INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2022-2023 – 1st Period

Digital Forensics Report

Authors: Diogo Venâncio (95555), Sara Marques (93342), Sofia Morgado (95675)

1 Do you find any traces of the Fake NASA files on Prof. Seagal's computers?

Sim, no disco de backup.

Inicialmente, começamos por analisar o carl_disk, no offset 1054720, onde estava o /root. Encontramos o seeds.txt (na diretoria home/carlseagal, inode 674518), e na pasta backups (688862) os scripts pass_gen.sh (675523), backup.sh (674515) e o obfuscator (675415). O script backup.sh cria um zip protegido por uma password, da diretoria /Desktop/moon (6888695). Essa password é gerada a partir do pass_gen.sh que recebe como argumento o timestamp atual em UNIX, que por sua vez chama o obfuscator. Descompilamos o obfuscator, através da ferramenta uncompyle6) e obtivemos o obfuscator.py. Este script de python usa a primeira linha do seeds.txt e o timestamp para gerar uma password, utilizando o algoritmo sha-256. Para além disso, reescreve o ficheiros seeds.txt, passando a primeira linha para o fim. No entanto, na diretoria Desktop/moon não encontramos zips.

```
┌──(sofia㉿sofia)-[~/Desktop/CSF/P2]
└─$ fls -o 1054720 carl_disk.img 673895 -r
d/d 688695:     moon
+ d/d 688696:   _firefox
++ r/r 674617:  SiteSecurityServiceState.txt
++ d/d 688701:  datareporting
+++ d/d 688702: archived
++++ d/d 688707:        2022-10
+++++ r/r 657642:       1665192488527.9e05e20e-870f-4811-9749-bf0d33ea7e78.event.jsonlz4
++ r/r 674247:  AlternateServices.txt
```

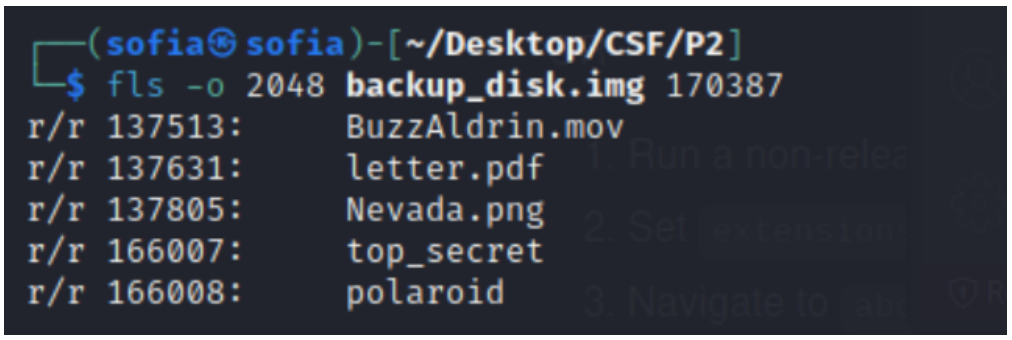
Extraímos e analisámos os ficheiros na imagem acima, no entanto, não nos deram grande informação.

Na diretoria home/carlseagal/Documents (673899) encontramos o schedule.jpeg (674520), e na diretoria home/carlseagal/Pictures (673901) as imagens dog.jpeg (674761) e index.jpeg (674570). Ainda encontramos o tool (674943) na diretoria (673896).

```
d/d 673896:     Downloads
+ d/d 674307:   thunderbird.tmp
+ r/r 674943:   tool
d/d 673897:     Templates
d/d 673898:     Public
d/d 673899:     Documents
+ r/r 674520:   schedule.jpeg
d/d 673900:     Music
d/d 673901:     Pictures
+ r/r 674570:   index.jpeg
+ r/r 674761:   dog.jpeg
```

De seguida, fomos analisar o backup_disk, no offset 2048, onde estava o /root. Na diretoria /home (137351), na pasta secrets (170387), encontrámos 5 dos 6 artefactos.

```
┌──(sofia㉿sofia)-[~/Desktop/CSF/P2]
└─$ fls -o 2048 backup_disk.img 137351
r/r 137353:     .profile
r/r 137354:     .bashrc
r/r 137355:     .bash_logout
d/d 137380:     .cache
d/d 137381:     .config
d/d 137387:     .local
d/d 137392:     Desktop
d/d 137394:     Downloads
d/d 137396:     Templates
d/d 137397:     Public
d/d 137398:     Documents
d/d 137399:     Music
d/d 137400:     Pictures
d/d 137401:     Videos
d/d 137577:     .ssh
d/d 137580:     .gnupg
r/r 166077:     .bash_history
d/d 137681:     .mozilla
d/d * 170373(realloc):  .fr-Vj8ECA
d/d 170387:     secrets
r/r 137417:     .vboxclient-clipboard.pid
r/r 166013:     backup_1665188803.zip
r/r 166050:     backup_1665189001.zip
r/r 137361:     backup_1665189601.zip
r/r 137626:     backup_1665190201.zip
r/r * 166077(realloc):  .goutputstream-HD15T1
r/r 137602:     .vboxclient-seamless.pid
r/r 165974:     .vboxclient-draganddrop.pid
r/r 166074:     .vboxclient-display-svga-x11.pid
```



Calculámos o SHA-256 através do comando "sha256sum" e depois de os comparar com os valores SHA-256 fornecidos, concluímos de que se tratavam dos mesmos documentos.

Ainda na diretoria /home (137351), encontramos ficheiros zips de backup protegidos por uma password (inodes 166013, 166050, 137361 e 137626). Pelo nome dos zips, concluímos que os scripts anteriormente descobertos foram usados para gerar estes zips. Como foram gerados 4 zips, a password do primeiro zip (backup_1665188803.zip, porque quanto menor o timestamp mais cedo foi criado) foi gerada com a 4ª última linha. Copiamos o ficheiro seeds.txt e criamos o seeds1.txt, restaurando para o seu estado original (passamos as quatro últimas linhas para o início). Criamos uma cópia do obfuscator.py (obfuscator1.py) para ler do seeds1.txt. Correndo o comando "python2 obfuscator1.py 1665188803", obtivemos a password d0d5ff7410dcf10125fbd7777740b2f0d8bb1c7043df78bb998b0ade2d6f3c3e, a qual usamos para fazer unzip do backup_1665188803.zip.

Depois de descomprimir todos os zips com o método anterior, obtivemos uma pasta, que tinha todos os documentos que tinham sido entregues na primeira entrega (incluindo o ficheiro "worksmanship.png" que não tinha sido encontrado anteriormente, e encontrava-se apenas no backup_1665190201.zip com a password 296c0a0eb14443561fa31256ab05a90fa3439e4b3c830a6971a4d87d20bfec56), assim como uma pasta "_firefox".

Ficheiros Entregues no Laboratório 1	SHA-256	Ficheiros encontrados	SHA-256
f3.mov	bc8a2d12aa1e8f280294a7b413612e739927b789181c826c30cbe2b460513480	BuzzAldrin.mov	bc8a2d12aa1e8f280294a7b413612e739927b789181c826c30cbe2b460513480
f2.png	4ec286d1b6fbb9466d1f68dcdd6d248441645be85be6f4bf0365f068060486da	Nevada.png	4ec286d1b6fbb9466d1f68dcdd6d248441645be85be6f4bf0365f068060486da
f1.jpeg	15d41c98cba533dd7c9703409109d72c53bec3d85b20e687fe86c464caebf6b5	polaroid.jpeg	15d41c98cba533dd7c9703409109d72c53bec3d85b20e687fe86c464caebf6b5
f5.pdf	73a6b01845a1365e3f9a	top_secret.pdf	73a6b01845a1365e3f9a

	6f48fdf93651f0efc07575ce1a89c5f32e01babf20ec		6f48fdf93651f0efc07575ce1a89c5f32e01babf20ec
f6.pdf	631fb4c4aadc6ca3f46310466974c85d9ab226e6617096eb0206a22b6fbd5872o	letter.pdf	631fb4c4aadc6ca3f46310466974c85d9ab226e6617096eb0206a22b6fbd5872
f4.png	d330090e25b709aa1a9cdb28d60b103218aeeb470ecaa2df461157297a4a6444	worksmanship.png	d330090e25b709aa1a9cdb28d60b103218aeeb470ecaa2df461157297a4a6444

2 If so, can you track the source of these files and how they have been manipulated over time? Establish a timeline of relevant events.

No disco carl_disk.img, encontramos o ficheiro syslog (540979) na diretoria var/log (565702). Através deste ficheiro, conseguimos verificar que uma pen USB com o serial number 14c0f244af16f6 foi conectada às 15:27:02 no computador de Carl, depois de ter sido entregue por Meghan no café Muddy Charles.

Através da análise do ficheiro .bash_history (674722) na diretoria home/carseagal e do web history (obtido através da análise da pasta _firefox obtida do backup_1665188803.zip com o programa Autopsy, do ficheiro places.sqlite) , vimos que ele fez cópia do conteúdo da pen (comandos “ls /media/carlseagal/PEN/” “cp -r /media/carlseagal/PEN/files/ moon/”) para a pasta moon no Desktop.

Começou por desencriptar o Corrupted.pdf (“base64 -d Corrupted.pdf | less”) e, com o link obtido no início do ficheiro desencriptado, fez o download do ficheiro tool no link https://www.dropbox.com/s/noy9sq3i3cxzkol/tool, às 15:31:17. O resultado obtido é posto no ficheiro tool.pyc. De seguida, pesquisa por um descompilador online, e encontra o https://www.toolnb.com/tools-lang-en/pyc.html colocando a descompilação no ficheiro tool.py e corre o script (“python3 tool.py”). Depois pesquisa pela letra da canção Ice Baby e coloca-a no ficheiro ice.txt. Corre novamente o script com uma palavra da letra da música, e obtém o Corrupted.pdf_dec onde está a carta do ex-presidente.

A seguir, instala o exiftool e usa-o no Relativity.gif obtendo um zip “out” onde está uma imagem Nevada.png. Retoma a comunicação com a Meghan pelo irc, onde ela o aconselha a esconder os ficheiros num local seguro, num servidor, e de os eliminar de forma segura do seu computador. Então, Carl prepara e executa uma ligação ssh para um servidor localizado numa rede local (192.168.1.84) chamado backup, e testa a ligação.

Na diretoria home, no seu computador pessoal, cria a pasta backups. Depois cria os scripts que foram posteriormente usados para gerar passwords para proteger os artefactos nos zips encontrados. Depois move os artefactos para a diretoria moon no Desktop e corre o script backup.sh numa cron task que é executada 4 vezes criando os zips mencionados com este conteúdo e enviando-os utilizando a ferramenta “rsync” para o seu servidor de backup.

```
Oct  7 15:25:42 ubuntu systemd[1306]: Starting Tracker metadata extractor ...
Oct  7 15:25:42 ubuntu dbus-daemon[1328]: [session uid=1000 pid=1328] Successfully activated service 'org.freedesktop.Tracker3.Miner.Extract'
Oct  7 15:25:42 ubuntu systemd[1306]: Started Tracker metadata extractor.
Oct  7 15:27:02 ubuntu kernel: [ 1778.095946] usb 1-2: new full-speed USB device number 4 using ohci-pci
Oct  7 15:27:03 ubuntu kernel: [ 1778.607990] usb 1-2: config 1 interface 0 altsetting 0 endpoint 0x1 has invalid maxpacket 512, setting to 64
Oct  7 15:27:03 ubuntu kernel: [ 1778.607994] usb 1-2: config 1 interface 0 altsetting 0 endpoint 0x82 has invalid maxpacket 512, setting to 64
Oct  7 15:27:03 ubuntu kernel: [ 1778.628751] usb 1-2: New USB device found, idVendor=126f, idProduct=0161, bcdDevice= 1.00
Oct  7 15:27:03 ubuntu kernel: [ 1778.628756] usb 1-2: New USB device strings: Mfr=0, Product=2, SerialNumber=3
Oct  7 15:27:03 ubuntu kernel: [ 1778.628757] usb 1-2: Product: USB Mass Storage Device
Oct  7 15:27:03 ubuntu kernel: [ 1778.628759] usb 1-2: SerialNumber: 14c0f244af16f6
Oct  7 15:27:03 ubuntu mtp-probe: checking bus 1, device 4: "/sys/devices/pci0000:00/0000:00:06.0/usb1/1-2"
Oct  7 15:27:03 ubuntu mtp-probe: bus: 1, device: 4 was not an MTP device
Oct  7 15:27:03 ubuntu kernel: [ 1778.695790] usb-storage 1-2:1.0: USB Mass Storage device detected
Oct  7 15:27:03 ubuntu kernel: [ 1778.702064] scsi host3: usb-storage 1-2:1.0
Oct  7 15:27:03 ubuntu kernel: [ 1778.702833] usbcore: registered new interface driver usb-storage
Oct  7 15:27:03 ubuntu kernel: [ 1778.718098] usbcore: registered new interface driver uas
Oct  7 15:27:03 ubuntu mtp-probe: checking bus 1, device 4: "/sys/devices/pci0000:00/0000:00:06.0/usb1/1-2"
Oct  7 15:27:03 ubuntu mtp-probe: bus: 1, device: 4 was not an MTP device
Oct  7 15:27:04 ubuntu kernel: [ 1779.748938] scsi 3:0:0:0: Direct-Access     USB2.0   Mobile Disk      1.00 PQ: 0 ANSI: 2
Oct  7 15:27:04 ubuntu kernel: [ 1779.752990] sd 3:0:0:0: Attached scsi generic sg2 type 0
Oct  7 15:27:04 ubuntu kernel: [ 1779.780322] sd 3:0:0:0: [sdb] 2007040 512-byte logical blocks: (1.03 GB/980 MiB)
Oct  7 15:27:04 ubuntu kernel: [ 1779.797221] sd 3:0:0:0: [sdb] Write Protect is off
Oct  7 15:27:04 ubuntu kernel: [ 1779.797227] sd 3:0:0:0: [sdb] Mode Sense: 00 00 00 00
Oct  7 15:27:04 ubuntu kernel: [ 1779.813957] sd 3:0:0:0: [sdb] Asking for cache data failed
Oct  7 15:27:04 ubuntu kernel: [ 1779.813965] sd 3:0:0:0: [sdb] Assuming drive cache: write through
Oct  7 15:27:04 ubuntu kernel: [ 1780.006635]  sdb: sdb1
Oct  7 15:27:04 ubuntu kernel: [ 1780.092658] sd 3:0:0:0: [sdb] Attached SCSI removable disk
Oct  7 15:27:05 ubuntu systemd-udevd[3815]: sdb: Process '/usr/bin/unshare -m /usr/bin/snap auto-import --mount=/dev/sdb' failed with exit code 1.
Oct  7 15:27:06 ubuntu dbus-daemon[1328]: [session uid=1000 pid=1328] Activating service name='org.gnome.Nautilus' requested by ':1.38' (uid=1000 pid=1499
Oct  7 15:27:06 ubuntu dbus-daemon[1328]: [session uid=1000 pid=1328] Successfully activated service 'org.gnome.Nautilus'
Oct  7 15:27:06 ubuntu systemd-udevd[3815]: sdb1: Process '/usr/bin/unshare -m /usr/bin/snap auto-import --mount=/dev/sdb1' failed with exit code 1.
Oct  7 15:27:07 ubuntu dbus-daemon[550]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.ser
tion-service " label="unconfined")
Oct  7 15:27:07 ubuntu systemd[1]: Starting Hostname Service ...
Oct  7 15:27:07 ubuntu gnome-shell[1499]: Could not create transient scope for PID 0: GDBus.Error:org.freedesktop.systemd1.UnitExists: Unit app-gnome-org.g
Oct  7 15:27:07 ubuntu kernel: [ 1782.879002] FAT-fs (sdb1): Volume was not properly unmounted. Some data may be corrupt. Please run fsck.
Oct  7 15:27:07 ubuntu udisksd[594]: Mounted /dev/sdb1 at /media/carlseagal/PEN on behalf of uid 1000
Oct  7 15:27:07 ubuntu dbus-daemon[550]: [system] Successfully activated service 'org.freedesktop.hostname1'
Oct  7 15:27:07 ubuntu systemd[1]: Started Hostname Service.
```

Web history:

Web History

Table | Thumbnail | Summary

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
places.sqlite			1	https://www.mozilla.org/en-US/privacy/firefox/	2022-10-07 15:30:23 BST	https://www.mozilla.org/privacy/firefox/	Firefox Privacy Notice — Mozilla
places.sqlite			2	https://www.dropbox.com/s/noy9sq3i3cxzkol/tool	2022-10-07 15:31:17 BST	https://tiny.cc/7o2d6LuDVN5d	tool
places.sqlite			1	https://ucb3567716b0610686d96a89061b.dl.dropboxuser...	2022-10-07 15:31:35 BST	https://www.dropbox.com/s/noy9sq3i3cxzkol/tool	tool
places.sqlite			2	https://www.google.com/search?channel=fs&client=ubunt...	2022-10-07 15:32:58 BST		python decompiler online - Pesquisa Google
places.sqlite			2	https://www.toolnb.com/tools-lang-en/pyc.html	2022-10-07 15:33:08 BST		PyC decompile - Toolnb online toolbox
places.sqlite			2	https://www.google.com/search?channel=fs&client=ubunt...	2022-10-07 15:37:58 BST		ice baby lyrics - Pesquisa Google
places.sqlite			2	https://www.google.com/search?channel=fs&client=ubunt...	2022-10-07 15:40:50 BST		hexedit - Pesquisa Google
places.sqlite			1	https://hexed.it/	2022-10-07 15:40:53 BST		HexEd.it - Browser-based Online and Offline Hex Editing
places.sqlite			2	https://www.google.com/search?channel=fs&client=ubunt...	2022-10-07 23:39:01 BST		hexedit - Pesquisa Google

Estabelecemos a seguinte timeline para os eventos:

- **05/10/22 19:49** - Primeiro contacto de Meghan Polanski a Carl Seagal pelo ThunderBird, em que informa que está a trabalhar em algo que pode ser do interesse de Carl. Sugere continuar a conversa por IRC.
- **07/10/22 15:08 -** Os dois indivíduos começam o contacto por IRC. Meghan informa que tem consigo provas de que a chegada à Lua foi falsa e combina encontrar-se por volta das 15:21 com Carl no Muddy Charles, no MIT.
- **07/10/22 15:21 até 15:48 -** Pen recebida por Carl.
- **07/10/22 15:27:02 -** Pen inserida no computador de Carl.
- **07/10/22 15:28:17 -** Pen removida do computador de Carl
- **07/10/22 15:31:17 -** Acede ao website https://www.dropbox.com/s/noy9sq3i3cxzkol/tool e faz download do ficheiro tool
- **07/10/22 15:32:58 -** Pesquisa de descompilador online
- **07/10/22 15:33:08 -** Acede ao website https://www.toolnb.com/tools-lang-en/pyc.htm
- **07/10/22 15:37:58 -** Pesquisa das letras da música Ice Baby
- **07/10/22 15:40:53 -** Acede ao website https://hexed.it/

- **07/10/22 15:48 -** Um contacto por IRC é novamente criado pelos dois indivíduos, em que Meghan pergunta se Carl já conseguiu extrair todos os ficheiros. Aconselha-o a esconder os ficheiros num local seguro, como por exemplo, num servidor, e a eliminá-los de forma segura do seu computador. Combinam também em não contactar um ao outro nos próximos tempos.
- **08/10/22 01:26:43** - Ficheiro backup_1665188803.zip criado
- **08/10/22 01:30:01** - Ficheiro backup_1665189001.zip criado
- **08/10/22 01:40:01** - Ficheiro backup_1665189601.zip criado
- **08/10/22 01:50:01** - Ficheiro backup_1665190201.zip criado

3 Do you find any evidence of anti-forensic activity?

No ficheiro .bash_history (674722), presente na home/carlseagal, do disco carl_disk.img, conseguimos ver que o Carl Seagal instalou a ferramenta "srm" através do comando "sudo apt-get install secure-delete". Após uma pequena pesquisa (https://www.mankier.com/1/srm), chegámos à conclusão que esta ferramenta é usada para apagar os ficheiros de forma segura, pois faz overwrite dos dados dos ficheiros, antes de os apagar, pelo que não é possível recuperá-los, por exemplo, através de ferramentas de file carving, como Scalpel e Foremost. Após a sua instalação, foi usada para apagar os artefactos que havia colocado na diretoria Desktop/moon.

```
man srm
sudo apt-get install secure-delete
man srm
man srm > man_srm_txt
mv man_srm_txt Desktop/moon/
cd Desktop/moon/
ls
rm -r _
cd ..
srm -vz moon/*
srm -vz -r  moon/*
rm -r moon/
```

Para além disto, dentro da pasta recuperado nos zips protegidos por palavras passe "home/carlseagal/Desktop/moon/_firefox/places.sqlite", encontramos pesquisas e referências às ferramentas que utilizou para ocultar os artefactos que lhe haviam sido dados como o hexedit e um link de dropbox para a ferramenta que usou para encriptar o ficheiro .pdf (tool.py).

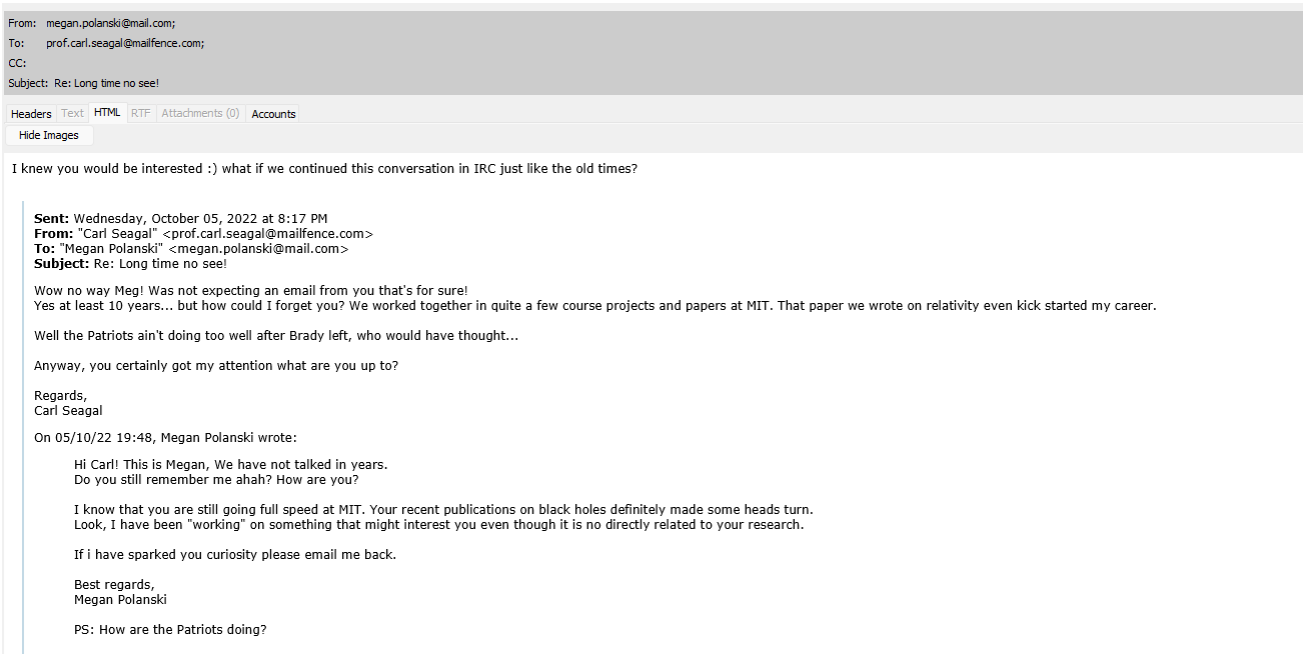
Web History

Table | Thumbnail | Summary

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	Domain
places.sqlite			1	https://www.mozilla.org/en-US/privacy/firefox/	2022-10-07 15:30:23 BST	https://www.mozilla.org/privacy/firefox/	Firefox Privacy Notice — Mozilla	FireFox	mozilla.org
places.sqlite			2	https://www.dropbox.com/s/noy9sq3i3cxzkol/tool	2022-10-07 15:31:17 BST	https://tiny.cc/7o2d6LuDVNSd	tool	FireFox	dropbox.com
places.sqlite			1	https://ucb3567716b0610686d96a89061b.dl.dropboxuser...	2022-10-07 15:31:35 BST	https://www.dropbox.com/s/noy9sq3i3cxzkol/tool	tool	FireFox	dropboxusercontent.com
places.sqlite			2	https://www.google.com/search?channel=fs&client=ubunt...	2022-10-07 15:32:58 BST		python decompiler online - Pesquisa Google	FireFox	google.com
places.sqlite			2	https://www.toolnb.com/tools-lang-en/pyc.html	2022-10-07 15:33:08 BST		PyC decompile - Toolnb online toolbox	FireFox	toolnb.com
places.sqlite			2	https://www.google.com/search?channel=fs&client=ubunt...	2022-10-07 15:37:58 BST		ice baby lyrics - Pesquisa Google	FireFox	google.com
places.sqlite			2	https://www.google.com/search?channel=fs&client=ubunt...	2022-10-07 15:40:50 BST		hexedit - Pesquisa Google	FireFox	google.com
places.sqlite			1	https://hexed.it/	2022-10-07 15:40:53 BST		HexEd.it - Browser-based Online and Offline Hex Editing	FireFox	hexed.it
places.sqlite			2	https://www.google.com/search?channel=fs&client=ubunt...	2022-10-07 23:39:01 BST		hexedit - Pesquisa Google	FireFox	google.com

4 What can you tell about the identity of the person(s) involved in the leakage of the files?

Começamos por procurar emails do Thunderbird na diretoria home/carseagal/snap (655363) . Encontramos o ficheiro Inbox (674446) na diretoria home/carseagal/snap/thunderbird/common/.thunderbird/weis2yij.default/Mail/pop.mailfence.com (674445). Ao analisarmos o ficheiro, deparamo-nos com vários emails, sendo o mais relevante a troca de emails entre prof.carl.seagal@mailfence.com e megan.polanski@mail.com. Nestes emails, Meghan refere que está a trabalhar sobre um assunto que pode interessar Carl e sugere continuar a conversa por irc.



From: megan.polanski@mail.com;
To: prof.carl.seagal@mailfence.com;
CC:
Subject: Re: Long time no see!

Headers Text HTML RTF Attachments (0) Accounts

Hide Images

I knew you would be interested :) what if we continued this conversation in IRC just like the old times?

Sent: Wednesday, October 05, 2022 at 8:17 PM
From: "Carl Seagal" <prof.carl.seagal@mailfence.com>
To: "Megan Polanski" <megan.polanski@mail.com>
Subject: Re: Long time no see!

Wow no way Meg! Was not expecting an email from you that's for sure!
Yes at least 10 years... but how could I forget you? We worked together in quite a few course projects and papers at MIT. That paper we wrote on relativity even kick started my career.

Well the Patriots ain't doing too well after Brady left, who would have thought...

Anyway, you certainly got my attention what are you up to?

Regards,
Carl Seagal

On 05/10/22 19:48, Megan Polanski wrote:

> Hi Carl! This is Megan, We have not talked in years.
> Do you still remember me ahah? How are you?
>
> I know that you are still going full speed at MIT. Your recent publications on black holes definitely made some heads turn.
> Look, I have been "working" on something that might interest you even though it is no directly related to your research.
>
> If i have sparked you curiosity please email me back.
>
> Best regards,
> Megan Polanski
>
> PS: How are the Patriots doing?

Procuramos estas comunicações na pasta irssi (688597) na diretoria home/carseagal/snap (673929).

```
┌──(sofia㉿sofia)-[~/Desktop/CSF/P2]
└─$ fls -o  1054720 carl_disk.img 688597 -r
d/d 688598:     838
d/d 688599:     common
+ d/d 688602:   .irssi
++ r/r 675259:  config
+ d/d 688603:   irclogs
++ d/d 688604:  2022
+++ d/d 688605: EFNet
++++ r/r 674443:        auth.10-07.log
++++ r/r 674245:        #lrh.10-07.log
++++ r/r 674246:        mpolanski.10-07.log
+++ d/d 688859: EFNet2
++++ r/r 675336:        auth.10-07.log
+++ d/d 688860: EFNet3
++++ r/r 674633:        auth.10-07.log
++++ r/r 675380:        nlopm.10-07.log
+++ d/d 688861: EFNet4
++++ r/r 675340:        auth.10-07.log
l/l 674248:     current
```

Ao investigar o log de mpolanski.10-07 (674246), deparamo-nos com uma conversa entre Meghan Polanski e Carl Seagal sobre como no passado ambos já tinham suspeitas sobre a chegada à Lua. Meghan refere que é casada com Chris Cox, o neto do ex-presidente da NASA, o qual recebeu uma carta do avô em que confessa que a chegada à Lua foi uma farsa. Combinam encontrar-se no café Muddy Charles no MIT por volta das 15:21 no dia 7 de Outubro, onde Meghan terá dado a Carl a pen com as restantes provas.

```
--- Log opened Fri Oct 07 15:08:42 2022
15:08 -!- Irssi: Starting query in EFNet with MPolanski
15:08 <carlseaga> Hi Meg!!
15:09 <carlseaga> just finished installing the irc client
15:09 <carlseaga> you dont even know how much nostalgia this brings me
15:09 <MPolanski> hey carl!
15:09 <MPolanski> ikr, we used to talk through here all the time
15:09 <MPolanski> brings back memories of the good old times
15:09 <MPolanski> nowadays no one uses this anymore
15:09 <carlseaga> i mean, its fair, now there are a thousand other apps that are much more practical, like skype and whatsapp
15:10 <MPolanski> thats true
15:10 <carlseaga> anyways, what did you want to tell me? im quite curious...
15:10 <MPolanski> okay, so do you remember our many conversations about the moon landing of 1969?
15:10 <carlseaga> of course i do
15:10 <carlseaga>  i used to be so determined on exposing that fraud
15:10 <MPolanski> yeah, i had to endure so many long rants about how obviously fake it was, and how stupid everyone was for believing it
15:10 <MPolanski> honestly it was scary how passionate you were about that ahahah
15:11 <carlseaga> yeah... but ive given up on that already
15:11 <MPolanski> i was naive in thinking that science could diprove that level of lies
15:11 <MPolanski> you better rekindle that passion then
15:11 <MPolanski> i have something that you might like
15:11 <carlseaga> huh?
15:11 <carlseaga> what is it?
15:12 <MPolanski> i have proof carl
15:12 <MPolanski> proof that the moon landing was fake
15:12 <MPolanski> its not scientific proof, its even better
15:12 <MPolanski> i have secret documents
15:12 <carlseaga> no way
15:12 <carlseaga> youre not joking around with me are you?
15:12 <MPolanski> im not!!
15:12 <MPolanski> i know how important this is for you, i would never lie to you about something like this
15:13 <carlseaga> hhmm
15:13 <carlseaga> what kind of documents do you have then?
15:13 <MPolanski> do you know my husband?
15:13 <carlseaga> your husband?
15:13 <carlseaga> Chris Cox right?
15:13 <carlseaga> grandson of the ex-president?
15:13 <MPolanski> exactly
15:13 <MPolanski> would you believe me if i told you that i got hold of the letter that Richard Nixon wrote to Chris, telling him that the moon landing was fake?
15:13 <carlseaga> NO WAY
15:14 <MPolanski> yes way ;)
15:14 <carlseaga> but are you fine with leaking that? its your husbands secret
15:15 <MPolanski> dont worry about that, there is no way i wasnt going to share something as important as this with my ol pal
15:15 <MPolanski> anyway
15:15 <MPolanski> I really go to go
15:16 <MPolanski> can you meet me at the muddy charles in like 5min?
15:16 <carlseaga> I had no idea you were in town
15:16 <carlseaga> 5min? sure
15:16 <carlseaga> you can bet ill be there
15:16 <MPolanski> see you there then
15:16 <carlseaga> bey
15:17 -!- MPolanski [~meganpola@bl17-148-196.dsl.telepac.pt] has quit [Quit: leaving]
```

Depois do encontro, Meghan pede a Carl que esconda os ficheiros e os elimine do computador.

```
15:17 -!- MPolanski [~meganpola@bl17-148-196.dsl.telepac.pt] has quit [Quit: leaving]
--- Log closed Fri Oct 07 15:17:08 2022
--- Log opened Fri Oct 07 15:48:05 2022
15:48 -!- Irssi: Starting query in EFNet with MPolanski
15:48 <MPolanski> Hi again
15:48 <MPolanski> Have you managed to obtain all the secret files?
15:48 <carlseaga> I am working on it
15:48 <carlseaga> you hid them well
15:49 <MPolanski> sorry about that
15:49 <MPolanski> i had to make sure only you could access them
15:49 <MPolanski> just in case something happened
15:50 <carlseaga> of course
15:50 <carlseaga> i've looked at some of the files and it really is unbelievable
15:50 <carlseaga> how is it possible that all of these documents, all of this proof, was buried for such a long time
15:50 <MPolanski> it really is carl! i couldn't believe it as well.. really makes you wonder on what secrets people can hide
15:51 <MPolanski> but remember that it is really important for you too hide the files
15:51 <MPolanski> we must leave no traces
15:51 <carlseaga> definitely
15:52 <carlseaga> i'll do my best to lay low and hide the files.. but how should i go with it??
15:52 <MPolanski> first off you need to find a way to securely delete them from your pc
15:52 <MPolanski> as well as hide them in a secure mean, like a server
15:52 <MPolanski> the internet will have your answers ;)
15:52 <carlseaga> ok, i'll do so
15:52 <MPolanski> good luck!
15:53 <MPolanski> we're writting history carl, look at us
15:53 <carlseaga> indeed we are..
15:53 <carlseaga> once again, i'm so very grateful meg this is truly something
15:53 <carlseaga> now, i must resist the urge to share it with the world
15:54 <MPolanski> its best if we dont talk for a while now Carl
15:54 <carlseaga> yes
15:54 <MPolanski> see you carl, stay safe
15:55 <carlseaga> you too meg, you too
--- Log closed Fri Oct 07 15:55:19 2022
```

SHA-256 dos Evidence Artifacts

Ficheiro	SHA-256
seeds.txt	3296b803bf327dfe9e26caf89df23f4d23ee6222871be80d4178fa2d1815cc70
obfuscator	e3d217351855e3caab70c49f761816dc66f102f095d7391c08cbac5a743dd0bc
backup.sh	de1307a1be0a72d8286d5804cba931f8259cf0b31c38599547b8abda0405ab50
pass_gen.sh	535dafaf7e7f6eefa12ea6ae4b1d00e859c41adb683fc298387de38e151ebe8e
obfuscator.py	82d9f9f557a24ead06a8166840ac5e2eb909592c1d7ef6e3fb6e461365c6b471
mpolanski.10-07.log	870e71c0f270a0261631e882539ebd2972421ed391abbbf0d93fb9a8bf46c5b6
syslog	bfa7d49a446e4f9f5d44ad98eab0159bf7116ac1a7d36ac1d28462a7a8efe6db
bash_history	338d485d9ffb200e34abdb69e08d0c0a9eb962819146a710d935f224efa4dc82
Inbox	18d2d3616206771a8583de6fb3d4c0d4b82f175ffbee6102786c2ebe04303491
dog.jpeg	33f529c886139263beb88b904dde31e4f594e896f4ec703294fbc251148dd8b6
index.jpeg	9ac54bc46ef75257ff13aa738003f6ef6b89b030b78201a4bda75ebbe4c98ac8
tool	88c57fb63c8fa3c11580b3217c4ebd99c09bf2c3838a908e9ba94e9b9f02c625
BuzzAldrin.mov	bc8a2d12aa1e8f280294a7b413612e739927b789181c826c30cbe2b460513480
Nevada.png	4ec286d1b6fbb9466d1f68dcdd6d248441645be85be6f4bf0365f068060486da
polaroid.jpeg	15d41c98cba533dd7c9703409109d72c53bec3d85b20e687fe86c464caebf6b5
top_secret.pdf	73a6b01845a1365e3f9a6f48fdf93651f0efc07575ce1a89c5f32e01babf20ec

letter.pdf	631fb4c4aadc6ca3f46310466974c85d9ab226e6617096eb0206a22b6fbd5872
places.sqlite	da12f02c021b3de7180282bf1f242684116f616600b54b0121de1dded3985888
backup_1665188803.zip	06fdbd1733a4bea7fd236247fc7a5bfaf8c51048943b7e5929d1494ceb170a02
backup_1665189001.zip	32493d41005defb0f651fa3d35d9464e470f1e4c73ca8d8eff562c652f1be50e
backup_1665189601.zip	f4db053055617927c978deb71411885a1ea627fafeac2c8c3c3bcb0ee0f914ac
backup_1665190201.zip	1d2b90f0786d5db9aeadb7f006e6f7a3ff1339038d610d81c5022f54beb8ee44