

Packet Capture Analysis:

I have analysed the provided packet capture file using Wireshark.

I filtered the network traffic to only see HTTP requests information. This allowed me to see http GET requests.

Sub-task 1:

anz-logo.jpg and bank-card.jpg are two images that show up in the users network traffic, I viewed the TCP stream of the images.

The data there contained header for jpeg , which is FFD8.

I viewed the data in raw format and copied all the data between ffd8-ffd9.

Then I saved the copied into HxD and saved them in .jpeg format to obtain both the images.



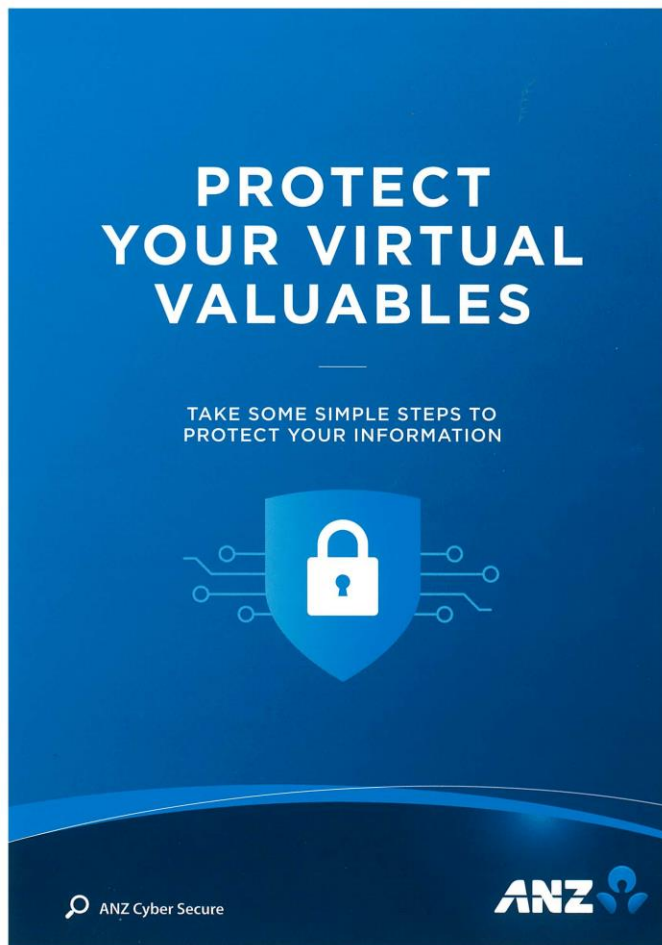
Anz-logo.jpg



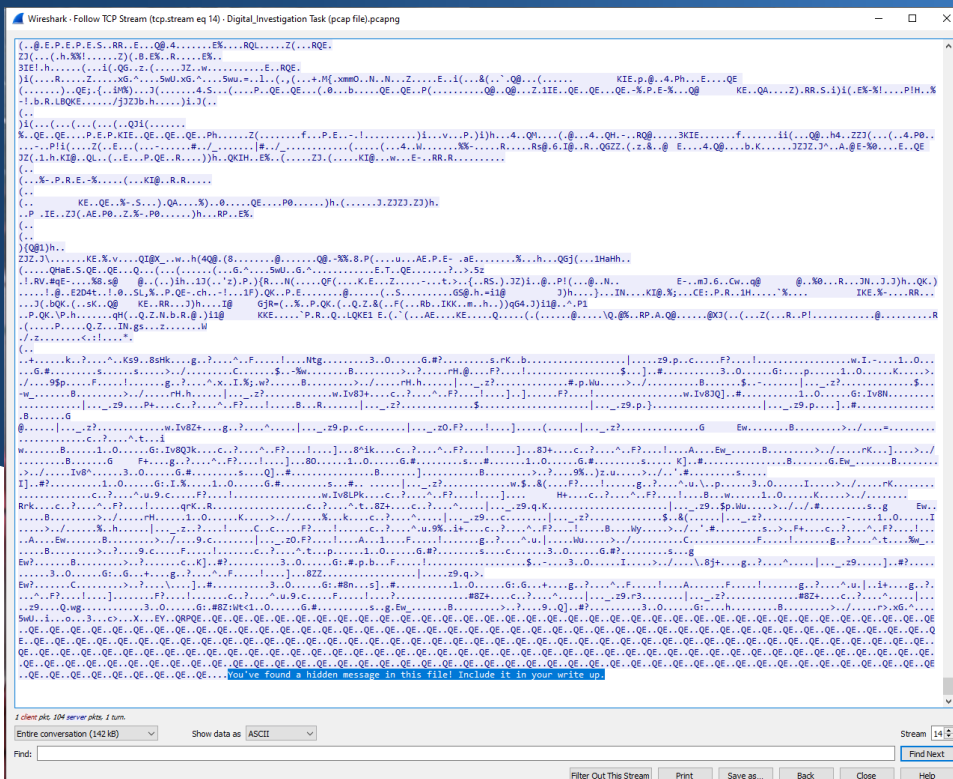
Bank-card.jpg

Sub-task 2:

Upon viewing the TCP stream of the two images ANZ1.jpg and ANZ2.jpg in ASCII format, I found that there is a hidden message at the bottom for both the files. The hidden message in ANZ1.jpg was "You've found a hidden message in this file! Include it in your write up." The hidden message in ANZ2.jpg was "You've found the hidden message! Images are sometimes more than they appear." Then I viewed the data in raw format and copied everything between ffd8-ffd9 and saved it in HxD in .jpeg format to extract both the images.



ANZ1.jpg



Hidden message in 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.



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.

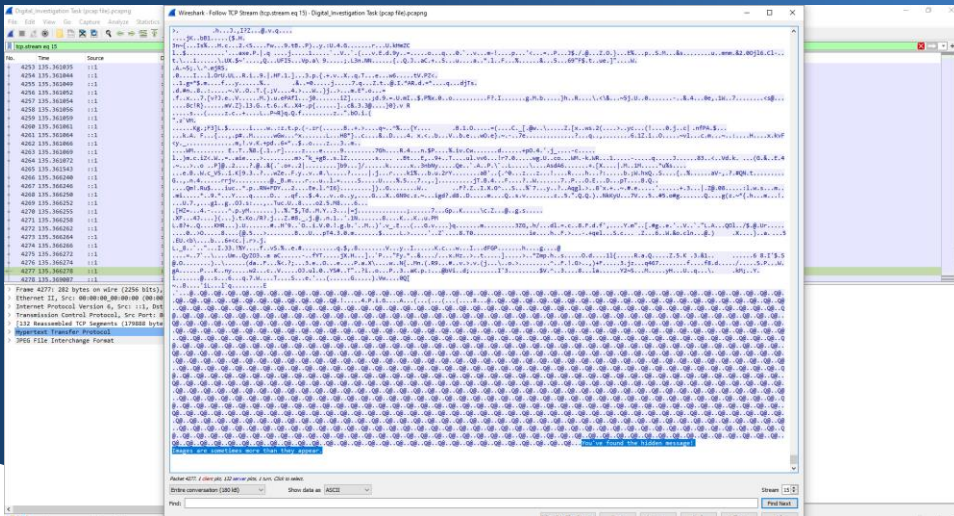
Report suspicious messages from ANZ:

Email hoax@cybersecurity.anz.com

Report fraudulent or unusual ANZ account activity:

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

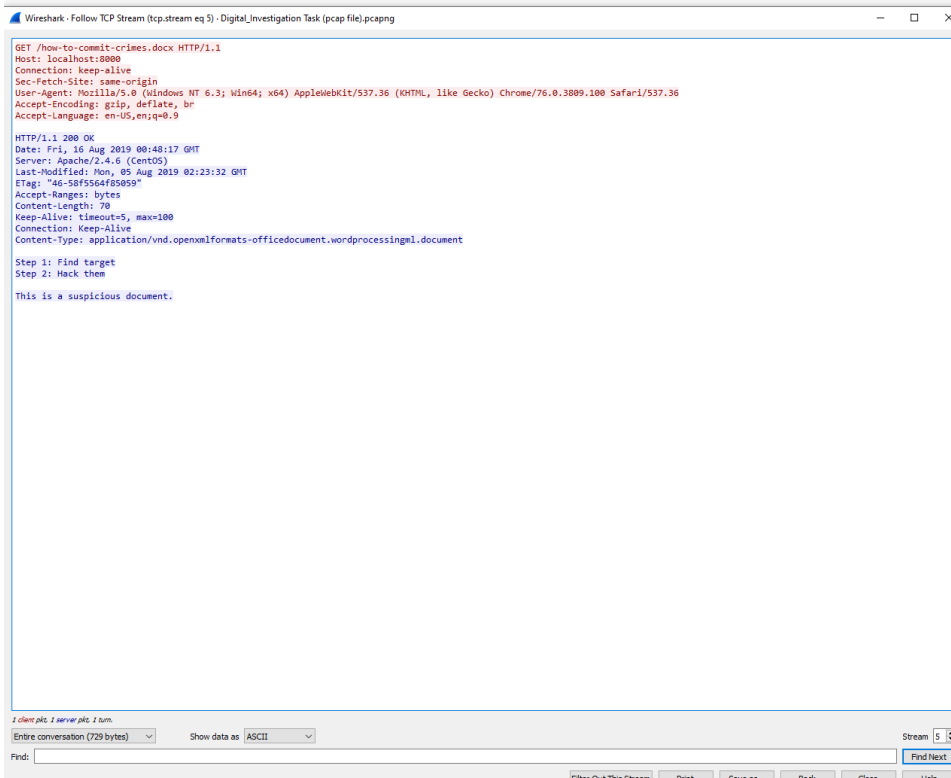
133 350 / +61 3 9683 8833 (Personal Banking Customers)



Hidden message in ANZ2.jpg

Sub-task 3:

Upon viewing the TCP stream of the document “how-to-commit-crimes.docx” in ASCII format, I was able to see the contents of the document.



Contents of the document "how-to-commit-crimes.docx"

Sub-task 4:

I opened the TCP stream of the three PDF's ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf and found out that the file signature was for a pdf, which is “25 50 44 46”.

I copied all the hex data from the file signature onwards and saved it in .pdf format in HxD.

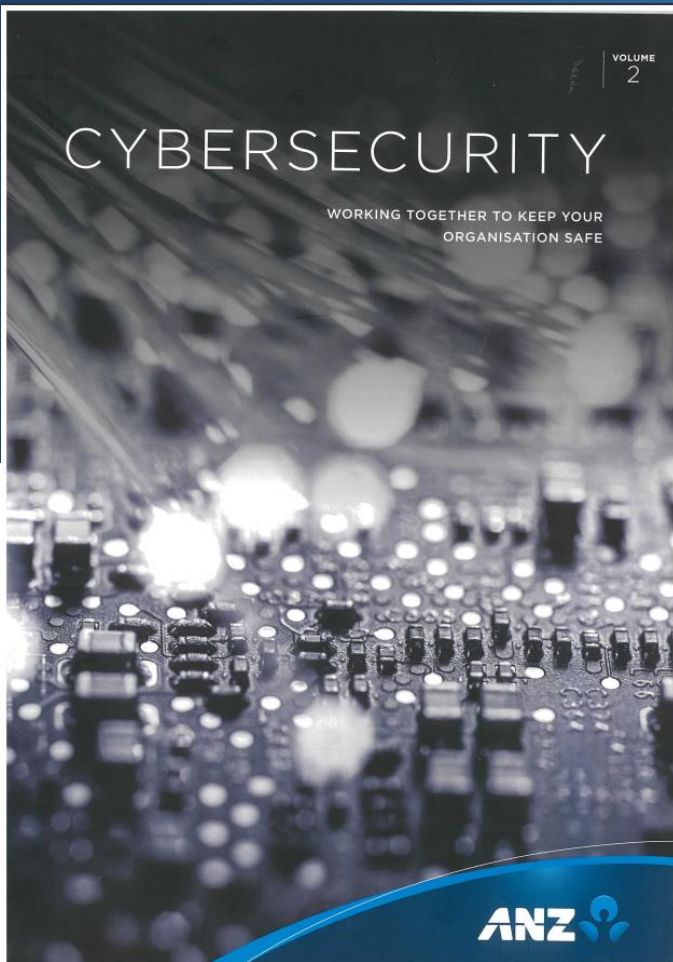


Image of ANZ_document.pdf

THE CHANGING CYBER THREAT LANDSCAPE

COMMON ATTACK VECTORS

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 critical
- Organisations benefit from a multi-layered risk management strategy – defence in depth
- The ability 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, malware targeting, and changes in the frequency, scale, sophistication and severity of cyber incidents.

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 helpdesks 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 system 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 unnamed multinational internet companies via an email phishing attack. Google and Twitter later confirmed they were the two companies that fell victim to the scam costing them \$500 million USD. He allegedly posed as a manufacturer in Asia and defrauded the companies from 2011 until 2015, siphoning the money in bank accounts across Eastern Europe.

The email 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 this 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: a widespread ransomware attack that hit organisations in more than 160 countries within the span of 48 hours. The ransomware known as 'WannaCry' were believed to have caused the biggest attack of its kind ever recorded. Hospitals, oil systems, 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 research tracking spam trends found that the top five ransomware spam in 2016 reached an astonishing 6,000 percent, going from 0.2 percent of spam emails in 2015 to an average of 40 percent of email 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.

<https://www.acsc.gov.au/australian-cybersecurity-centre/2017/03/2017-phishing-report/>
<https://www.ibm.com/security/ransomware>
<https://www.fbi.gov/newsroom/press-releases/2017/05/17/fbi-issues-warning-ransomware-attacks>

Image of ANZ_document2.pdf

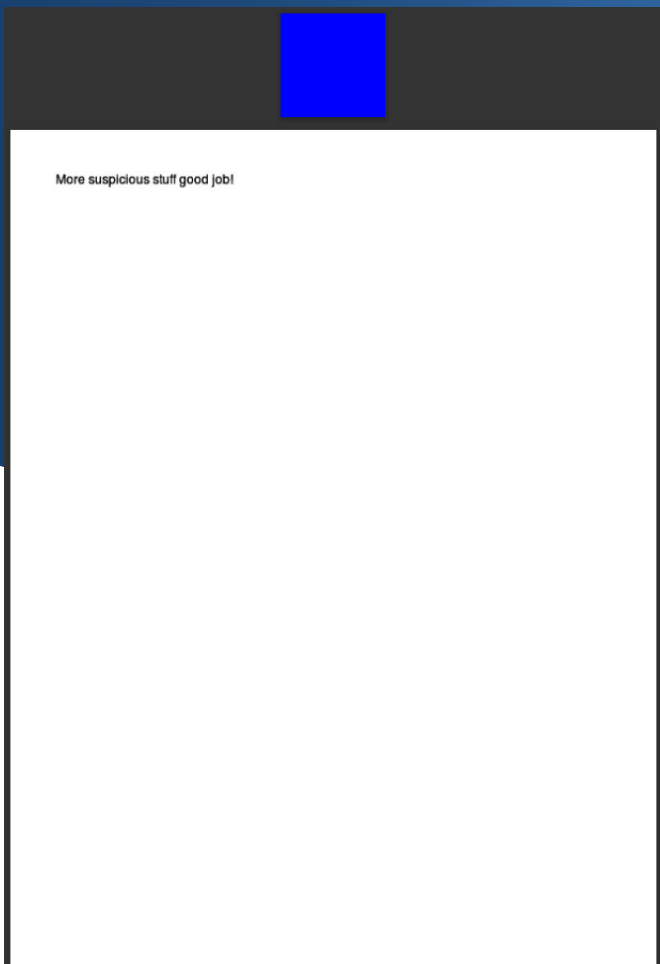
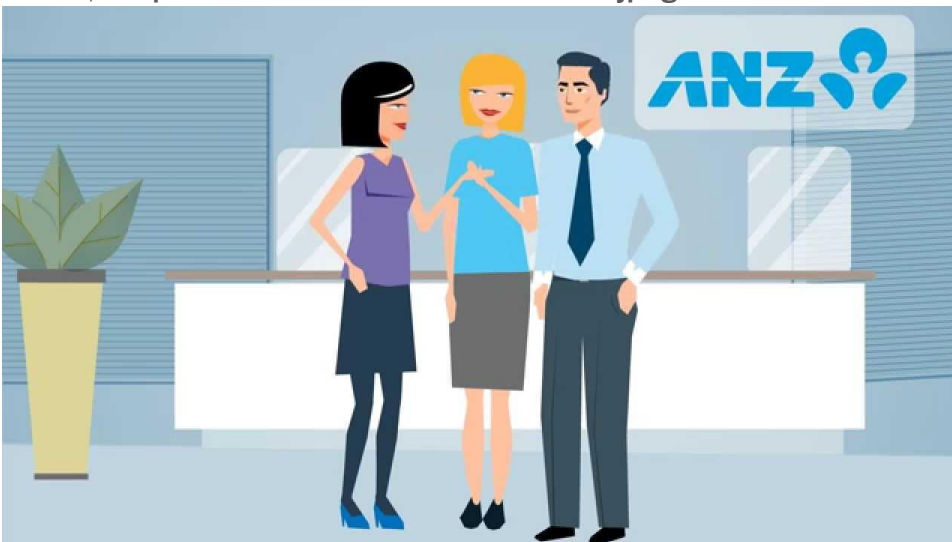


Image of evil.pdf

Sub-task 5:

I opened the TCP stream for “hiddenmessage2.txt” and viewed it as hex. I found out that the file signature is same as that of a jpeg file. So, the text file “hiddenmessage2.txt” was actually an image. Hence, I copied and saved the data in HxD in jpeg format.



Actual content of hiddenmessage2.txt

Sub-task 6:

I opened the TCP stream for "atm-image.jpg" and found out that there are two sets of file signature same as that of a jpeg file.
I opened the TCP stream in raw format and tried extracting both sets of data and I was able to get two different images.



1st Image



2nd Image

Sub-task 7:

Upon viewing the TCP stream for "broken.png" in raw format, I discovered that the file signature was "80 50 4e 47 0d 0a" which is the file signature for a png.
I copied everything following that signature and saved it in .png format in HxD editor to obtain the image.



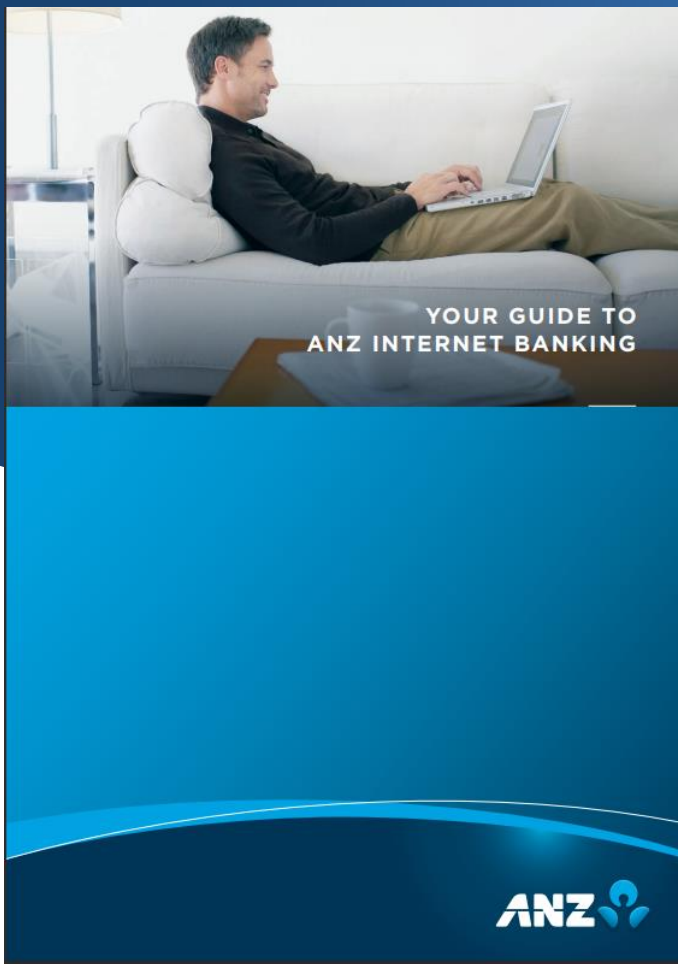
Sub-task 8:

I opened the TCP stream for “securepdf.pdf” in ASCII format and found out that at the bottom there was a message “Password is Secure”. This indicated that the file was actually a ZIP file.

So, I opened the data in raw format and found the file signature for a ZIP file which is “504B0304”.

Hence , I copied everything following that signature and saved it in .rar format in HxD editor.

After extracting the ZIP file using the password “Secure”, I was able to extract the content of the zip file which was a pdf containing two pages.



1st page of the extracted pdf

TABLE OF CONTENTS

Why use ANZ Internet Banking?	3
Online Security	4
Getting started	5
Viewing your accounts	6
Transferring funds	7
Check the details before you pay	8
Your transfer receipt	9
Paying bills	10
Using Pay Anyone	11
International Money Transfers	12
Logging Off	13
Things you need to know	14
Frequently asked questions	15