

Task 2

Análise de captura de pacotes.



Introdução

A ideia é analisar os pacotes em uma ferramenta gratuita chamada WireShark, ao conseguir analisar, devem ser coletados metadados para conversão em outra ferramenta gratuita chamada HxD, a qual converte os metadados em um arquivo legível.

Esse relatório apresentará resultados de análises de metadados que foram encontrados no arquivo de formato pcap, essa análise foi subdividida em 8 partes, chamadas sub-tasks. Cada sub-task mostrará o código e o arquivo ao qual resulta do código.

Por fim, o objetivo é trazer esclarecimento sobre o que é transportado ao navegar na internet e o que o computador do usuário absorve desse transporte.

Task 2

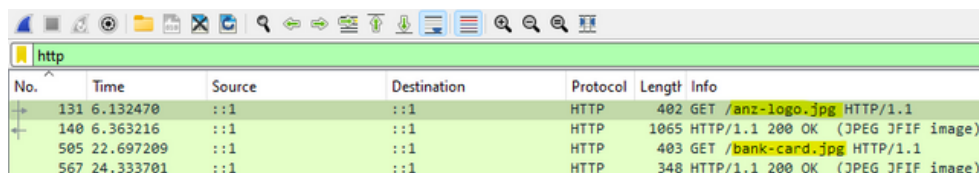
Análise de captura de pacotes.



Sub-Tasks

Primeira sub-task

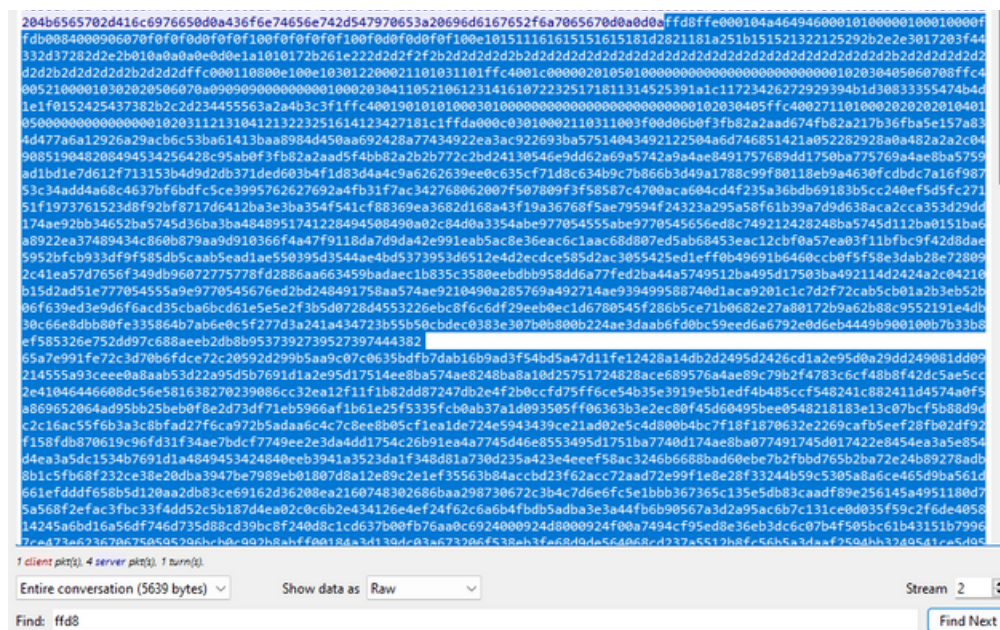
Nessa primeira análise, serão observados dois arquivos de transferência do arquivo pcap, conforme mostra a figura a seguir.



No.	Time	Source	Destination	Protocol	Length	Info
131	6.132470	:::1	:::1	HTTP	402	GET /anz-logo.jpg HTTP/1.1
140	6.363216	:::1	:::1	HTTP	1065	HTTP/1.1 200 OK (JPEG JFIF image)
505	22.697209	:::1	:::1	HTTP	403	GET /bank-card.jpg HTTP/1.1
567	24.333701	:::1	:::1	HTTP	348	HTTP/1.1 200 OK (JPEG JFIF image)

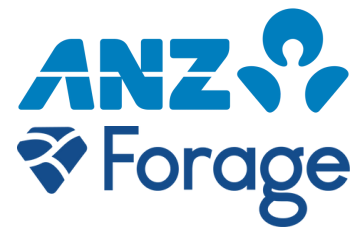
A primeira análise partirá do anz-logo.jpg, entrando em suas configurações em *Follow/TCP Stream*, abrirá uma janela com metadados em *Raw*, a partir dessa imagem, é necessário selecionar os metadados entre *ffd8* até o *ffd9*, como mostra a imagem a seguir.

Nessa primeira análise, serão observados dois arquivos de transferência do arquivo pcap, conforme mostra a figura a seguir.



Task 2

Análise de captura de pacotes.



Após selecionar esse intervalo *Raw*, é necessário copiá-lo e colá-lo no programa *HxD*. Ao colar no programa, será apenas necessário salvar para poder obter um arquivo legível ao dispositivo, como nesse primeiro caso, o *anz-logo* será convertido como um arquivo *jpg* e será visualizado como uma imagem. Como mostrado na figura a seguir.

```
Sem Título1.
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Texto decodificado.
00001260 7C 52 B6 09 29 A7 9A 3F 05 25 83 C4 70 B2 32 E0 |Rt.)$s?.tfAp*2A
00001270 0D ED 71 BB 25 6B A3 3A 71 88 61 B1 BE 2A 49 5A .iq=kkE:q'as*IZ
00001280 D8 DE FF 00 08 59 24 4D 90 07 D8 02 45 F6 5C 01 0Py..YGM..Q.Eo\
00001290 E8 52 31 CF AE 89 C9 5F 6D BD 50 85 E7 0F 75 DC eRI0nE_mhP.q.uU
000012A0 6B CE C1 F5 56 23 DD 73 1A F3 D0 7D 55 8B 1F 8A kIA0V#Ys.6D)Ux.š
000012B0 CC FE SA BD 1E 85 E7 0F 75 CC 67 CE C1 F5 56 23 Ip2%...q.uigIA0V#
000012C0 DD 73 19 F3 B0 7D 55 89 F1 59 3E 5A AC F9 5A 3F Ys.6*)UhAY>2-0Z?
000012D0 D3 78 8F CA 83 F5 78 D6 A4 AE 71 5C 46 6A A9 E5 0x.Ef0x0=0q\Fj0A
000012E0 A9 9D DA F3 4C ED 67 BA C0 5C D8 01 60 36 00 00 0.U0Lig*À0.'6..
000012F0 1D CA D6 EB A6 B1 A8 72 DA 77 3B 49 0A 28 55 12 .È0e;=rUw:I.(U
00001300 42 8A 10 49 09 5D 08 84 4A 10 52 55 4D 09 21 45 Bš.I.)...J.RUM.!E
00001310 34 24 84 43 42 57 42 80 42 10 8A 12 4D 08 12 13 4s.CBN0EB.S.M...
00001320 42 04 84 D0 81 21 34 20 10 84 20 61 09 21 10 D0 B..D.!4 .. a.!D
00001330 84 20 10 92 15 53 42 48 40 D0 92 13 68 0A 12 42 ..'.SBH0D'.h..B
00001340 8A 68 49 08 1A 12 42 01 08 42 06 84 90 81 A1 24 ŠhI...B..B...i$
00001350 22 84 21 08 04 21 08 1A 12 42 06 84 90 81 A4 84 "!!...!...B...h..
00001360 22 04 D2 42 06 84 90 81 A1 24 20 68 49 0A 81 08 ".0B...;š hi...
00001370 42 80 42 10 80 42 10 80 42 10 80 42 48 40 D0 84 B0B.0B.0B.0B0D..
00001380 22 84 21 08 04 21 08 04 21 08 04 90 84 0C 21 08 "!!...!...!...!..
00001390 44 08 42 10 08 42 10 08 42 10 08 42 10 7F FF D9 D.B..B..B..B..y0]
```

Com isso obtém-se o arquivo *anz-logo.jpg* e é visualizado conforme a figura abaixo:



Task 2

Análise de captura de pacotes.



Agora faremos o mesmo processo com o *bank-card*, partindo direto do *Follow/TCP Stream*, copiando o intervalo *ffd8* à *ffd9*, colando no *HxD* e salvando como *bank-card.jpg*, visualizamos a seguinte imagem:



Segunda sub-task

O processo de obtenção será o mesmo, pois como o primeiro tópico, ambos os arquivos são duas imagens e passam pelas mesmas etapas.

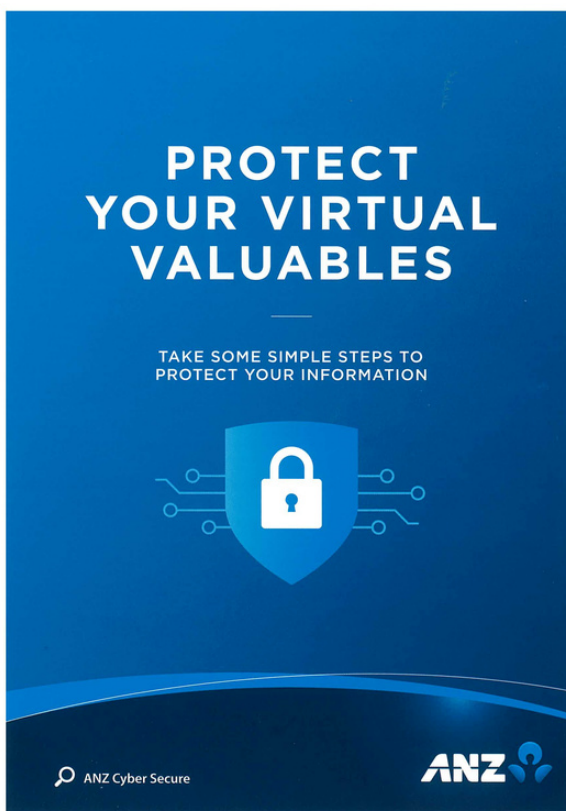
3683	119.921382	::1	::1	HTTP	398	GET /ANZ1.jpg HTTP/1.1
3861	122.973950	::1	::1	HTTP	1471	HTTP/1.1 200 OK (JPEG JFIF image)
4074	132.661962	::1	::1	HTTP	398	GET /ANZ2.jpg HTTP/1.1
4277	135.366278	::1	::1	HTTP	282	HTTP/1.1 200 OK (JPEG JFIF image)

Task 2

Análise de captura de pacotes.



Portanto, após obter os intervalos *ffd8* e *ffd9* de cada *TCP Stream*, colar no *HxD* e salvar como arquivo legível ao usuário, seguirá abaixo o resultado de cada, seguindo a ordem de *ANZ1.jpg* e *ANZ2.jpg*.



ANZ1.jpg

MAKE A 'PACT' TO PROTECT YOUR VIRTUAL VALUABLES



PAUSE
before sharing your
personal information

Ask yourself, do I really need to give my information to this website or this person? If it doesn't feel right, don't share it.



ACTIVATE
two layers of security with
two-factor authentication

Use two-factor authentication for an extra layer of security to keep your personal information safe.



CALL OUT
suspicious messages

Be aware of current scams. If an email, call or SMS seems unusual, check it through official contact points or report it.



TURN ON
automatic
software updates

Set your software, operating system and apps to auto update to make sure you get the latest security features.

Report suspicious messages from ANZ:

Email hoax@cybersecurity.anz.com

Report fraudulent or unusual ANZ account activity:

137 028 / +61 3 8693 7153 (Corporate/Business Clients)

133 350 / +61 3 9683 8833 (Personal Banking Customers)

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Item No. 961848 09/2018 AU22349

ANZ2.jpg

Task 2

Análise de captura de pacotes.



Terceira sub-task

No caso desse arquivo, o *WireShark* bloqueou o seu conteúdo devido ser malicioso. A figura abaixo mostra o protocolo.

1051	46.737160	::1	::1	HTTP	389 GET /how-to-commit-crimes.docx HTTP/1.1
1077	47.744581	::1	::1	HTTP	488 HTTP/1.1 200 OK (application/vnd.openxm

Nesse caso, será necessário ir em *Follow/TCP Stream*, porém, diferente dos demais que analisamos no formato *Raw*, nesse caso em especial, irá ser necessário analisar os dados em *ASCII*, e por isso, pode-se identificar que o arquivo é malicioso, conforme mostra a figura abaixo.

```
GET /how-to-commit-crimes.docx HTTP/1.1
Host: localhost:8000
Connection: keep-alive
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Fri, 16 Aug 2019 00:48:17 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Mon, 05 Aug 2019 02:23:32 GMT
ETag: "46-58f5564f85059"
Accept-Ranges: bytes
Content-Length: 70
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document

Step 1: Find target
Step 2: Hack them

This is a suspicious document.
```


Task 2

Análise de captura de pacotes.

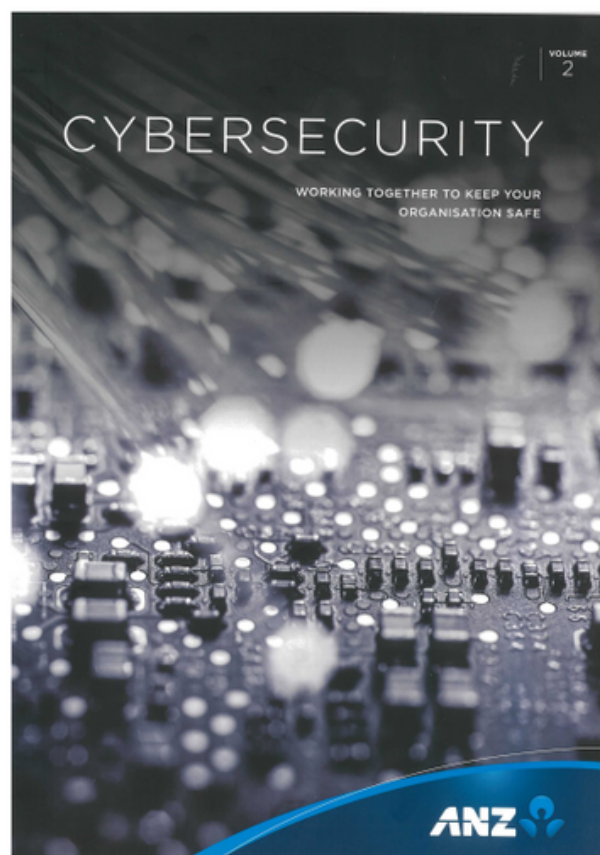


Quarta sub-task

Outro procedimento será feito a partir daqui, indo para /Follow/TCP Stream, ao invés de selecionar a visualização em ASCII ou Raw, agora partirá em analisar por meio de HexDump. A figura abaixo mostra os arquivos ANZ_Document, ANZ_Document2 e o evil.

2085	89.620153	::1	::1	HTTP	617	GET /ANZ_Document.pdf HTTP/1.1
2537	97.648691	::1	::1	HTTP	1284	HTTP/1.1 200 OK (application/pdf)
2662	103.007294	::1	::1	HTTP	618	GET /ANZ_Document2.pdf HTTP/1.1
3522	112.142837	::1	::1	HTTP	744	HTTP/1.1 200 OK (application/pdf)

Investigando a *ANZ_Document* e extraíndo seu *HexDump*, agora a ideia é colocá-lo no *CyberChef* e obter o arquivo em *PDF*, conforme mostra o resultado na figura abaixo.

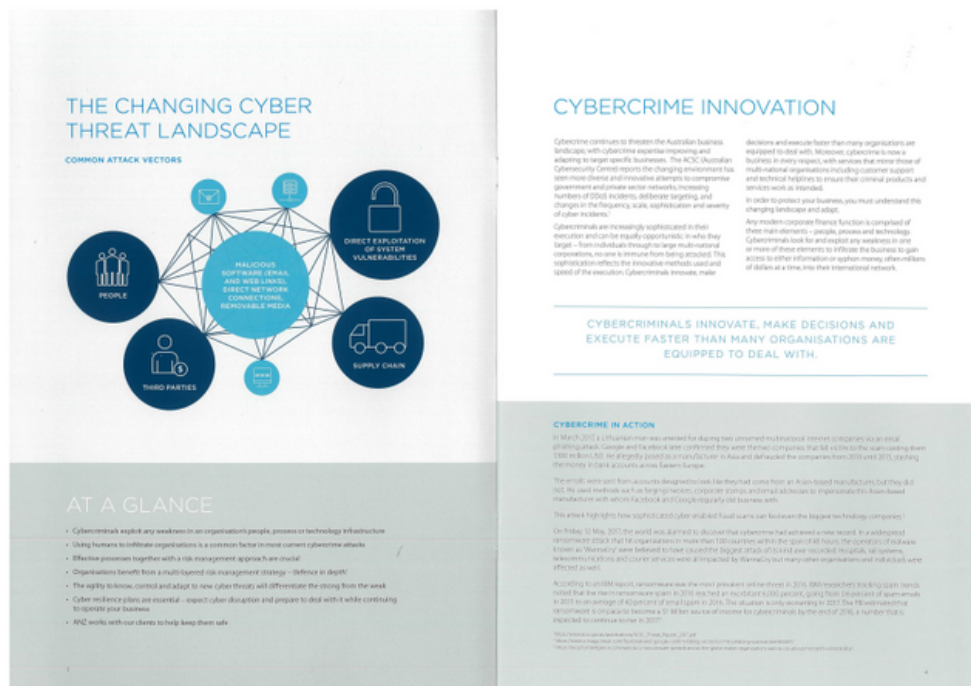


Task 2

Análise de captura de pacotes.



O ANZ_Document2 partirá do mesmo método, os metadados em *HexDump* serão convertidos pelo *CyberChef*, O resultado será o *ANZ_Document2.pdf*, como mostra a figura abaixo:

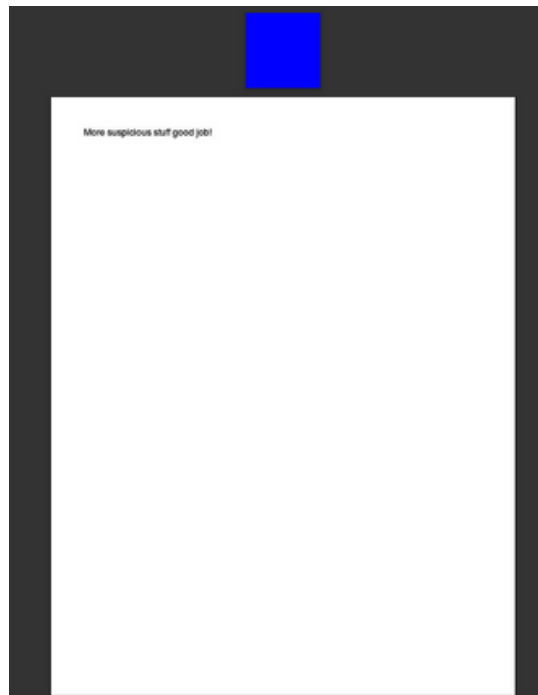


Task 2

Análise de captura de pacotes.



O arquivo *evil* também será feito da mesma forma que os demais, seu nome de arquivo é *evil.pdf* e seu conteúdo é mostrado na imagem abaixo



Task 2

Análise de captura de pacotes.



Quinta sub-task

Ao colocar o protocolo em *ASCII*, pode-se notar que seu formato era em *JFIF*, logo, o método de conversão como foi mostrado na **Primeira sub-task**, Foi necessário apenas colar o intervalo de *ffd8* à *ffd9* no programa *HxD* e salvar em *jpg*, a figura abaixo é o resultado disso.



Task 2

Análise de captura de pacotes.



Sexta sub-task

Mesmo procedimento do 2.1, já que é um arquivo no formato *jpg*. Logo, o resultado do *atm-image.jpg* é mostrado nessa imagem abaixo.



Sétima sub-task

Procedimento igual aos demais, devido ser uma imagem. O resultado será apresentado abaixo do arquivo *broken.png*.



Task 2

Análise de captura de pacotes.



Oitava sub-task

Devido à complexidade de obter os metadados do arquivo zip da última sub-task, ela não será apresentada aqui, devido não conseguir obtê-la.