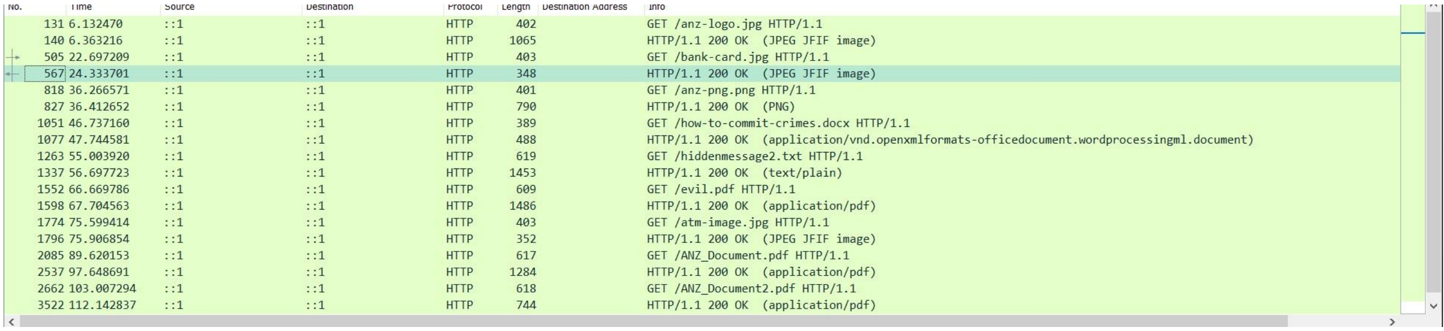
Provide a report on your findings from the pcap file and outline what processes / the steps you followed to achieve this. Here are each of your sub-tasks with additional instructions. Please record your findings under each sub-task title.

Sub-task 1:

- *anz-logo.jpg and bank-card.jpg are two images that show up in the users network traffic.*
- *Extract these images from the pcap file and attach them to your report.*

This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including one for anz-logo.jpg and bank-card.jpg



No.	Time	Source	Destination	Protocol	Length	Destination Address	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)
818	36.266571	::1	::1	HTTP	401		GET /anz-png.png HTTP/1.1
827	36.412652	::1	::1	HTTP	790		HTTP/1.1 200 OK (PNG)
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.openxmlformats-officedocument.wordprocessingml.document)
1263	55.003920	::1	::1	HTTP	619		GET /hiddenmessage2.txt HTTP/1.1
1337	56.697723	::1	::1	HTTP	1453		HTTP/1.1 200 OK (text/plain)
1552	66.669786	::1	::1	HTTP	609		GET /evil.pdf HTTP/1.1
1598	67.704563	::1	::1	HTTP	1486		HTTP/1.1 200 OK (application/pdf)
1774	75.599414	::1	::1	HTTP	403		GET /atm-image.jpg HTTP/1.1
1796	75.906854	::1	::1	HTTP	352		HTTP/1.1 200 OK (JPEG JFIF image)
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)

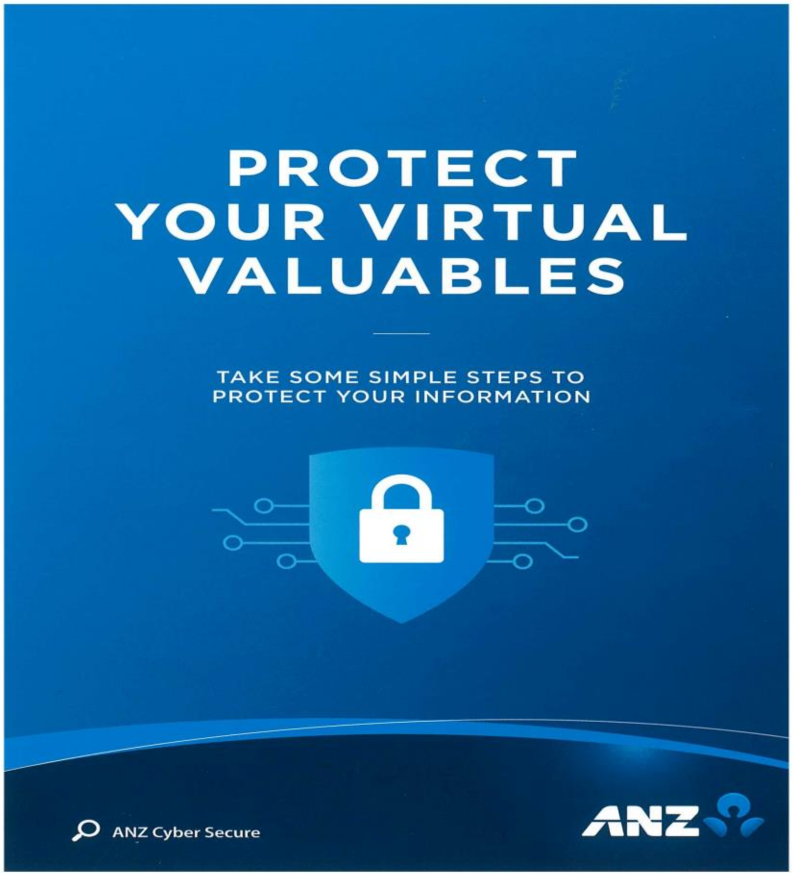
To investigate this image download further, I viewed its TCP stream to see what I could find. Looking through the data in the TCP stream showed that this get request actually downloaded two images, as the data contained two headers and two footers for a .jpg image. The header/footer is FFD8 – FFD9 in hex and the images are also recognizable in ASCII by the string ‘JFIF’ near the start.

Here is the both photos downloaded.

Sub-task 2:

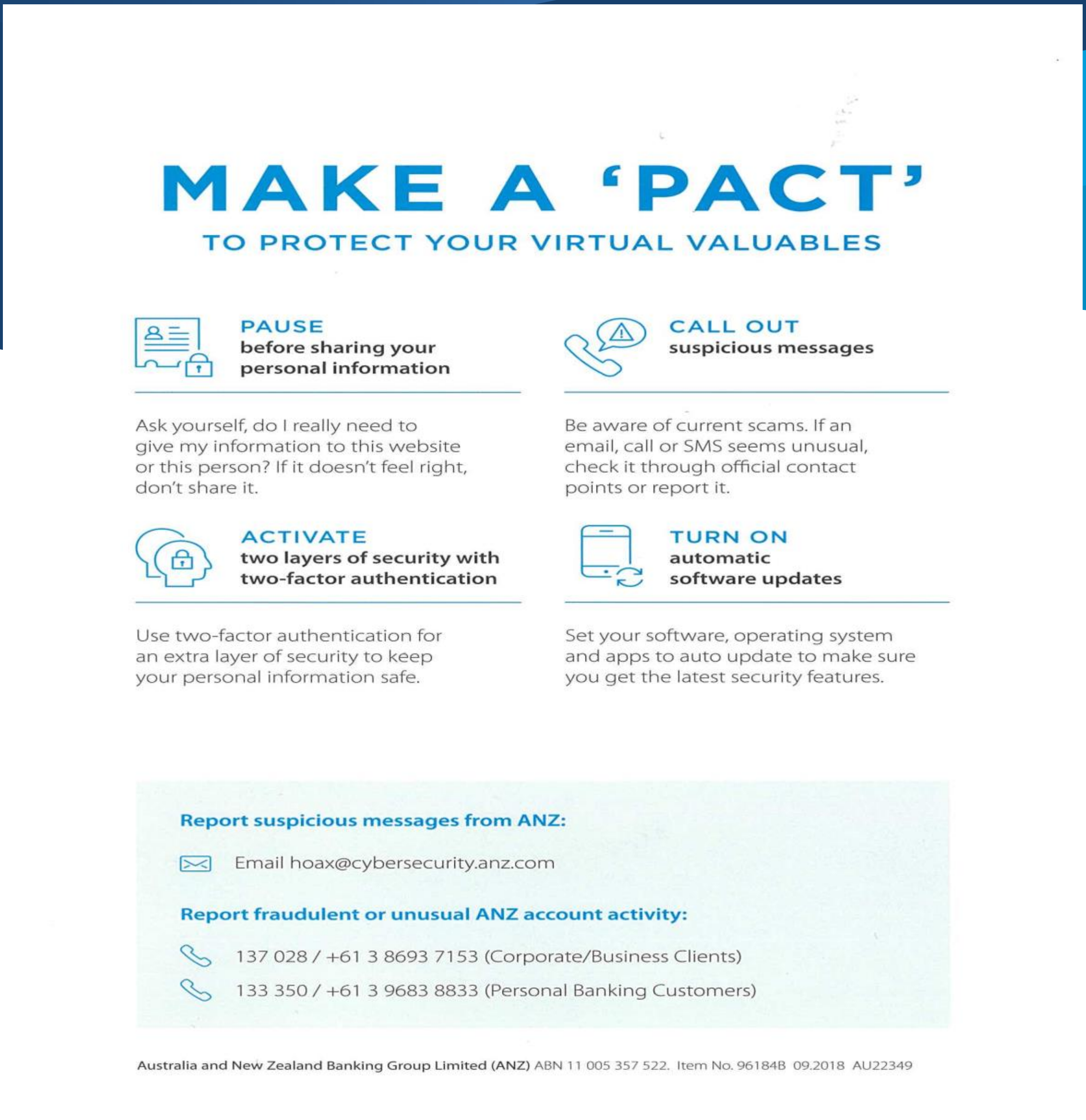
- *The network traffic for the images "ANZ1.jpg" and "ANZ2.jpg" is more than it appears.*
- *Extract the images, include them and mention what is different about them in your report.*

I followed the same process to extract these images as I did in the sub-task1.
The image for ANZ1.jpg


PROTECT YOUR VIRTUAL VALUABLES
TAKE SOME SIMPLE STEPS TO PROTECT YOUR INFORMATION
ANZ Cyber Secure
ANZ

The difference in the images that I downloaded I have found a hidden massage in their data after the end of the image.
The message in ANZ1.jpg is "**You've found a hidden message in this file! Include it in your write up.**"

ANZ2.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.

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.

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.

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. 96184B 09.2018 AU22349

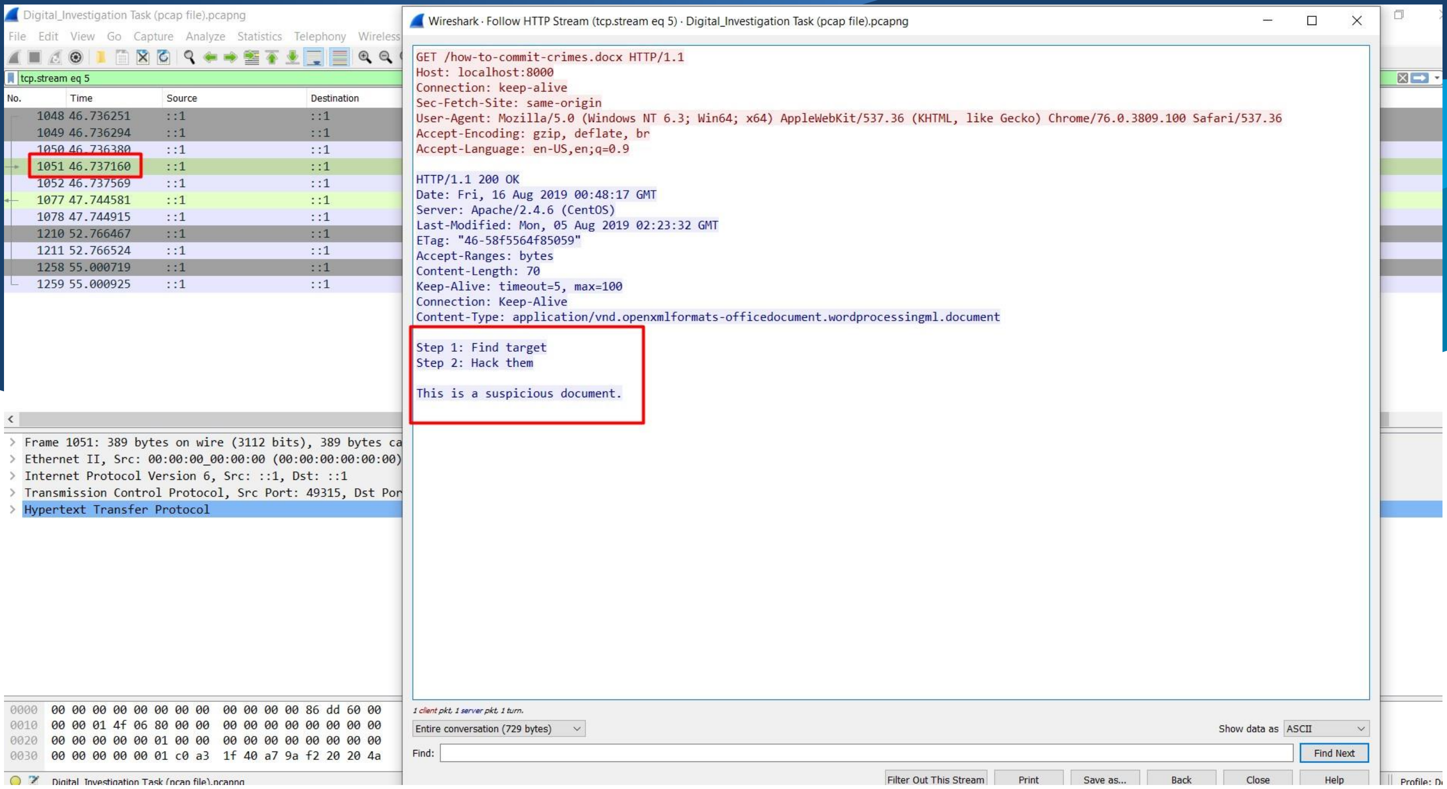
The hidden message in ANZ2.jpg is "**You've found the hidden message! Images are sometimes more than they appear.**"

Sub-task 3:

- *The user downloaded a suspicious document called "how-to-commit-crimes.docx"*
- *Find the contents of this file and include it in your report.*

In order to find the contents of this file I followed the frame number 1051 and the documents contents are visible in the ASCII view.
Step 1: Find target
Step 2: Hack them

This is a suspicious document.


Digital_Investigation Task (pcap file).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless
tcp.stream eq 5
Wireshark · Follow HTTP Stream (tcp.stream eq 5) · Digital_Investigation Task (pcap file).pcapng
1 client pkt, 1 server pkt, 1 turn.
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Profile: D

```
No.        Time           Source        Destination
  1048 46.736251      ::1           ::1
  1049 46.736294      ::1           ::1
  1050 46.736380      ::1           ::1
  1051 46.737160      ::1           ::1
  1052 46.737569      ::1           ::1
  1077 47.744581      ::1           ::1
  1078 47.744915      ::1           ::1
  1210 52.766467      ::1           ::1
  1211 52.766524      ::1           ::1
  1258 55.000719      ::1           ::1
  1259 55.000925      ::1           ::1

> Frame 1051: 389 bytes on wire (3112 bits), 389 bytes ca
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 49315, Dst Por
> Hypertext Transfer Protocol

0000  00 00 00 00 00 00 00 00  00 00 00 00 86 dd 60 00
0010  00 00 01 4f 06 80 00 00  00 00 00 00 00 00 00 00
0020  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00
0030  00 00 00 00 00 01 c0 a3  1f 40 a7 9a f2 20 20 4a

Digital_Investigation Task (pcap file).pcapng
```

```
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.
```

Entire conversation (729 bytes)

Show data as ASCII

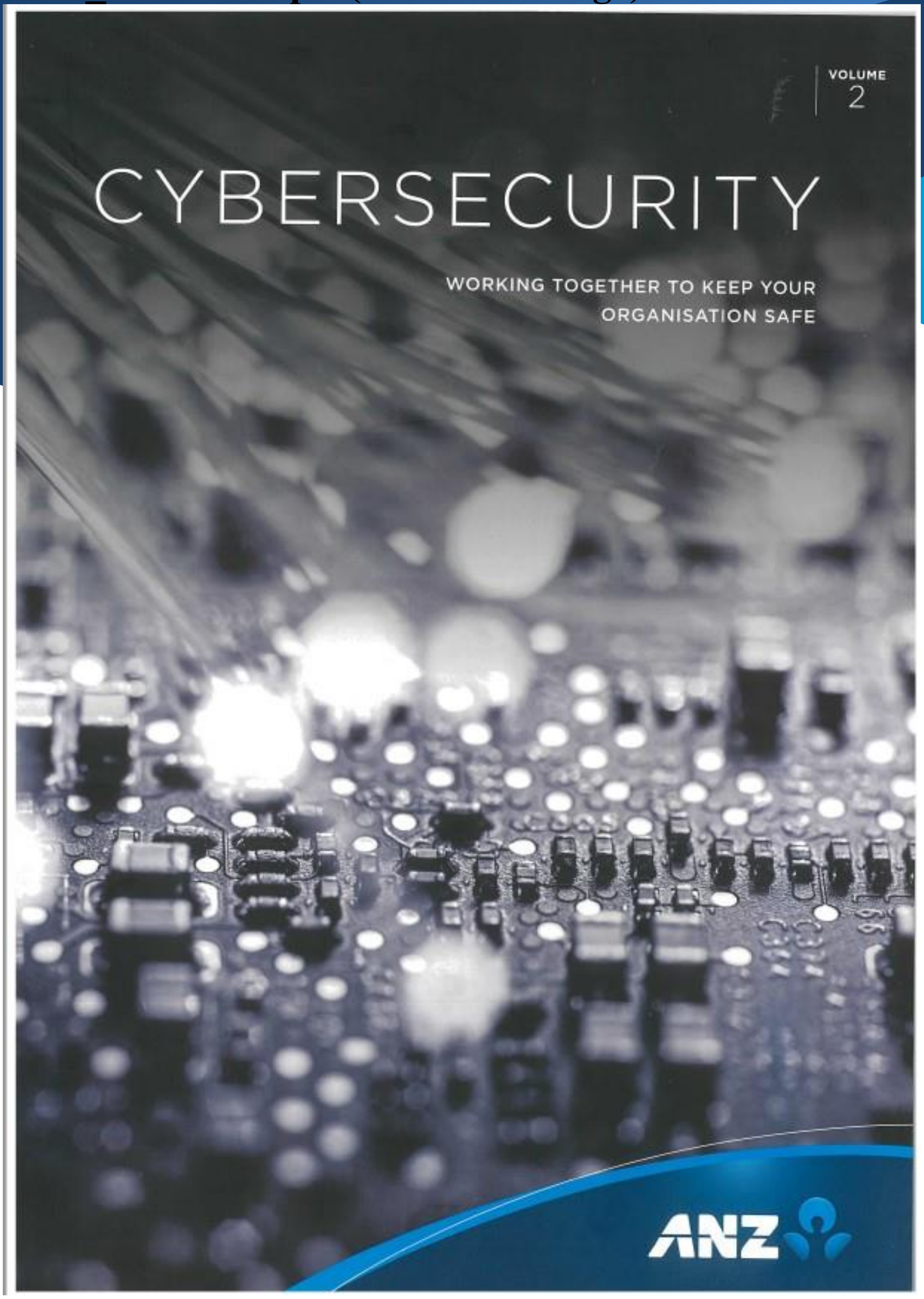
Sub-task 4:

- *The user accessed 3 pdf documents: ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf*
- *Extract and view these documents. Include images of them in your report.*

I followed the TCP stream as usual and found the signature for a PDF, which is the hex data “25 50 44 46”. I copied all the hex data into HxD and saved it.

This process worked for all three files:

ANZ_Document.pdf(extracted image)



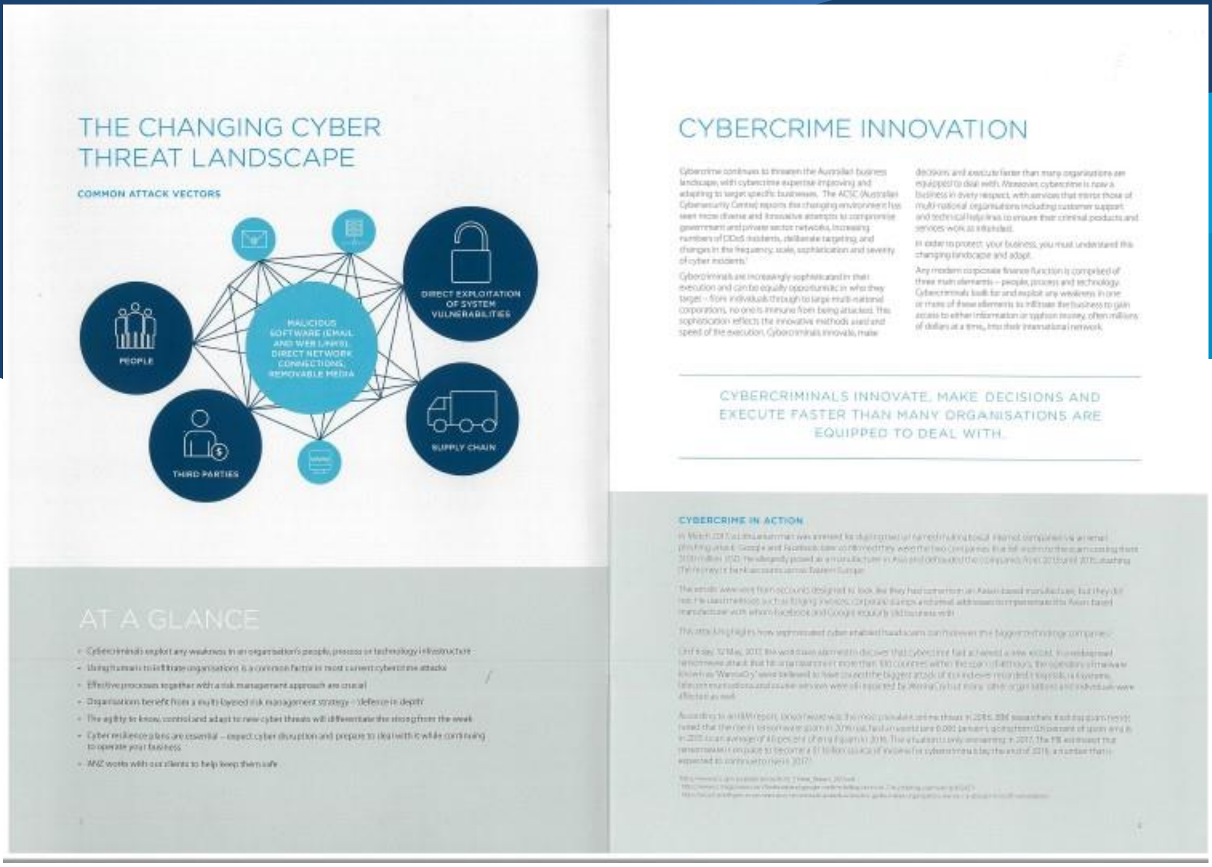
VOLUME
2

CYBERSECURITY

WORKING TOGETHER TO KEEP YOUR
ORGANISATION SAFE

ANZ

ANZ_Document2.pdf(extracted image)



THE CHANGING CYBER THREAT LANDSCAPE

COMMON ATTACK VECTORS

MALICIOUS SOFTWARE (EMAIL AND WEB LINKS), DIRECT NETWORK CONNECTIONS, REMOVABLE MEDIA
PEOPLE
THIRD PARTIES
DIRECT EXPLOITATION OF SYSTEM VULNERABILITIES
SUPPLY CHAIN

AT A GLANCE

- Cybercriminals exploit any weakness in an organisation's people, process or technology infrastructure
- Using humans to infiltrate organisations is a common factor in most current cybercrime attacks
- Effective processes together with a risk management approach are crucial
- Organisations benefit from a multi-layered risk management strategy – 'defence in depth'
- The agility to know, control and adapt to new cyber threats will differentiate the strong from the weak
- Cyber resilience plans are essential – expect cyber disruption and prepare to deal with it while continuing to operate your business
- ANZ works with our clients to help keep them safe

CYBERCRIME INNOVATION

Cybercrime continues to threaten the Australian business landscape, with cybercrime expertise improving and adapting to target specific businesses. The ACSC (Australian Cybersecurity Centre) reports the changing environment has seen more diverse and innovative attempts to compromise government and private sector networks, increasing numbers of DDoS incidents, deliberate targeting, and changes in the frequency, scale, sophistication and severity of cyber incidents.[1]

Cybercriminals are increasingly sophisticated in their execution and can be equally opportunistic in who they target – from individuals through to large multi-national corporations, no one is immune from being attacked. This sophistication reflects the innovative methods used and speed of the execution. Cybercriminals innovate, make decisions and execute faster than many organisations are equipped to deal with. Moreover, cybercrime is now a business in every respect, with services that mirror those of multi-national organisations including customer support and technical help lines to ensure their criminal products and services work as intended.

In order to protect your business, you must understand this changing landscape and adapt.

Any modern corporate finance function is comprised of three main elements – people, process and technology. Cybercriminals look for and exploit any weakness in one or more of these elements to infiltrate the business to gain access to either information or siphon money, often millions of dollars at a time, into their international network.

CYBERCRIMINALS INNOVATE, MAKE DECISIONS AND EXECUTE FASTER THAN MANY ORGANISATIONS ARE EQUIPPED TO DEAL WITH.

CYBERCRIME IN ACTION

In March 2017 a Lithuanian man was arrested for duping two [illegible] multinational internet companies via an email phishing attack. Google and Facebook later confirmed they were the two companies that fell victim to the scam costing them 100 million USD. He allegedly posed as a manufacturer in Asia and defrauded the companies from 2013 until 2015, stashing the money in bank accounts across Eastern Europe.

The emails were sent from accounts designed to look like they had come from an Asian based manufacturer, but they did not. He used methods such as forging invoices, corporate stamps and email addresses to impersonate the Asian based manufacturer with whom Facebook and Google regularly did business with.

This attack highlights how sophisticated cyber enabled fraud scams can fool even the biggest technology companies.

On Friday, 12 May, 2017 the world was alarmed to discover that cybercrime had achieved a new record. In a widespread ransomware attack that hit organisations in more than 100 countries within the span of 48 hours, the operators of malware known as 'WannaCry' were believed to have caused the biggest attack of its kind ever recorded. Hospitals, railways, telecommunications and courier services were all impacted by WannaCry but many other organisations and individuals were affected as well.

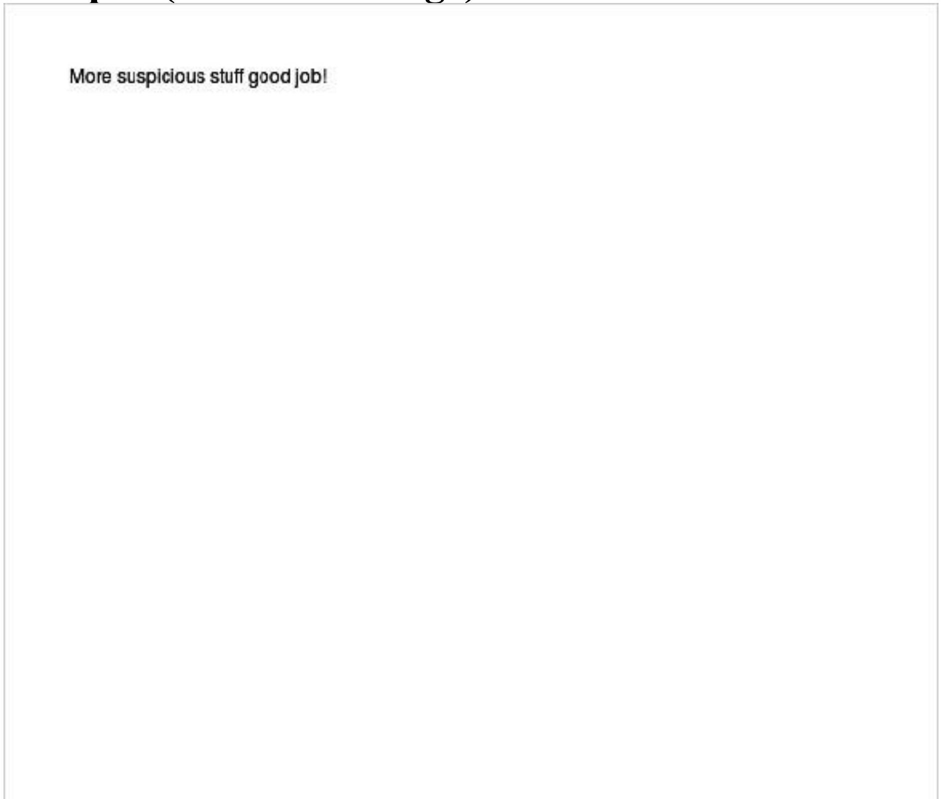
According to an IBM report, ransomware was the most prevalent online threat in 2016. IBM researchers tracking spam [illegible] noted that the rise in ransomware spam in 2016 [illegible] 0.001 percent [illegible] percent of spam [illegible] in 2015 to an average of 40 percent of all spam in 2016. The situation is only worsening in 2017. The FBI estimated that ransomware is on pace to become a $1 billion source of income for cybercriminals by the end of 2016, a number that is expected to continue to rise in 2017.

[illegible]

[illegible]

[illegible]

Evil.pdf (extracted image)

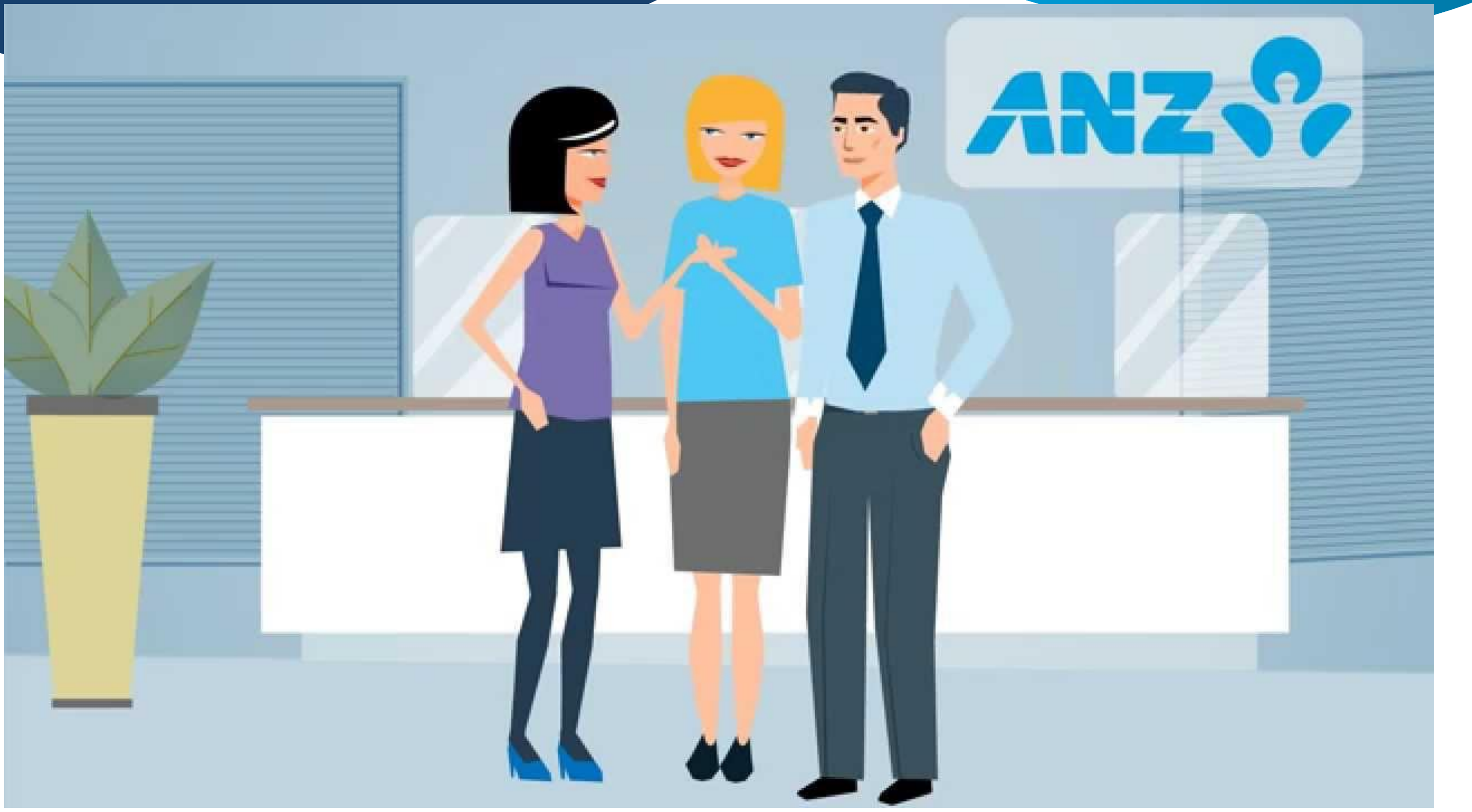


More suspicious stuff good job!

Sub-task 5:

- *The user also accessed a file called "hiddenmessage2.txt"*
- *What is the contents of this file? Include it in your report*

I followed the TCP stream of the file. I have noticed the data is encoded. I viewed the data as hex and I find out it has the same signature as a jpg image. I copied the data into HxD and saved.After saving it I find out the the text file was aactually an image file which is down below.



Sub-task 6:

- *The user accessed an image called "atm-image.jpg"*
- *Identify what is different about this traffic and include everything in your report.*

I viewed the TCP stream as usual, and found two different signatures and they are jpeg file signatures. After finding the FFD8 and FFD9 I copied the raw data in to HxD and saved it.

Image 1 :

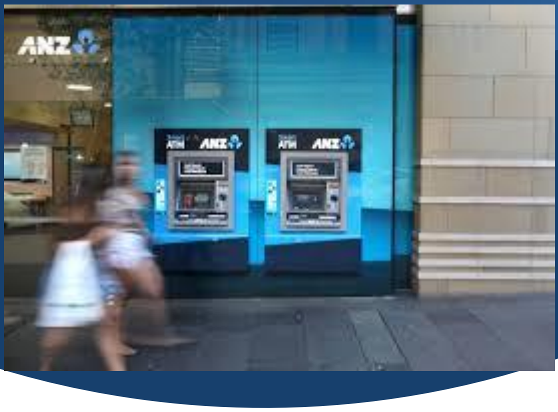
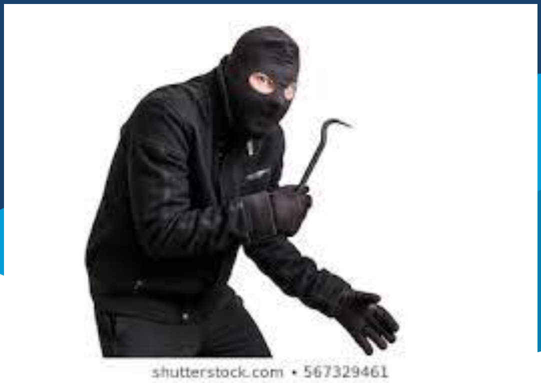


Image 2 :

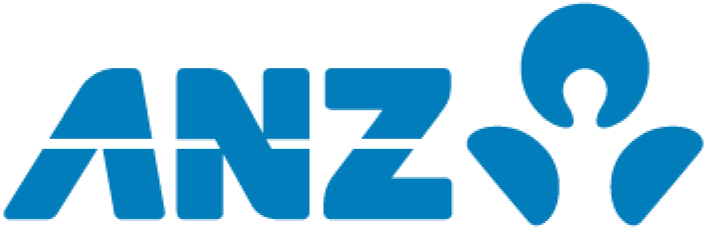


The difference about this traffic is there is only single GET request but the user downloaded two different images.

Sub-task 7:

- *The network traffic shows that the user accessed the image "broken.png"*
- *Extract and include the image in your report.*

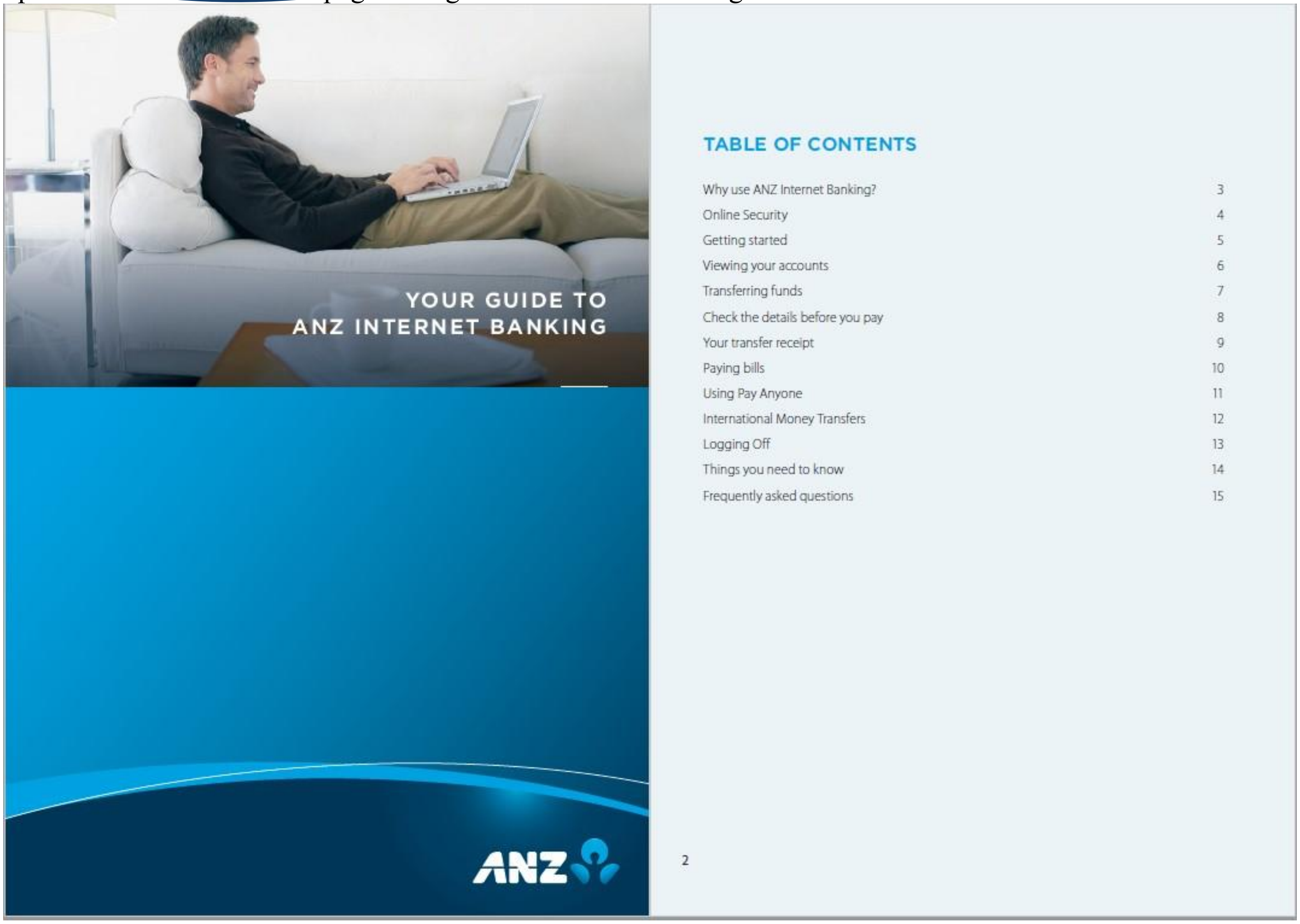
In order to find the image I filtered the pcap for http to find the GET request for this file. I found the frame and followed it.When I look into data I chanced the format into raw to look for png signatures.I find out the the data is encoded. I used CyberChef to encode data and copy it in hex format. I copied the data into HxD and found the image.



Sub-task 8:

- *The user accessed one more document called securepdf.pdf*
- *Access this document include an image of the pdf in your report. Detail the steps to access it.*

I followed the TCP stream for secure.pdf. I discover the data in the frame is not for a pdf file. There was hidden message at the bottom of the data which is : Password is “secure”. In data I saw a file named rawpdf.pdf.Also data is contained the file signature for a zip file, meaning that the what the user downloaded was actually a zip file. So I copied the hex of the zip file into HxD and saved it as a zip file. I opened this zip file, and found it contained a pdf file called rawpdf.pdf. When opened, the pdf it asked for a password. The password ‘secure’ shown at the bottom of the data and it worked, and the PDF opened. It was the first two pages to a guide for internet banking.



YOUR GUIDE TO
ANZ INTERNET BANKING

ANZ

TABLE OF CONTENTS