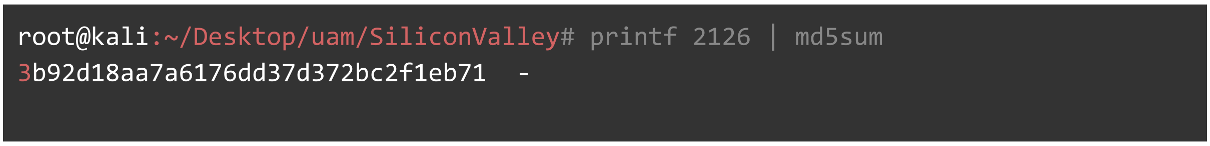
Palo Alto, California

Google, Inc.

Street View - Mar 2011

Obtención de la Flag

Pasamos el número 2126 a md5:



```
root@kali:~/Desktop/uam/SiliconValley# printf 2126 | md5sum
3b92d18aa7a6176dd37d372bc2f1eb71  -
```

Y la solución es ***UAM{3b92d18aa7a6176dd37d372bc2f1eb71}***

Autor: MXY0bg== a.k.a. 1v4n

Twitter: https://twitter.com/Hackers4f // https://twitter.com/1r0Dm48O