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 Did you find any traces of relevant documents that Prof. Seagal is probably relying on to support this claims? Present your findings explaining how you retrieved said documents.

Foram encontradas 6 evidências relacionadas com a alegação do Prof.Seagal de que teria na sua posse informações sobre a NASA.

Em primeiro lugar, vimos que na imagem "Dog.png" havia bandas no céu, o que nos fazia suspeitar do uso do uso do algoritmo LSB. Para extrair possível informação da imagem, recorremos à ferramenta zsteg (https://github.com/zed-0xff/zsteg) e corremos o comando "zsteg -a Dog.png", que testa as várias combinações do algoritmo LSB e enumera os dados extraídos. Percebemos que com a combinação "b6,g,lsb,xy" (lsb-6, pixeis a verde, na direção xy, ou seja, por linhas) estávamos na presença de um jpeg, por isso extraímos o ficheiro com o comando "zsteg -E b6,g,lsb,xy Dog.png > DogOut.jpeg". O ficheiro encontrado continha uma foto do astronauta a aterrar na lua, a informar que foi tirada com uma Polaroid em Nevada.

De seguida, suspeitando de mais imagens com informação escondida pelo algoritmo LSB e visto que o zsteg funciona apenas para .png e para .bpm, usamos esta ferramenta para analisar o "MIT.png", "Blackstone.png" e "Schedule.png" (corremos os comandos "zsteg -a MIT.png", "zsteg -a "Blackstone.png", "zsteg -a Schedule.png"). Apenas encontramos outro ficheiro escondido no "Schedule.png", uma imagem png, com a combinação "b6,r,lsb,xy" (lsb-6, pixeis a vermelho, na direção xy). Extraímos com o comando "zsteg -E b6,r,lsb,xy Schedule.png > ScheduleOut.png" e na imagem, encontramos um texto que relata a má qualidade prestada pelos empregadores da NASA, e como na opinião do autor do texto, é inconcebível que terão chegado à Lua com trabalhadores assim.

Em terceiro lugar, para o ficheiro Corrupted.pdf começamos por o tentar abrir mas não conseguimos e decidimos verificar os magic numbers fazendo hexdump Corrupted.pdf. Com isto obtivemos 61 48 52 30 63 que não correspondiam aos magic numbers da extensão pdf (25 50 44 46 2D). Tentámos mudar estes 5 bytes e abrir o pdf novamente mas pareceu continuar corrompido. Verificámos também se os magic numbers indicados no hexdump correspondiam a outro tipo de ficheiro conhecido, e tentamos substituí-los, mas sem sucesso. Ao utilizar o comando strings no ficheiro Corrupted.pdf verificámos que este parecia estar codificado em base64 devido aos caracteres presentes e aos dois últimos símbolos '=='. Assim, decodificamos o seu conteúdo ("base64 -d Corrupted.pdf") obtendo um conjunto de caracteres não imprimíveis. No entanto, na primeira linha do texto decodificado estava conteúdo legível que parecia ser um link. Ao pesquisar por esse link no browser reparámos que ia dar ao um ficheiro "tools.pyc" na dropbox e fizemos o seu download. Fazendo o comando "file tool.pyc" apercebemos-nos que era um ficheiro python 3.7 byte-compiled. Para descompilar este ficheiro, usámos uma ferramente chamada decompile3 (https://github.com/rocky/python-decompile3) e ao correr o comando "decompyle3 tool.pyc > tool.py" obtivemos um script em python. Este script ao correr perguntava ao utilizador se queria encriptar (e) ou desencriptar (d) o qual escolhemos d, o nome de um ficheiro que assumimos ser o Corrupted.pdf e uma password que ainda não sabíamos a este ponto. Ao analisar melhor o script percebemos que este utilizava o algoritmo sha512 para encriptar a password fornecida e caso este hash seja igual a um definido no programa conseguimos desencriptar o conteúdo do pdf. Como não tínhamos nenhuma indicação do que a password pudesse ser, e como apenas usar brute force iria ser dispendioso em termos de tempo, decidimos recorrer a um ataque de dicionário. Assim criamos um ficheiro com todas as passwords possíveis. Esta incluía as palavras do ficheiro TCOS.txt e a letra da música "Ice". Para facilitar este processo, fizemos um script em python, "prepare_dictionary.py", para que a partir do ficheiro das letras da música ("IceLyrics.txt") e do ficheiro TCOS.txt, extraísse as palavras uma a uma por cada linha e eliminasse as repetidas. A partir disso ficamos com o ficheiro "Results.txt". Para além disso, acrescentamos palavras-chave presentes nas imagens presentes em ambas as pastas, tais como "Tom", "Brady", "12", o nome das equipas, a pontuação do touchdown, entre outras, criando o ficheiro "Results+.txt". De seguida realizamos um ataque dicionário, fizemos uma cópia do código tool ("toolFile.py") para que em vez de uma palavra, recebesse um ficheiro com palavras e que verificasse qual delas era a correta. Com isto obtivemos a palavra "poisonous" e correndo o programa "tool.py" com esta password obtemos o ficheiro Corrupted.pdf _dec que pelos magic numbers percebemos que era também um pdf. Ao mudar a extensão obtivemos uma carta.

Analisamos depois o ficheiro Golf que não tinha extensão. Começamos por verificar se os seus magic numbers coincidiam com alguma extensão conhecida mas sem sucesso. Ao utilizar a ferramenta binwalk (https://github.com/ReFirmLabs/binwalk) neste

ficheiro (“binwalk Golf”) percebemos que este tinha 6 ficheiros .jpeg lá dentro. Assim extraímos o seu conteúdo (“binwalk -e Golf”) obtendo a pasta “output/”. Lá dentro encontravam-se então as 6 imagens .jpeg que ao abrir pareciam ser partes de uma só imagem. Tentámos então juntar as 6 usando a ferramenta Adobe Illustrator e obtivemos uma carta Top Secret… (“Untitled-1.png”).

Analisando agora o ficheiro Relativity.gif com a ferramenta binwalk usando o seguinte comando “binwalk Relativity.gif”, observamos que é detectado um ficheiro .zip que contém uma imagem chamada “Nevada.png”. Como primeira tentativa, utilizamos o comando “binwalk -e Relativity.gif”, mas sem sucesso (a imagem aparece distorcida). Seguidamente, usamos os comandos “strings Relativity.gif” e “hexeditor Relativity.gif” que voltaram a confirmar a existência de um artefacto embebido no gif por conter o nome “Nevada.png”. De forma a tentar descobrir onde se encontrava e extraí-lo, decidimos analisar os headers do ficheiro Relativity.gif usando a ferramenta “exiftool” que ao utilizar o comando “exiftool Relativity.gif”, denunciou imediatamente a presença do artefacto nos headers do ficheiro. Para finalmente o extrair, foi utilizado o comando “exiftool -b Relativity.gif > file.zip && unzip file.zip” para extrair o quinto artefacto “Nevada.png”.

Por fim, ao utilizar o comando “binwalk Sports.zip” no ficheiro Sports.zip verificamos que este continha um ficheiro “BuzzAldrin.mov” que, ao correr o comando ”unzip Sports.zip”, não era realmente extraído como os restantes. De seguida, foi usado o comando “binwalk -e Sports.zip” de modo a extraí-lo, porém sem sucesso. Com o objetivo de o conseguir extrair, foi utilizada uma coleção de ferramentas chamada “stego-toolkit” (https://github.com/DominicBreuker/stego-toolkit) que permitiu utilizar, de novo o comando “binwalk -e Sports.zip” mas desta vez, com sucesso e extraindo assim, o ultimo artefacto “BuzzAldrin.mov”.

File	SHA-256 Value
DogOut.png	4d10bcbe31a17c866b305750685d87878bb58fa68dc934440b528f9796642a65
ScheduleOut.png	4bfd97afe8a1d510e84a52094d888bc8907f643f5793b6d259260505d33920f4
Corrupted_dec.pdf	631fb4c4aadc6ca3f46310466974c85d9ab226e6617096eb0206a22b6fbd5872
Untitled-1.pdf	d758892d11207b7ca51b3ee08df7238d2

	d07b1499c0c594c14fda0c66a3b86c9
Nevada.png	4ec286d1b6fbb9466d1f68dcdd6d24844 1645be85be6f4bf0365f068060486da
BuzzAldrin.mov	bc8a2d12aa1e8f280294a7b413612e739 927b789181c826c30cbe2b460513480

2 If you found any relevant documents, do they support Prof. Seagal's thesis that NASA's moon landing was fake? Based on these documents, suggest how Prof. Seagal explains how the moon landing event occurred and why these documents constitute ``irrefutable evidence''.

A partir dos documentos, encontramos 6 evidências relacionadas com o caso.

O primeiro ficheiro encontrado, “DogOut.jpeg” é um ficheiro que contém uma imagem de um astronauta na Lua, com a descrição a relatar que a foto tinha sido tirada com uma câmera polaroid na sede da NASA em Nevada. O autor do ficheiro intitulou-se como R.P, que, através do cruzamento de outras evidências, supomos que é o Raymond Polanski.

O segundo ficheiro “Schedule.png” é uma imagem cujo texto é uma crítica aos trabalhadores da NASA, e cujo último parágrafo evidencia a sua dúvida quanto à chegada à Lua.

O terceiro ficheiro “Corrupted_dec.pdf” é uma carta escrita pelo presidente dos Estados Unidos Richard Nixon ao seu neto Christopher que a iria ler depois do seu avô morrer. Richard dá-lhe conselhos para a sua vida e diz ter-lhe deixado 60.000 dólares no testamento para o ajudar e para os usar de forma sábia. Finalmente, revela um segredo que iria ter grandes consequências para o mundo e que não consegue levar sozinho para a campa. Conta-lhe então da falsificação da aterragem à Lua em 1969 tendo este dado ordens para que esta ocorresse no deserto do Nevada. Diz que sabe que o que fez foi errado mas que o fez pelo bem do país. No fim diz ao neto para queimar a carta e não deixar nenhum traço desta para trás.

O quarto ficheiro “Untitled-1.pdf” continha um documento Top Secret que descrevia o problema dos Estados Unidos estarem a perder a corrida espacial contra a União Soviética e que a possível vitória apenas aconteceria se os Estados Unidos puserem os pés na lua. No entanto, nesse documento afirmam que só daqui a pelo menos 5 anos é que terão a tecnologia suficiente para o fazer. Assim, Washington aprovou a filmagem da falsa filmagem da Lua e que esta ocorresse em Nevada e dirigida por Raymond

Polanski em colaboração com peritos da NASA. Este documento revela ainda que qualquer uso destas filmagens requer a autorização do presidente Richard Nixon.

O quinto ficheiro “Nevada.png” é uma imagem com um mapa de Nevada onde alegadamente foi filmada a falsa aterragem a lua em “Nevada Filming Facility"

O sexto ficheiro “BuzzAldrin.mov” é um vídeo do Buzz Aldrin a dizer “Scariest? It didn’t happen. It could have been scary…”.

Após a análise das evidências, não podemos afirmar que estas apresentam provas irrefutáveis, pois não temos certeza de que são autênticas, nem que temos toda a informação para concluir tal. No entanto, à luz da hipótese do Prof. Seagal, elas podem apoiar a sua teoria.

Segundo esta, a chegada à Lua foi na verdade uma filmagem realizada na sede da NASA em Nevada, aprovada pelo presidente dos Estados Unidos Richard Nixon, e dirigida por Raymond Polanski. As provas referenciam-los e também a um astronauta, Buzz Aldrin que foi o segundo homem a pisar a lua.

3 From the analysis of all provided artifacts, what else have you learned? Present additional insights that you may have gained, e.g., about other involved stakeholders.

Neste caso, existem vários stakeholders, nomeadamente:

- Richard Nixon
- Christopher Cox (neto do Richard Nixon)
- Buzz Aldrin
- Raymond Polanski

Pela análise crítica dos documentos, encontramos o vídeo original da sexta evidência (https://www.youtube.com/watch?v=HV_bD3xQG9Y). Trata-se de uma entrevista do Buzz Aldrin, e a evidência foi retirada do excerto a partir do minuto 30:32, à qual ele responde à pergunta “Qual foi a parte mais assustadora da viagem?”, dizendo inicialmente “Scariest? It didn’t happen. It could have been scared…", e de seguida relata como uma falha técnica poderia causar problemas na aterragem. A partir disto, podemos concluir que o excerto foi retirado do vídeo sem o seu devido contexto.

Para além disso, após consulta sobre o manual da Polaroid 350 (https://www.polaroid-passion.com/manuel/manuel-polaroid-350.pdf), a última página é referido que para tirar uma foto com luz, esta deve estar de trás ou de lado. No entanto, ao ver a imagem “DogOut.jpeg”, vemos que pela sombra do astronauta, a

luz está por trás, contrariando a informação do manual. Isso levanta dúvidas sobre a autenticidade sobre a informação de que foi retirada pela Polaroid 350. Ainda em relação à foto, visto que pelas iniciais seja mais provável Raymond Polanski que tenha assinado, podemos suspeitar que ele tenha falsificado esta informação ou, como não se trata de uma assinatura, podemos suspeitar que outra pessoa tenha falsificado em nome dele.

4 Based on your findings, suggest the next steps you would take to pursue this investigation.

Tendo em conta que a autenticidade (ou falta dela) dos documentos que foram encontrados, de modo a perceber se a afirmação do professor Seagal tem fundamento, o próximo passo da investigação deveria ser chegar a uma conclusão em relação a este assunto.

Para tal, um dos primeiros objetivos seria procurar a câmera Polaroid Land modelo 350 com que foi tirada a foto e tentar replicar a mesma no suposto local de filmagens marcado pela foto para verificar a posição da sombra do astronauta. O segundo passo, passaria por uma análise à caligrafia da carta de Nixon ao seu neto para comprovar que foi escrita pelo próprio e não foi forjada.

Seguidamente, o terceiro passo seria a procura e subsequente investigação do local de armazenamento das filmagens referenciado no artefacto “Untitled-1.pdf” como “undisclosed location” de modo a averiguar a existência de tais filmagens.

Como nota final, este caso em específico, tem uma dificuldade acrescida porque antes dos astronautas irem (ou não) à Lua, foram realizados inúmeros testes de preparação (tanto por astraunatas como por engenheiros) para a aterragem na lua no deserto do Nevada (https://st.llnl.gov/news/look-back/apollo-astronauts-train-nevada-test-site), o que torna complicado distinguir e separar o que possa ter sido um teste e a real encenação da ida à lua por parte da NASA. Com isto, é sugerida precaução e atenção a este detalhe durante as restantes investigações.