INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2022-2023 – 1st Period

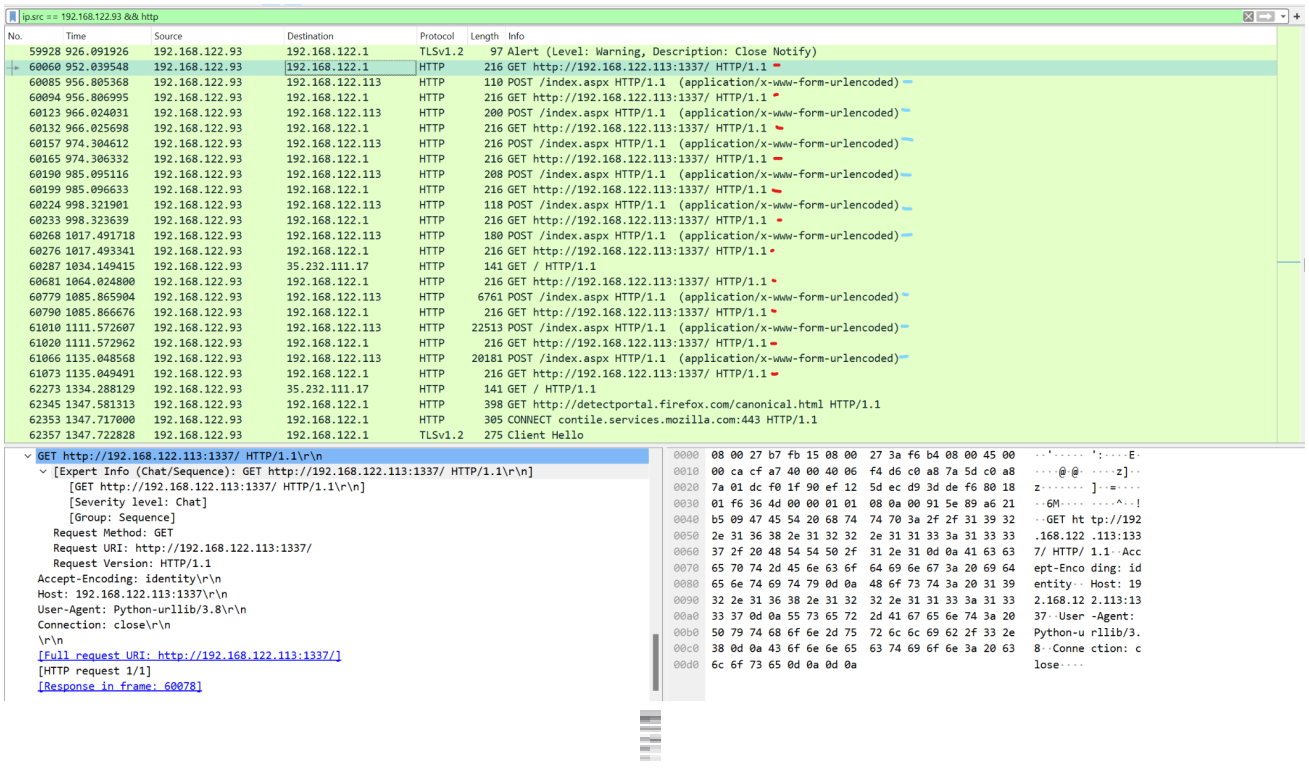
Digital Forensics Report

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

1 Do you find any evidence of transfers involving the documents in the analyzed network traces? What can you tell about the source and authenticity of these documents?

O zip que encontramos, “maldives-video”, continha o ficheiro “maldives”, uma pasta .video com um "vídeo de palmeiras, a pasta .malware com o ficheiro “shell”. Ao analisar o ficheiro “maldives”, este reproduz o vídeo de palmeiras enquanto instala um módulo de python e executa o ficheiro python “shell” com os argumentos 192.168.122.113 1337, cujo endereço IP pertence ao computador de Meghan. O ficheiro “shell” estabelece uma conexão HTTP entre a máquina onde o código está a ser executado e a máquina cujo IP recebe como argumento. Os ficheiros da primeira máquina são encriptados com o algoritmo SHA-256 e com uma password ("Fj39@vF4@54&8dE@!)(*^+-pL;'dK3J2").

Decidimos filtrar os pacotes enviados a partir do endereço 192.168.122.93:



Fizemos follow de cada pacote marcado a vermelho:

Para desencriptar mensagens dos 11 pacotes, criamos o ficheiro python auxiliar “shell1.py” através do “shell.py” e obtivemos os seguintes resultados:

Pacote	**Encriptado**	**Desencriptado**
60060	7uKGGrCFDsZhTxlSCtdDLtQC	b'ls’
60094	JROTcr+vnDcGKiRGt6x5CzWyF3fK4SSNrVBJnDb0	b'ls /home/chris’
60132	RFoloJlp1s0zjrV8qFEE+tz7wnEU0KFmeJkISJ09Khu041kXCk0=	b'ls /home/chris/Desktop’
60165	E2lRkF4pT6NX57fFK3vTh4wdO3mqyYTsUyWtjb+4EFWXrfVehhUVv1G8W8wEnv+t	b'ls /home/chris/Desktop/vacations’
60199	MzkSipvjAUgWzvo2YIL1H0ZgcPwctkKhTtYny8hLplfxKBlinag6yF6/hLeWKAEh	b'ls /home/chris/Desktop/topsecret’
60233	IDUF0OVUMJY0jkR3E/nSwsNzirGwHLrF8JQZrZ5k+6LypQ/PNr6Lq2t34TFTSBeCTBcBNblhHecA	b'ls /home/chris/Desktop/topsecret/moon1969’
60276	jRLBq+f8LMXh39nUZE2T8FzfMeRfKM36nfnrM3Ft+2/wg5MKoNKegjo58g78UjEzMFFzJHm7nRJAnbgeNwmDo+JTYuROwr4	b'download /home/chris/Desktop/topsecret/moon1969/Buzz.mov’
60681	0egWK1R2eDbKtYLIHIYa/gajE8vbAKo64fyjnN2M42YbFLkv4gQA+u+ZbUxfDGaRccvJZYG1NdqTA03irwtX24ic8E+FZAH4Li0=	b'download /home/chris/Desktop/topsecret/moon1969/Nevada.png’

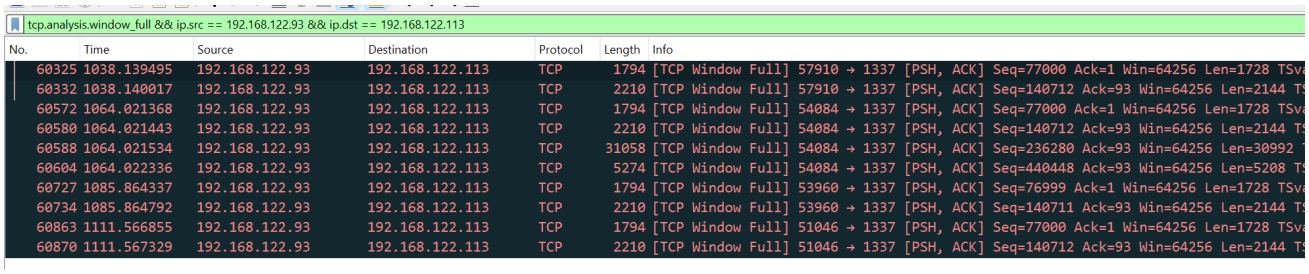
60790	CFvdkehoiacc0JTrxeelfY3OSOUk77gGcgsPWZtGMsZ2fDNMVcMtqldKXa/L2D0/IeYS748VOyh6nVQi6HeIdiJXJEF7ASk2JWiPNyjK	b'download /home/chris/Desktop/topsecret/moon1969/TOP_SECRET.pdf'
61020	lsoSf6AjPYrPmMxHk3neDHadf27hXoc5j1S0RcX1n+Zcw+K0r55RwIMw58a0tAb9FIHa+6ZapyE+HGKYqOsg5fkUw1aMjrYGXOygrQzkWQ==	b'download /home/chris/Desktop/topsecret/moon1969/Workmanship.png'
60173	zyi+SbG5mKI1lijv601N+84Lt4s=	b'quit'

Como os resultados destes comandos eram enviados de volta para o emissor sob a forma de um "index.aspx", fomos filtrar os pacotes marcados a azul na imagem acima (que correspondem aos resultados), sendo que 6 deles continham mensagens do tipo "cmd=" e 3 deles "file=". De seguida, foi criado um programa python auxiliar "cmd.py" que desencripta o conteudo dos ficheiros .aspx recebidos mostrando para o terminal no caso de um "cmd=" ou guardando para o disco no caso de um "file=":

Pacote	**Ficheiro**	**Encriptado ("file"s foram truncados)**	**Desencriptado**
60085	index.aspx	cmd=ZswjGthfqtLrhXX28gOFngrlnRUToGjI2Q==	shell.py
60123	index(1).aspx	cmd=OPAHLUMzhv7aDAwT0Esu4F6RWzltOrPSLmmjIdsNo9RRbSi9P3+e5yPyN8funWJm1WNijniOLuFBRCRLAFSgE0vW8qmf8aL++gREgTc2NJz9tvAJVrB3Dg==	Desktop Documents Downloads Music Pictures Public snap Templates Videos
60157	index(2).aspx	cmd=BQbz45waz5jfv3HHr/zDu1ndu1+7mAkItzIcHCtwRWr2875g8PsW8EvilxL/zYZNQbm4FQHFPb+UJ+73UfGTRBCDRsr8RHiylvaYsWB6xEpOBeYyChNh4e2LHLJplkhiamYATjkO	NASA_RESULTS_Q2 NASA_RESULTS_Q3 NASA_RESULTS_Q4 topsecret vacations wishlist.txt work
60190	index(3).aspx	cmd=134nr%2BC%2Bv8kLyf05beUF%2BGxJMBix6Tt4diounm21FamCtAXytXMFoyXyXKKPO6nOD92mMFfBQldM2O7zdnU12OExdAVpxq3CvGePKl7o0FP0UU%2FMnf%2BO%2FXSOGOE%3D	berlin2019 iceland 2021 lisbon2019 malasya202 maldives2022 pre2019_unsorted
60224	index(4).aspx	cmd=%2Bd5OYlRrRx2JLNG	monica

		mr6YIJNNoxYiURu93ouEPMAKVLDc%3D	moon1969
60268	index(5).aspx	cmd=YKsdxs7y%2FE5TXlQFZINKblQyBpsEwBb1%2FvshikV8ppipL12aoITKDkPjGL1ay0ldxsJ%2FldaKFrKMPgmxJaBg83Z7f5LwGqWsrnhXJxL5	Buzz.mov Letter.pdf Nevada.png TOP_SECRET.pdf Workmanship.png
60779	index(6).aspx	file=sn5137e0IvgeoWhi96XbpSXt2%2BFRObhpqfdXttVvxkDrXyBi8ayl6FNQY2WP71sDOHZhTaAPb%2B8xH2DV%2	Nevada.png
61010	index(7).aspx	file=xUSV34sNh7F533nACf1RwDYYVSB5htz4jODrDBhqH1TESXcvUOWFlRKc6Lu3BagtZT7CT	top_secret.pdf
61066	index(8).aspx	file=iP4PFAxstM7aLGoOyzfBxngPoatk2T4p8NFZlHMeIzUNlNkuofC1JurwJmqZsE4W84c%2Bm	worksmanship.pdf

Suspeitamos que havia outros dois ficheiros que não foram bem enviados, porque na pasta secrets do Christ constavam 5 ficheiros. Assim, depois de filtrarmos os pacotes com o filtro ip.src == 192.168.122.93 && ip.dst == 192.168.122.113, vemos que há pacotes TCP que estão marcados com "TCP WINDOW FULL". Filtramos então por esse tipo de pacotes (tcp.analysis.window_full && ip.src == 192.168.122.93 && ip.dst == 192.168.122.113):



Ao darmos follow da TCP stream do pacote 60325, exportarmos o resultado, ajustarmos o conteúdo (remover os headers HTTP e informações associadas que não é suposto estarem lá) e desencriptar como no passo anterior, obtivemos uma versão corrompida do video "BuzzAldrin.mov".

Ao repetir o mesmo processo para o pacote 60574, obtivemos o ficheiro "letter-corrompida.pdf".

TCP stream	Conteúdo	Resultado
7137	file=7s7B6%2B5	BuzzAldrin-corrompido.mov
7141	file=csNhxmej3zmPL3Gr3HNIhuuYX24G4W3KHZ3dIY4yN6Y%2B5Sqci	letter-corrompida.pdf

Com isto, deduzimos que ambos os ficheiros corrompidos tenham sido transferidos na íntegra para o computador de Meghan, dado que os tinha na sua posse, no entanto, o wireshark não foi capaz de capturar bem os pacotes em trânsito de forma a poder-se extrair um ficheiro idêntico.

Assim, ficamos com as seguintes chaves:

Ficheiros Lab 2	Valor SHA-256 Lab 2	Ficheiros Lab 3	Valor SHA-256 Lab 3
Nevada.png	4ec286d1b6fbb9466d1f68dcdd6d248441645be85be6f4bf0365f068060486da	Nevada.png	4ec286d1b6fbb9466d1f68dcdd6d248441645be85be6f4bf0365f068060486da
BuzzAldrin.mov	bc8a2d12aa1e8f280294a7b413612e739927b789181c826c30cbe2b460513480	BuzzAldrin-corrompido.mov	4830847db9fcdce785a45d9fb4dfa1a205e049f224a6253eb6d0a87bda654478
top_secret.pdf	73a6b01845a1365e3f9a6f48fdf93651f0efc07575ce1a89c5f32e01babf20ec	top_secret.pdf	73a6b01845a1365e3f9a6f48fdf93651f0efc07575ce1a89c5f32e01babf20ec
worksmanship.pdf	d330090e25b709aa1a9cdb28d60b103218aeeb470ecaa2df461157297a4a6444	worksmanship.pdf	d330090e25b709aa1a9cdb28d60b103218aeeb470ecaa2df461157297a4a6444
letter.pdf	631fb4c4aadc6ca3f46310466974c85d9ab226e6617096eb0206a22b6fbd5872	letter-corrompida.pdf	1c5d45ac6112575c1436e4980a357c4749ac9a11f47ec7ac5f10418fac48c92b

2 What can you tell about the identity of the person(s) responsible for leaking the secrets?

Foi a Meghan de acordo com o IP, a usar o email da Mónica para o Chris. Ao analisarmos os pacotes relativos às trocas de mail entre a Mónica e o Chris verificámos que o IP do computador de onde estavam a ser enviados os mails da Mónica era o computador da Meghan, por isso supomos que deva ter acedido ao mail da Mónica e enviado os mails. Neste mails encontramos uma conversa iniciada pela suposta Mónica para o Chris sobre o quanto gostou das férias juntos ao qual o Chris responde que deviam repetir nas férias visto que a Meghan vai estar fora da cidade. Meghan, ao passar-se por Mónica, responde que já começou a ver hotéis e manda-lhe uma imagem de um dos que encontrou. Nesta imagem acreditamos que pudesse estar um vírus que ao ser aberto por Chris no seu computador fez com que fossem enviadas as provas da falsificação da chegada à Lua para o computador da Meghan.

Existe depois uma troca de mails entre o Chris e uma entidade chamada real.life.trinity@protonmail.com a qual acreditamos ser a Meghan. A entidade real.life.trinity começa por mandar uma mail ao Chris a afirmar que sabem que a chegada à lua em 1969 foi falsificada e que o Chris tem desde aquele momento 12 horas para transferir 5 milhões de dólares em Bitcoin para o endereço que está no mail. Se ele não fizer a transferência ela irá fazer com que o resto do mundo saiba o que realmente aconteceu. Isto não é levado muito a sério pelo Chris que pela resposta percebemos que já costuma receber imensos mails de extorsão e então não acredita que este possa ser verdadeiro. Ela responde com um excerto da carta deixada a Chris pelo seu avô Richard Nixon - “Finally, I entrust you with my biggest secret as I feel i won't be able to rest in peace if I take this secret with me to the grave” - e

afirma que Chris deve reconhecer estas palavras. Isto provoca uma mudança de atitude do Chris que responde de uma maneira mais defensiva a dizer que a pessoa não deve estar a perceber com quem está a falar e sugere-lhe desistir de qualquer que seja o plano que tem. Segue abaixo todos os mails trocados.

Pacote	IP	From	To	Conteúdo
15786	192.168.122.113	"Monica Sky" monica.l.sky@mail.com	"Chris Cox" chris.nixon.cox@mail.com	Hi Chris!! Just letting you know that our little vacation was amazing. We really got to do it again XO. Monica
24340	192.168.122.93	"Chris Cox" chris.nixon.cox@mail.com	"Monica Sky" monica.l.sky@mail.com	It was really something wasn't it? I was thinking we could run it back this holiday season. Megan will be out of town for a cyber security conference after Xmas. I heard the weather in Cancun is great all year round.
47742	192.168.122.113	"Monica Sky" monica.l.sky@mail.com	"Chris Cox" chris.nixon.cox@mail.com	Warm weather in the winter!? sounds perfect! I already started to look into hotels. What do you think about this resort in the image?
		"real.life.trinity" real.life.trinity@protonmail.com	"Chris Cox" chris.nixon.cox@mail.com	We know. Greatings Mr.Cox, From this very moment you have exactly 12 hours to transfer 5 million USD in Bitcoin to the address 12Zy8YnQ5rWujPAKGimiQTyw7DRJnkWECT. We are aware that your main Bitcoin address is 1FPyLC1sK1jctnjgHiTSvUjaLsiWCqFZMQ therefore you can comfortably afford it. If the transfer is not done by the aforementioned

				deadline we will make sure the entire world knows that the United States of America never landed a man on the moon in 69.
69855	192.168.122.93	"Chris Cox" chris.nixon.cox@mail.com	"real.life.trinity" real.life.trinity@protonmail.com	If I had a dollar for every extortion email I received I would give 5 million right now... I commend you for the effort but surely you can do better than the moon landing ahahah.
		"real.life.trinity" real.life.trinity@protonmail.com	"Chris Cox" chris.nixon.cox@mail.com	We know. "Finally, I entrust you with my biggest secret as I feel i won't be able to rest in peace if I take this secret with me to the grave" Surely you recognize these words. Great men always carry the biggest secrets.
76371	192.168.122.93	"Chris Cox" chris.nixon.cox@mail.com	"real.life.trinity" real.life.trinity@protonmail.com	Listen, I don't think you understand with who you are talking to. I suggest you give up on whatever plan you have while still let you.

3 Can you establish a timeline of all relevant events that clarifies how the entire data exfiltration has taken place and the secrets ended up in Carl Seagal's computers?

Timeline de emails

- **22/10/22 10:49** - Primeiro mail enviado da Meghan com o mail da Mónica para o Chris sobre as suas férias
- **22/10/22 10:56** - Meghan envia mail para o Chris que contém o malware que vai enviar os ficheiros para o computador da Meghan

- **22/10/22 11:07** - Um indivíduo, que suspeitamos ser Meghan, com o mail real.life.trinity@protonmail.com envia ao Chris um mail fazendo chantagem com ele
- **22/10/22 12:07** - Meghan envia ao Chris provas de que tem evidências que mostram a falsificação da chegada à lua

Timeline da conversa com Car Seagal e a entrega da pen

- **26/10/22 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.
- **28/10/22 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.
- **28/10/22 15:21 até 15:48 -** Pen recebida por Carl.
- **28/10/22 15:27:02 -** Pen inserida no computador de Carl.
- **28/10/22 15:28:17 -** Pen removida do computador de Carl
- **28/10/22 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.

4 From all the collected evidence in this investigation, what can you deduce about the motivation of the actor(s) responsible for the data exfiltration?

Meghan faz exfiltração dos dados pois acredita que o seu marido Chris está a traí-la com a sua secretária, Mónica. Há várias evidências para suportar esta teoria:

- **Pacote 2190:** Mónica pesquisa sobre ser normal trabalhar aos sábados (https://www.google.com/search?channel=fs&client=ubuntu&q=why+is+it+normal+to+work+on+saturdays)
- **Pacote 4975:** Chris pesquisa no website quora o tópico "How can one hide an extramarital affair"´(https://www.quora.com/How-can-one-hide-an-extramarital-affair).
- **Pacote 6342:** Meghan pesquisa sobre ter encontrado um nome do telemóvel do marido (https://www.google.com/search?channel=fs&client=ubuntu&q=found+name+on+husband+phone)
- **Pacote 7906:** Meghan pesquisa sobre o marido ir em muitas viagens com a secretária (https://www.google.com/search?channel=fs&client=ubuntu&q=partner+goes+on+many+business+trips+with+assistant)
- **Pacote 7908:** Meghan acede ao website https://www.survivedivorce.com
- **Pacote 8056:** Meghan lê um artigo sobre sinais de que o marido está a trair (https://www.survivedivorce.com/cheating-husband-signs)
- **Pacote 20625:** Mónica pesquisa sobre formas de desperdiçar tempo no trabalho, o que pode indicar que não tem muito para fazer no trabalho. Assim, em contraste pela sua pesquisa no pacote 2190, podemos concluir de que não tem razões para trabalhar ao sábado e de que é uma farsa (https://www.quora.com/What-are-your-favourite-ways-of-wasting-time-at-work)
- **Pacote 30062:** Meghan pesquisa sobre formas de se vingar do marido (https://www.quora.com/What-are-some-ideas-to-safely-get-revenge-on-a-cheater-husband)

Para além disto, depois das trocas de emails entre Meghan a fazer-se passar por Mónica e Chris, Meghan confirma que os outros dois estão a ter um caso.

Como nota final, no wireshark também foi apanhada uma captura no site “twitter” que confirma que Meghan é filha de Raymond Polanski. Ora, como não foi encontrada a foto do astronauta no computador de Chris e a foto tinha as iniciais de Raymond, é possível que este tenha ajudado a filha a forjar a prova numa situação de solidariedade e apoio paterno ao ver a traição do genro e por isso, também deve ser algo de investigação.

SHA-256:

Ficheiro	SHA-256
cmd.py	4dc9a183360b8a5c9419a1670b96f9743f1e45b415d406a3b84e8230ea29e879
shell1.py	b6ba6ad8193e4fa1ceac21b9a1278e40905d5fee2510f5ee7393d7ac304f2890
maldives-video.zip	e8784f454e9c55ce49f8e6cb1ef5410f78bf8159243de2773d6331c6448eba20
index.aspx	d0e0da1ef6dff4fdf18769213a7a57144c8ffecb4cefb6b7b5c0f28dabb78246
index(1).aspx	f66177abd4dac49b286c73edafebce526dc5d57eb359ca618690539d25bf1a53
index(2).aspx	8f724833bcfa38e4dd806e0262ad80ae802a8bac1d6abfd05c746c922ba58baa
index(3).aspx	3e67ce0bf6bc7b1d49b620d08e6f79bbe460b15d2ae90f45ac53b9c124924681
index(4).aspx	b03c0a9436897a001c54c72473eef2a8bf5c20d60245cc49f0f294818636acc2
index(5).aspx	fde62e533267c01c09ed18020ae742dbdcce74d118852e2491e12473398c7566
index(6).aspx	8c6121327b3b08e692a4628d8987c00c417ed96be57496e1ac522cde2f5de4c3
index(7).aspx	1f5c879b85022f025212158f6357067908972262310e3e2a88caa4818a075a4c
index(8).aspx	9d64fae5a61d939cf09cea3042fcb3b97da70fcd7004b4f538a2b47ea9def079
Nevada.png	4ec286d1b6fbb9466d1f68dcdd6d248441645be85be6f4bf0365f068060486da
TOP_SECRET.pdf	73a6b01845a1365e3f9a6f48fdf93651f0efc07575ce1a89c5f32e01babf20ec
worksmanship.pdf	d330090e25b709aa1a9cdb28d60b103218aeeb470ec

	aa2df461157297a4a6444
BuzzAldrin-corrompido.mov	4830847db9fcdce785a45d9fb4dfa1a205e049f224a6253eb6d0a87bda654478
index.aspx	f1ae226f1ec166d441daa939aee87dafba813cc971f90079ca1a3d52f10676c0
index.aspx ajustado	0da9242618f458ba3be7fc3b12933f7184525f7b6b2d7f4f12e19743d23d82a0
letter-corrompida.pdf	1c5d45ac6112575c1436e4980a357c4749ac9a11f47ec7ac5f10418fac48c92b
index.aspx ajustado	84d363c2b2c377f7403d36d80e1544fb50a58ce8bee80d946e1c9a2c520d4c9b
index.aspx	199cc77659bf7c6b0d88096832d8c505db94b8e81e3198968c2e76e50abdab83