Digital Investigation Report.

I. Overview of Packet File.

The packet is analysed by utilising the open-source network and packet analysis Wireshark. The general information of the packet is analysed, which provides the general information of the packet for effective investigation.

“Statistic” was chosen at the panel's top, and I checked “Resolved Address”. I want to gather information on different hosts from this packet.

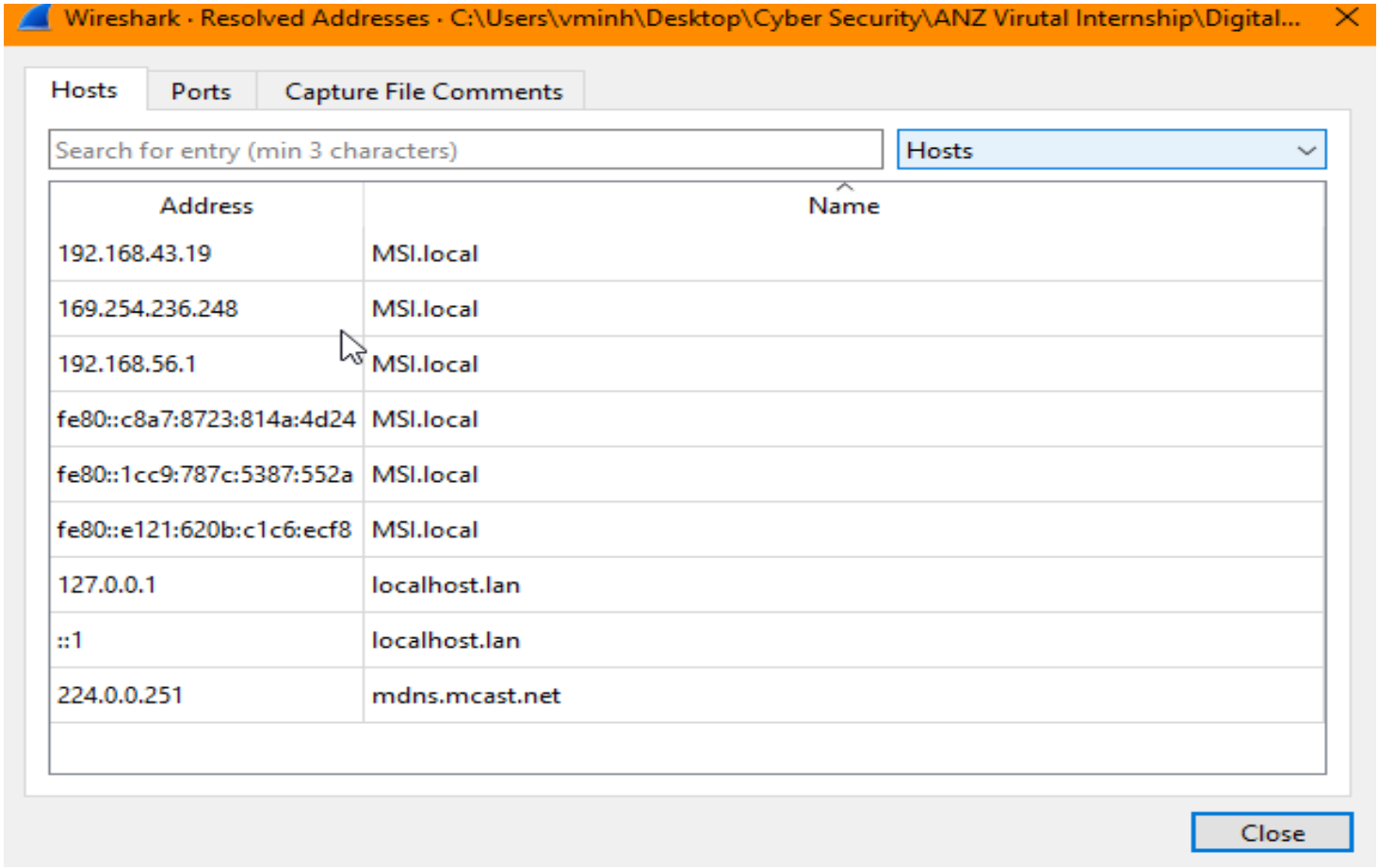


Figure 1: Resolved Address for different Hosts.

According to Figure 1, three main hosts were listed as MSI.local, localhost.lan and mdns.mcast.net. This indicated that the main conversation of this packet was within the LAN, not WAN, because the root domain name was .local and .lan, not .com, .org or .net.

Then, I analysed the “Protocol Hierarchy Statistic” to gather general information about which protocol is used and the percentage of packets.

Wireshark · Protocol Hierarchy Statistics · Digital_Investigation Task (pcap file).pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	26	100.0	17792	898	0	0	0	26
Ethernet	100.0	26	2.0	364	18	0	0	0	26
Internet Protocol Version 6	100.0	26	5.8	1040	52	0	0	0	26
Transmission Control Protocol	100.0	26	92.1	16388	827	0	0	0	26
Hypertext Transfer Protocol	100.0	26	13948.5	2481724	125 k	13	5493	277	26
Portable Network Graphics	3.8	1	26.7	4750	239	1	4750	239	1
Media Type	23.1	6	11623.5	2068060	104 k	6	2068060	104 k	6
Line-based text data	3.8	1	271.2	48244	2436	1	48244	2436	1
JPEG File Interchange Format	19.2	5	1974.7	351337	17 k	5	351337	17 k	5

Figure 2: Protocol Hierarchy Statistics.

According to Figure 2, different types of files were transferred through HTTP, and the two large files contributed the highest percentage: the media file and the JPEG file.

The packet's " Conversations " were analysed, showing the main conversation between two hosts. This provided the contact information between the user and the visited sites.

Wireshark · Conversations · Digital_Investigation Task (pcap file).pcapng

Conversation Settings

- [x] Name resolution
- [ ] Absolute start time
- [ ] Limit to display filter

Copy | Follow Stream... | Graph...

- [ ] Bluetooth
- [ ] BPv7
- [ ] DCCP
- [x] Ethernet

Ethernet · 1 | IPv4 · 15 | IPv6 · 4 | TCP · 19 | UDP · 50

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
localhost.lan	7790	localhost.lan	49183	3,391	542 kB	0	1,696	450 kB	1,695	92 kB	0.000000	171.8573	20 kbps	4266 bits/s
localhost.lan	49289	localhost.lan	8000	2	148 bytes	1	1	74 bytes	1	74 bytes	6.131179	0.0001		
localhost.lan	49294	localhost.lan	8000	14	7 kB	2	6	784 bytes	8	6 kB	6.131882	16.5638	378 bits/s	2856 bits/s
localhost.lan	49298	localhost.lan	8000	20	14 kB	3	7	859 bytes	13	13 kB	22.696600	13.5684	506 bits/s	7528 bits/s
localhost.lan	49299	localhost.lan	8000	14	6 kB	4	6	783 bytes	8	6 kB	36.265832	10.4693	598 bits/s	4309 bits/s
localhost.lan	49315	localhost.lan	8000	11	2 kB	5	6	771 bytes	5	796 bytes	46.736251	8.2647	746 bits/s	770 bits/s
localhost.lan	49318	localhost.lan	8000	48	53 kB	6	9	1 kB	39	51 kB	55.002517	11.6640	838 bits/s	35 kbps
localhost.lan	49319	localhost.lan	8000	7	542 bytes	7	4	308 bytes	3	234 bytes	55.006042	11.8054	208 bits/s	158 bits/s
localhost.lan	49320	localhost.lan	8000	25	20 kB	8	8	1 kB	17	19 kB	66.668064	8.9306	1020 bits/s	17 kbps
localhost.lan	49321	localhost.lan	8000	21	15 kB	9	7	859 bytes	14	14 kB	66.671389	22.9465	299 bits/s	4980 bits/s
localhost.lan	49323	localhost.lan	8000	277	357 kB	10	27	3 kB	250	355 kB	89.619109	8.0302	2543 bits/s	353 kbps
localhost.lan	49324	localhost.lan	8000	7	542 bytes	11	4	308 bytes	3	234 bytes	89.621740	13.4980	182 bits/s	138 bits/s
localhost.lan	49325	localhost.lan	8000	680	894 kB	12	58	5 kB	622	889 kB	103.004096	9.1391	4243 bits/s	778 kbps
localhost.lan	49326	localhost.lan	8000	7	542 bytes	13	4	308 bytes	3	234 bytes	103.010423	17.1444	143 bits/s	109 bits/s
localhost.lan	49329	localhost.lan	8000	123	152 kB	14	15	1 kB	108	151 kB	119.920782	12.7387	908 bits/s	94 kbps
localhost.lan	49331	localhost.lan	8000	153	192 kB	15	17	2 kB	136	190 kB	132.661089	11.1304	1145 bits/s	136 kbps
localhost.lan	49334	localhost.lan	8000	16	8 kB	16	7	1 kB	9	7 kB	143.792544	6.9538	1196 bits/s	8494 bits/s
localhost.lan	49335	localhost.lan	8000	697	918 kB	17	59	5 kB	638	913 kB	143.795521	20.7144	1899 bits/s	352 kbps
localhost.lan	49338	localhost.lan	8000	3	246 bytes	18	2	160 bytes	1	86 bytes	150.758957	0.0003		

Figure 3: Investigation of Conversation hosts via TCP stream.

According to Figure 3, the main conversation happened only between two localhost.lan. In addition, the conversation did not include ports like 80 and 443, meaning the user did not access the local webserver or a different webserver via the Internet. The whole conversation with the HTTP server was conducted within the LAN.

II. Investigation of the HHTP conversation.

From Figure 2 and Figure 3, I can conclude that the user contacted the HTTP server via the Local Area Network to Get some files from the server. Therefore, “http” was utilised within the filter field to narrow my investigation and give an in-depth understanding of the conversation.

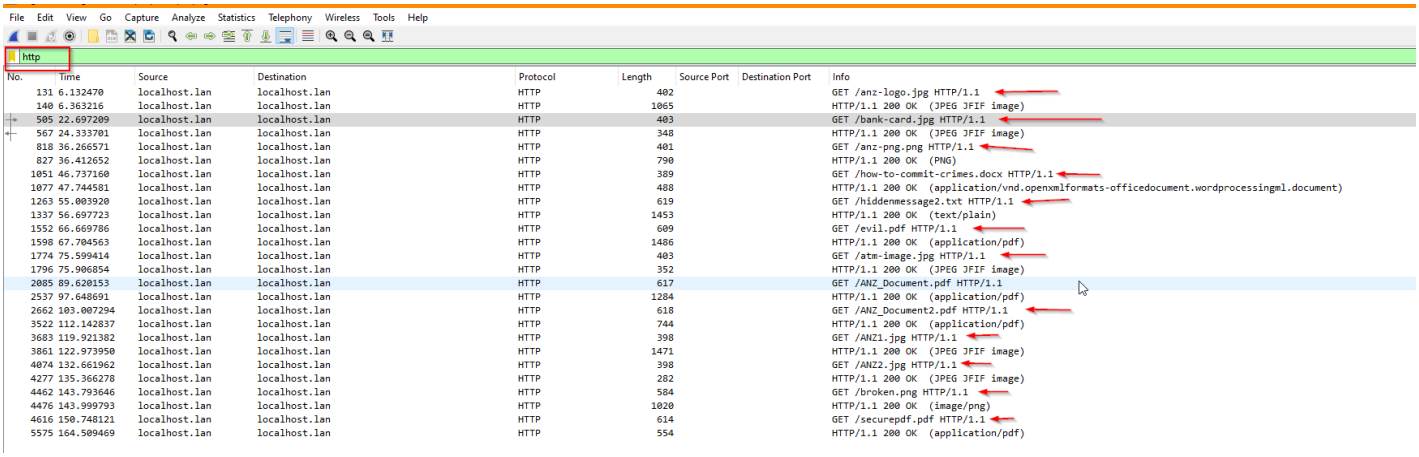


Figure 4: Investigation of HTTP conversation.

The main request from the HTTP server was GET and not PUT, which determined that the user had requested to download different files from the HTTP server: text, pdf, picture, and document files. The user didn't use the PUT request, which means that the user did not have privileged authorisation for any modification or updating of the content and data of the webserver.

III. Investigation of the anz-logo.jpg and bank-card.jpg files.

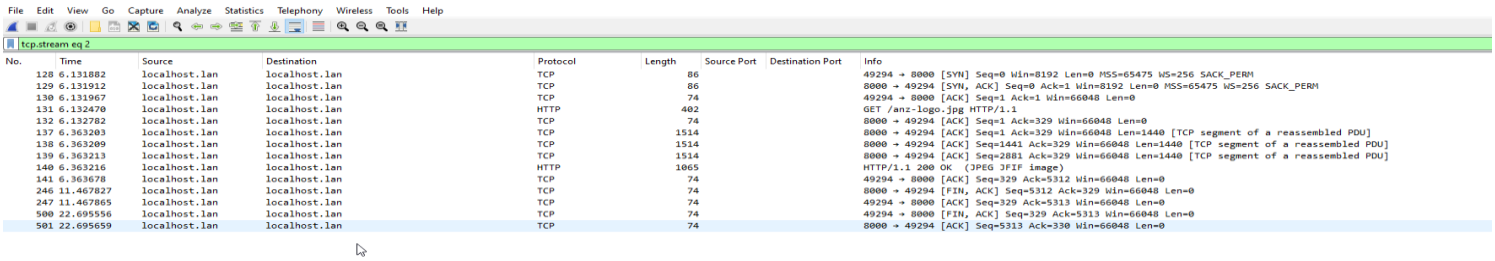


Figure 5: Investigation of anz-logo.jpg via TCP stream.

In terms of further investigation of different files, the following TCP stream was implemented so the raw data of the JPEG file was recorded and analysed later by the HxD to decode the Hexadecimal code of the file.

The Hex Signature of the JPEG file was found as FFD8 as the header and FFD9 as the footer. The image hex was extracted from the TCP stream by copying all the hexes from FFD8 to FFD9 and pasting them into the hex editor program HxD. Then, the file was saved as JPG and opened by Paint. The result of the image was shown in Image 1, which was the logo of ANZ.

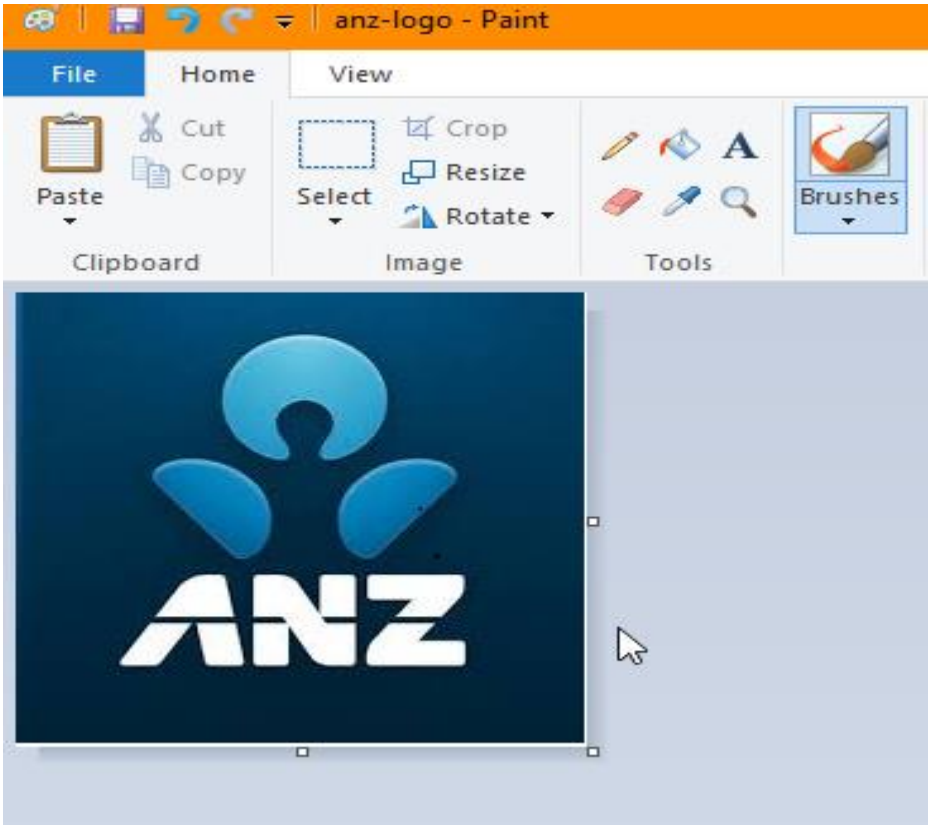


Image 1: ANZ Logo.

The same procedure was used to investigate the bank-card.jpg file. The result of this picture is shown in Image 2.

Image 2: ANZ bankcard.

IV. Investigation of ANZ1.jpg and ANZ2.jpg

After following the TCP stream, I analysed both files, which showed the extra message at the bottom of the files.

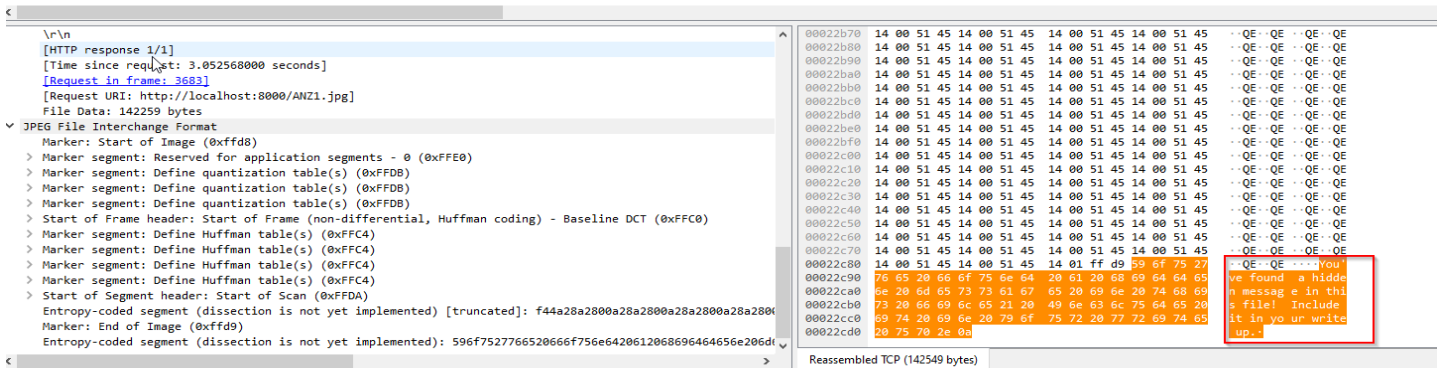


Figure 6: Embed message within the ANZ1 file.

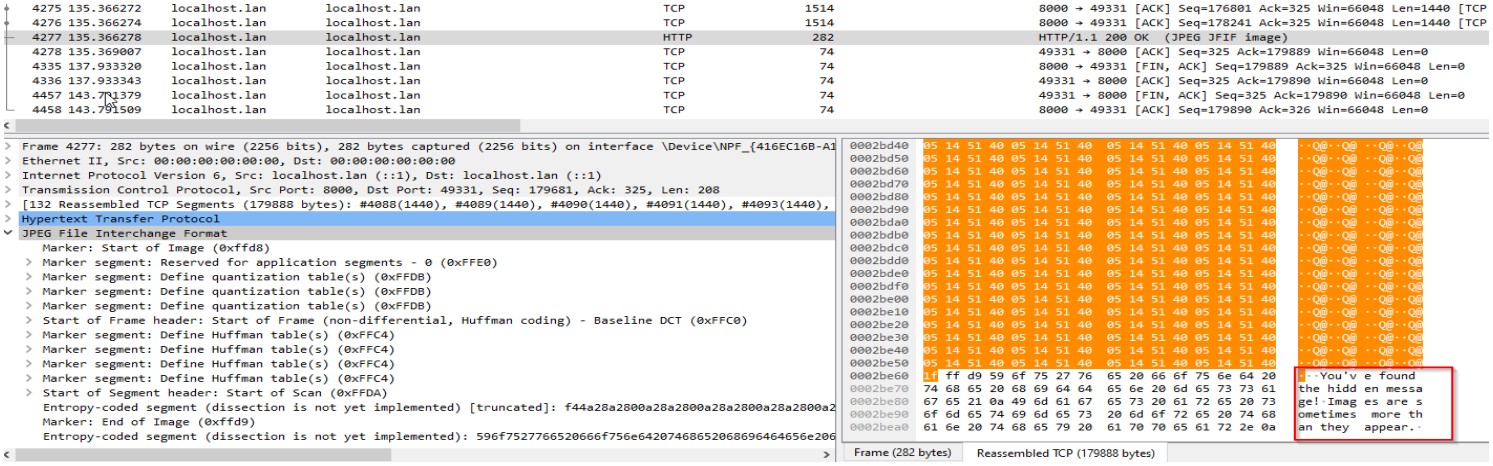


Figure 7: Embed message within the ANZ2 file.

The hex signature of the jpg contained FFD8 and FFD9 as the header and the footer, respectively. Therefore, the extra hex codes from the messages were deleted. The hex codes were then extracted and analysed by the HxD program. Both ANZ1 and AZ2 files were saved in the jpg format.

The images below show the output of these files.

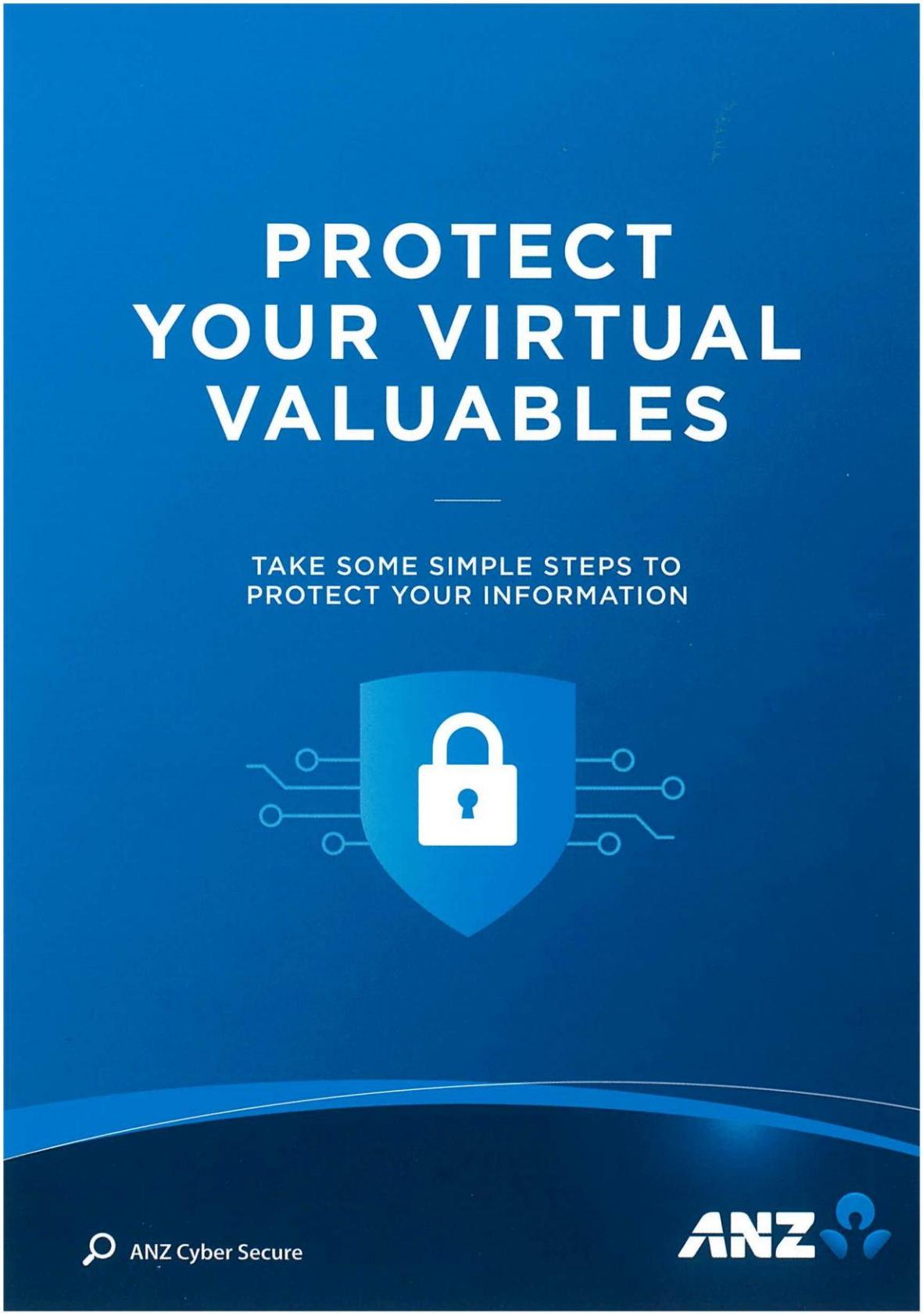


Image 3: The content of ANZ1.jpg

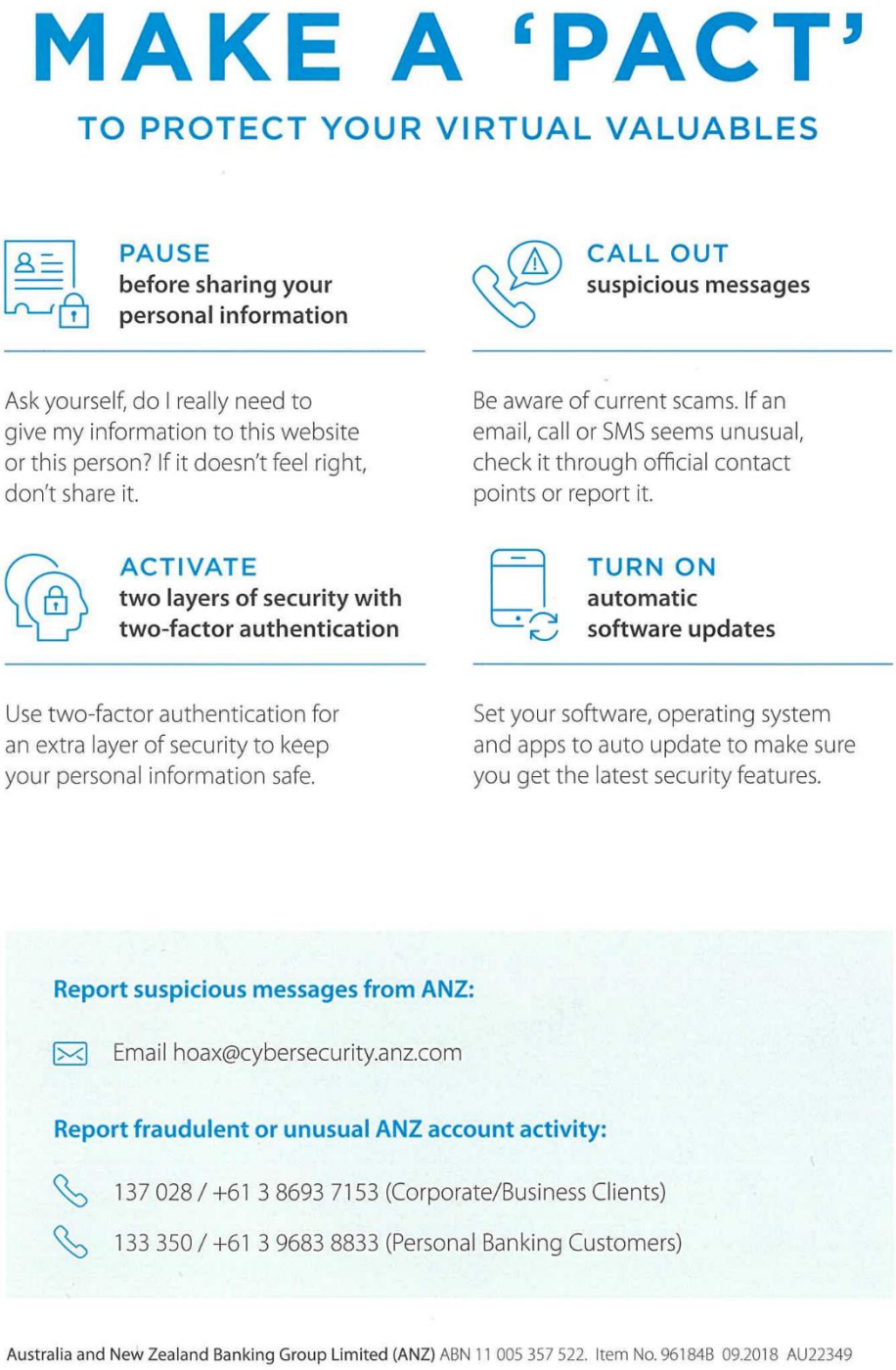


Image 4: The content of ANZ2.jpg.

V. Investigation of how-to-commit-crime.docx

The TCP stream of this document was utilised for further investigation of the content of this file.

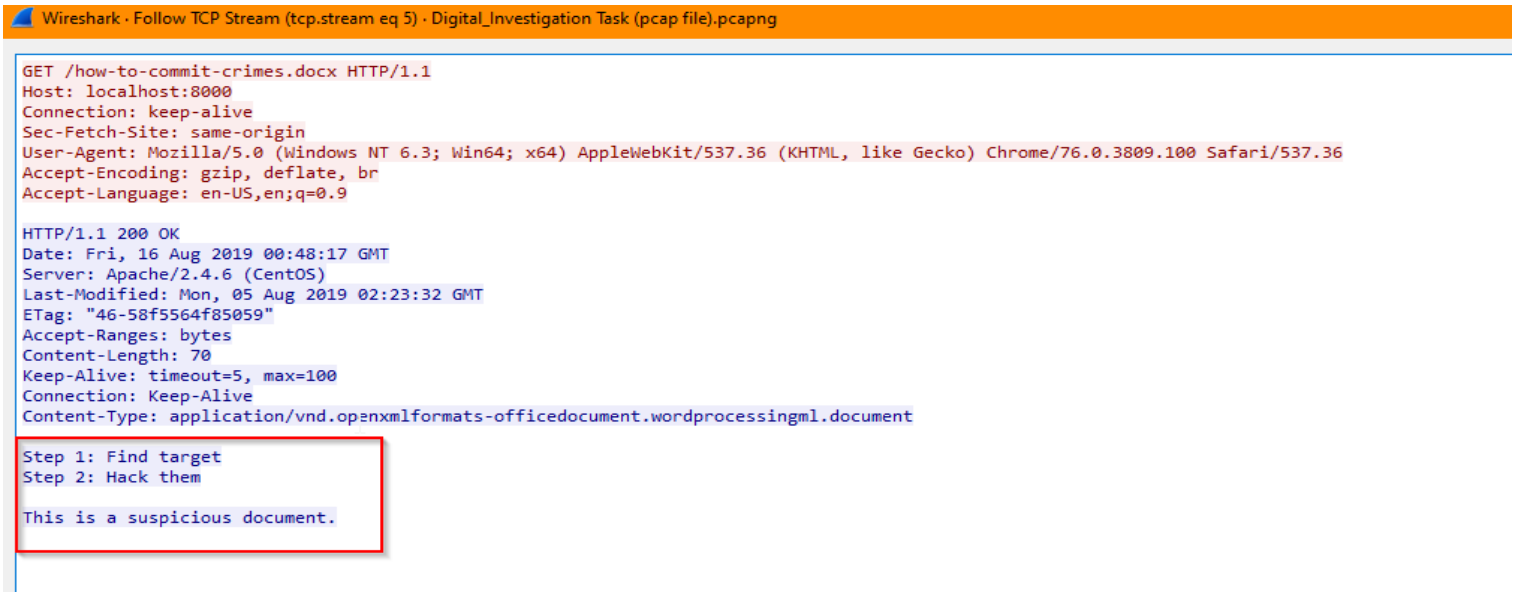


Figure 8: Content of how-to-commit-crimes.docx

The content of this file was considered suspicious when it mentioned hacking some targets within the organisation, and it was also labelled as “This is a suspicious document”. The organisation's employees must not have any authority to hack the organisation, system, or colleague unless they are penetration testers or members of the red team.

VI. Investigation of ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf

TCP stream of the ANZ_Document.pdf was followed for further investigation. The hexadecimal signature of the pdf files was recorded as 25504446 as the header and 0D0A2525454F460D0A as the footer. The extraction of all hexes from header to footer was proceeded and analysed further by the HEX program. Image 3 below shows the result.

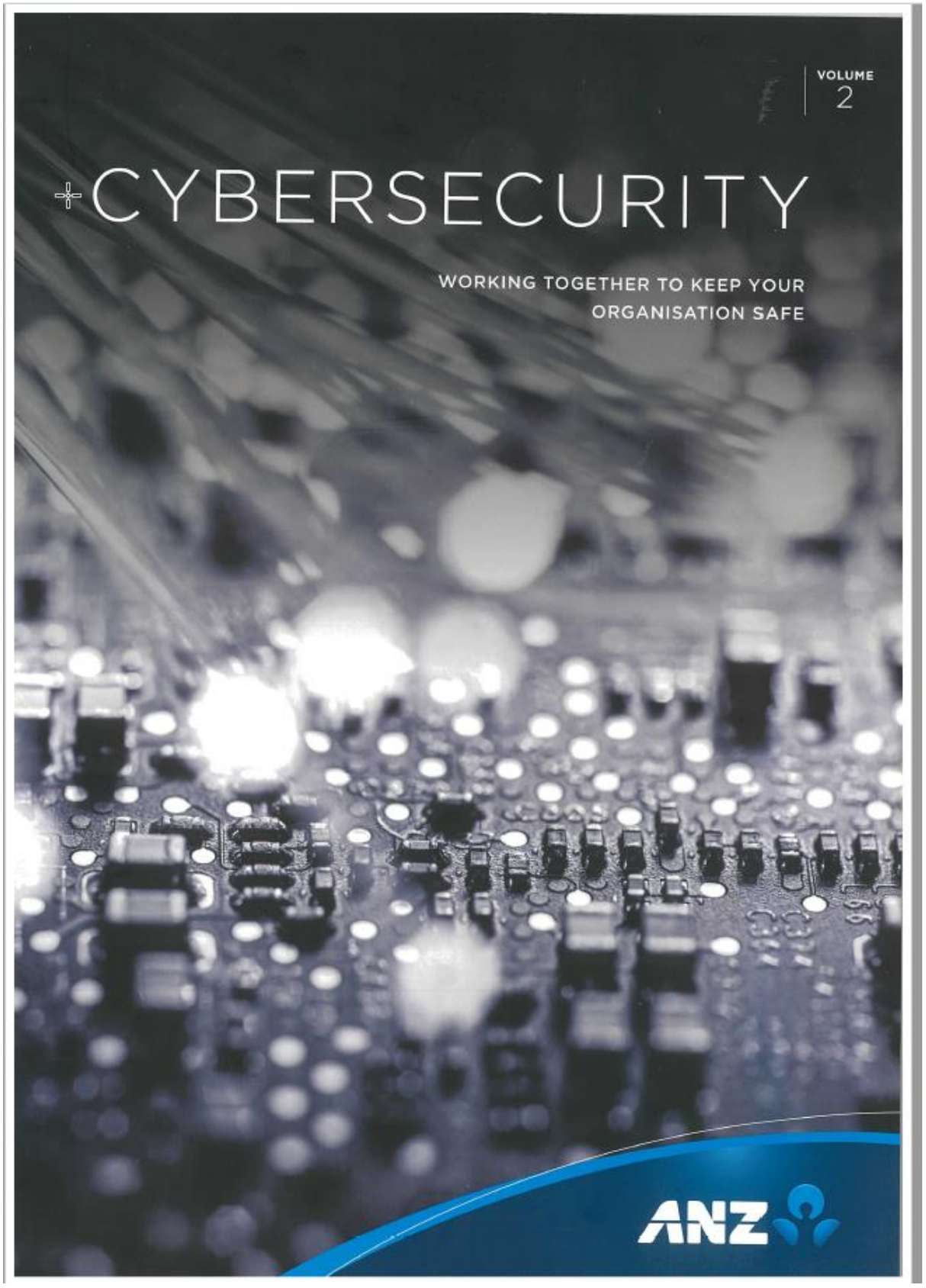
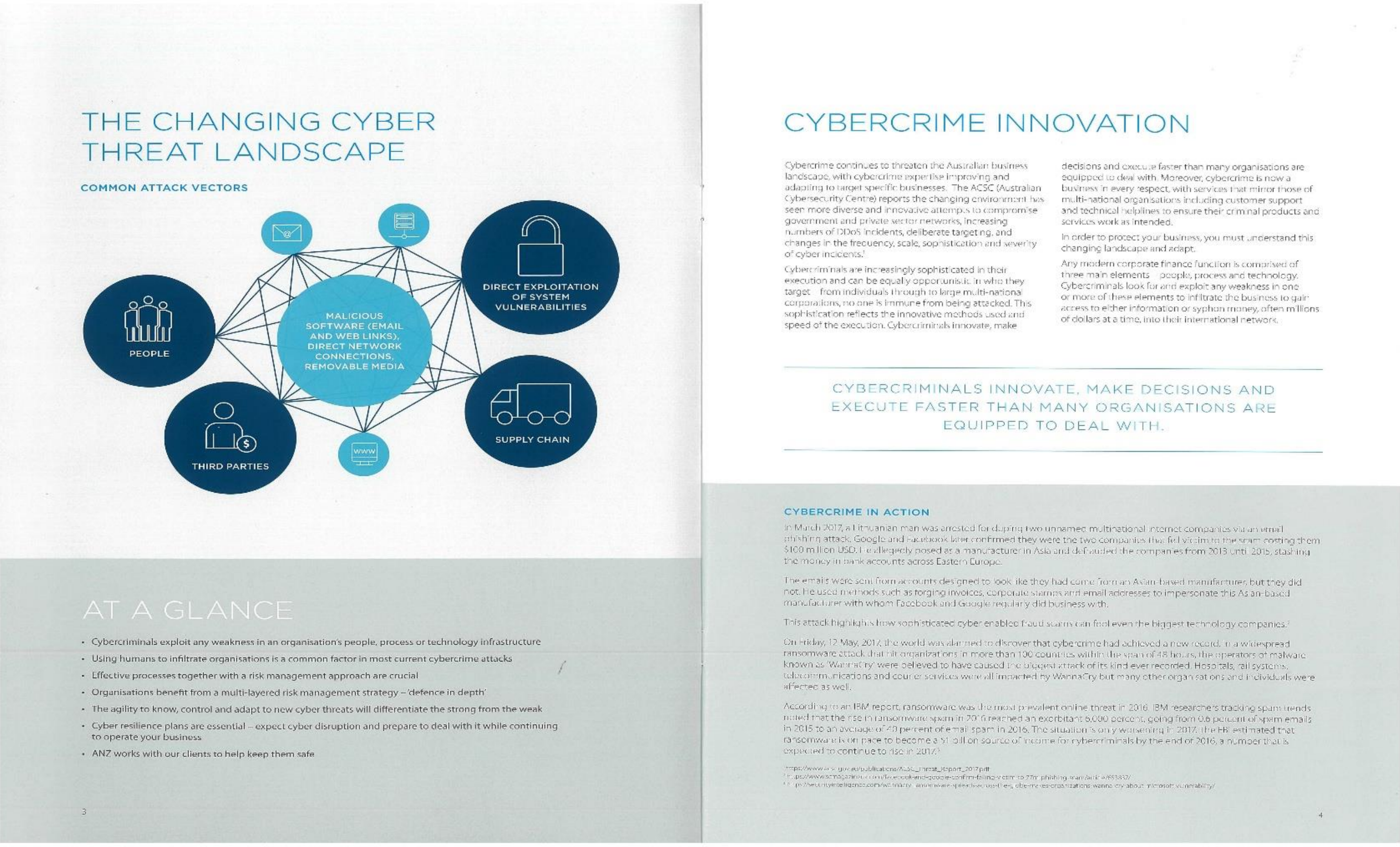


Image 5: The Content of ANZ_Document.pdf



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 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

3

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 helplines 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 syphon 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 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 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.[2]

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 organizations 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, rail 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 researchers tracking spam trends noted that the rise in ransomware spam in 2016 reached an exorbitant 6,000 percent, going from 0.6 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.[3]

[1] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf
[2] https://www.scmagazineuk.com/facebook-and-google-confirm-falling-victim-to-77m-phishing-scam/article/653837/
[3] https://securityintelligence.com/wannacry-ransomware-spreads-across-the-globe-makes-organizations-wanna-cry-about-microsoft-vulnerability/

4

Image 6: The Content of ANZ_Document2.pdf

More suspicious stuff good job!

Image 7: The Content of evil.pdf

A similar procedure was applied to investigate the ANZ_Document2.pdf and evil.pdf. However, the hexadecimal of Anz_Document2.pdf was very long, so I copied the whole content and passed it into the notepad. Then, I deleted all hexes that did not lie in the header and footer of the AnZ_Document2.pdf file.

VII. Investigation of hiddenmessage2.txt

I have researched the hex signature of the txt file, which has shown any results. This means that this extension text hides the file's actual extension. This is known as the obfuscation method, making the simple file challenging to understand or recognise.

The following stream TCP of this file was conducted for further investigation. Then, I have chosen Frame number 1337, which contains the actual data of the text file. After that, the “Lined based text data” on the left field was chosen to highlight the hex data on the right field. The header and footer of the text file were recorded as FFD8 and FFD9.

This hex signature was recorded as a JPEG file, so I have copied the hex content from FFD8 to FFD9 for further analysis by the HxD program. To achieve its actual content, it is crucial to save this file as a jpg extension, not a txt extension.

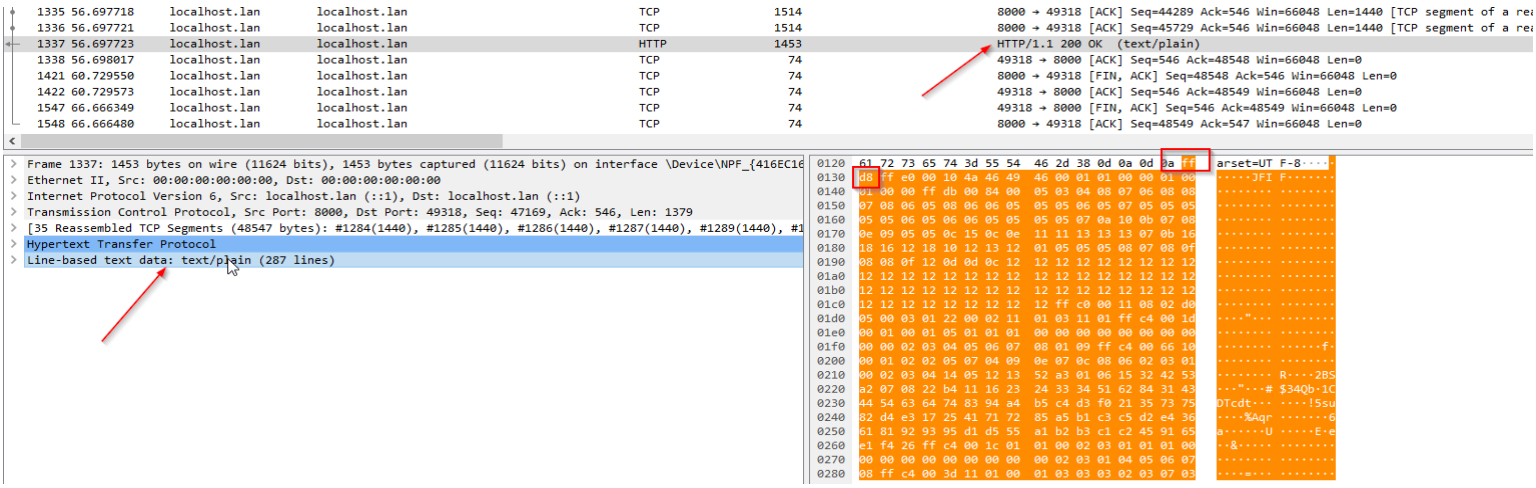


Figure 9: The Highlight Hex content of the text file.

Image 8: The actual content of hiddenmessage2.txt

VIII. Investigation atm-image.jpg

The traffic, which contains atm-image.jpg, was considered a malicious file. Only one file requested was atm-image.jpg, but the response files were two image files. The following TCP stream was filtered to gain access to this file. When I analysed the packet frame, which contains the data of atm-image.jpg, I figured that this traffic had two picture files because of two hex signatures captured.

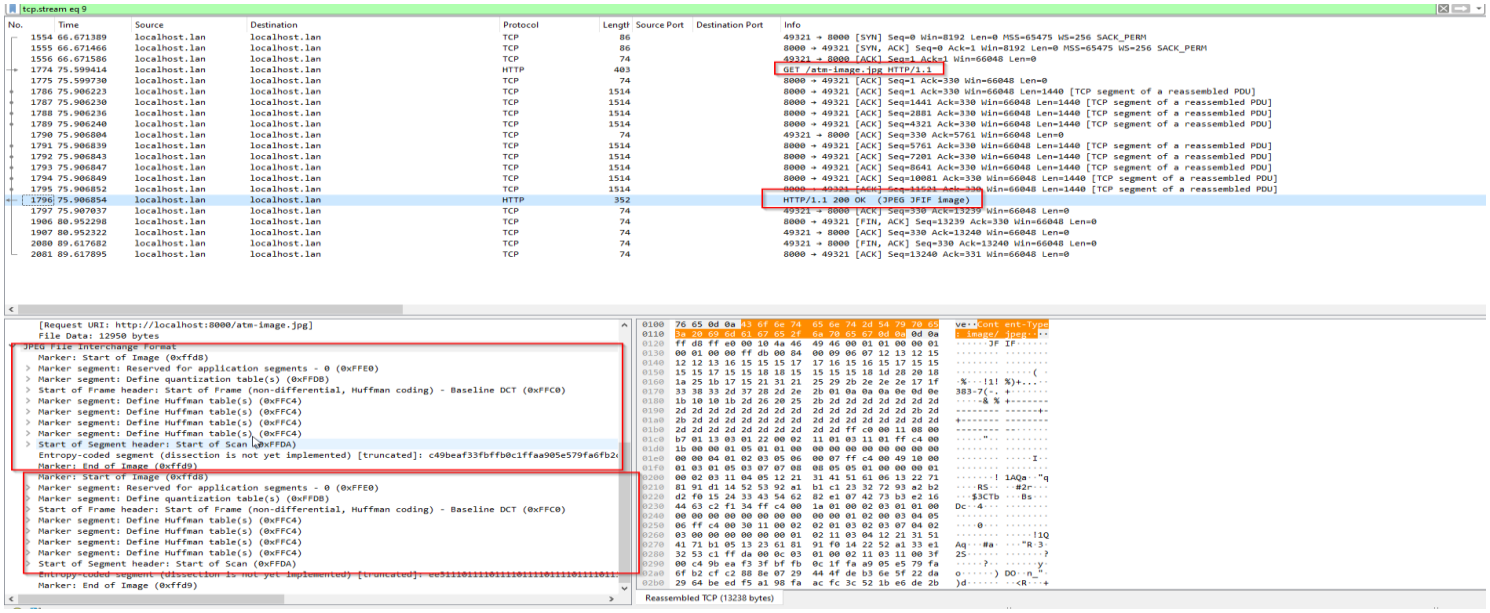


Figure 10: The response message containing two image files.

Figure 8 shows two hex signatures were recorded within this traffic, indicating that the user had downloaded the hidden malicious picture. After extracting the hex signatures of two files, the content of the hidden picture was the evidence of the malicious. Many attackers would use the techniques for hiding their malware from legitimate files to gain the victim's trust.

Image 9: Actual content of atm-image.jpg.

Image 10: Malicious image attached to the file.

IX. Investigation of broken.png file

After following the TCP stream, I investigated the broken.png file, but it did not provide any hex signature of the PNG file. My first approach was to follow the previous procedure and then save this file as broken.png. However, it showed the notification that the application does not support this file format. My second approach was to fix the broken.png using the online PNG file format, but the online application could not detect and fix the file. My last approach was to find the actual format of the PNG file from the PCAP file.

My filter was ***"http matches ".png""***which filtered and indicated any string with a PNG file. Two png files were found, which were anz-png.png and broken.png files.

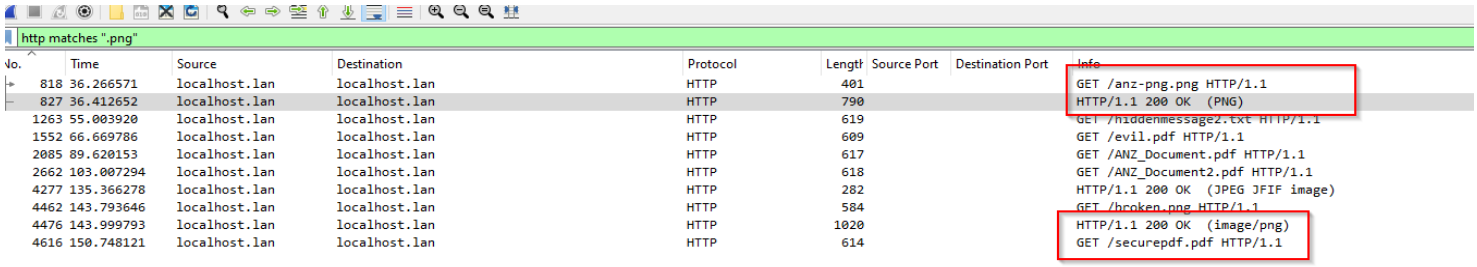


Figure 11: Identification of PNG file within the PCAP file.

Similar procedures are used to analyse the anz-png.png file with the hex signature as 89504E470D0A1A0A for the header and the 49454E44AE426082(IEND®B`,...) for the footer. The result of this PNG is displayed below.

Image 11: The content of picture anz-png.png.

This has proved that the PNG code of this file is legitimate code for extraction and producing the result. Therefore, it can be used as a base for comparison of the code of the broken.png.

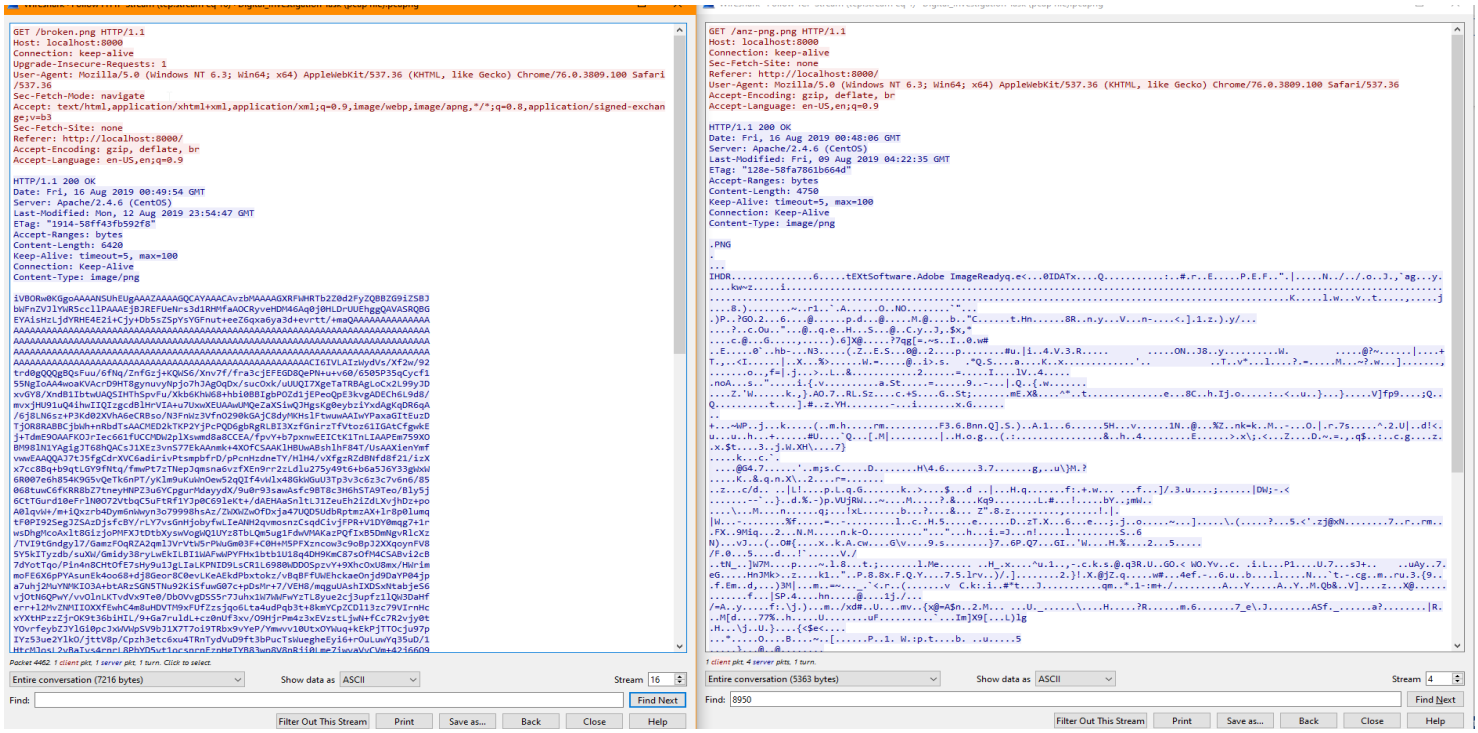


Image 12 compares ASCII codes between broken.png on the left-hand side and anz-png.png on the right-hand side.

Based on Image 10, the ASCII codes of the two PNG files are entirely different, indicating that this is another format different from the PNG format. Or the strings have been encoded by the algorithm.

After researching the Internet, I have found that BASE64 would be used to encode the binary data for storage or transfer over the media, which only deals with ASCII text. The BASE64 encryption of the png example was researched to compare with the broke.png file.


bitmap.txt

YU8kWgOeWJCQktEAoUkJvovQqvYYuVbARkkBCiSEhqNiRRQXWgooFK7IqYlsLIIsNCxYWwd4fFlSUdbFgQ+VNEkBXv
/fe906+uffPmTNnzjmZO7kDgGosWyTKQdUAyBXmi+NCA5gTUlKZpIcAkX8ogMDmSET+sbGRAMrw/Z/
y7jq0hHLFTubr5/7/
KupcnoQDABILOZ0r4eRCPgQA7soRifMBIPRCven0fBFkIowSaIphgJDNZJypYHcZpys4Um6TEBcIOQ0AJSqbLc4EQE
UWF7OAkwn9qJRDthdyBULIzZB9OHw2F/JnyKNzc6dBVrWCbJX+nZ/Mf/hMH/HJZmeOsCIXuSgFCSSiHPbM/7Mc/
1tyc6TDc5jCRuWLw+JkOcvqlj0tQsZUyOeE6dExkDUgXxVw5fYyfsKXhiUO2X/
gSAJhzQADAJTKZQdFQNaHbCLMiY4c0vtkCEJYkGHt0QRBPitBMRbliqfFDflHZ/AkwfHDzBbL55LZlEqzE/
2HfG7i81jDPpsK+QnJijjRjgJBUjRkFch3JdnxEUM2zwv5gdHDNmJpnCxm+JtjIEMcEqewwcxyJcN5YZ58ASt6iCPz
+QlhirHYFA5bHpsO5CyeZELkcJxcXlCwIi+siCdMHIofqxDlB8QN2deIcmKH7LFmXk6oTG8CuV1SED88ti8fLjZFvj
gQ5ccmKGLDNbPY4bGKGHAbEAkCQRBgAils6WAayAKC9t6GXvhN0RMC2EAMMgEP2A1phkcky3uE8BoPCsFfkHhAMjIu
QN7LAwVQ/
2VEq7jagQx5b4F8RDZ4AjkXRIAc+F0qHyUcmS0JPIYawU+zc2CsObDJ+n7SMVWHdcRgYhAxjBhCtMb1cB/cC4+EVz/
YHHF33GM4rm/2hCeETsJDwjVCF+HWVEGR+IfImSAKdMEYQ4ayS/8+O9wCenXBA3Bv6B/6xhm4HrDDneFM/
rgvnNsFar+PVTqS8bdaDvki25NRsjbZj2z1YwQqNiouI15klfq+Foq40keqFTjS82Megd/
VjwvvET9aYouxg1grdhI7jzVjDYCJHccasTbsqIxH1sZj+doYni1OHk829CP4aT720Jyyqkns6+x77D8P9YF83ox82
cMSOE00UyzI5Ocz/eFuzWOyhJwxo5m09g5wF5Xt/Yqt5Q1DvqcjjAvfdHknAPAohcrMbzo23IOOPAGA/
u6bzvQ1XPbLATjawZGKCxQ6XHYhwP8TVfik6AJDuHdZwYwcgSvwAn4gGISDGJAAUsAUWGc+XKdiMB3MBgtACSgDy8F
qsB5sBtvATrAHHAANoBmcBGfsRdABroE7cK10gxegD7wDAwiCkBAaQkd0ESPEHLFFHBF3xAcJRiKROCQFSUMyESEiR
WYjC5EypAJZj2xFapHfkSPISeQ80oncQh4gPchr5BOKoVRUEzVALdCxqDvqj0agCehkNBPNQwvRYnQpuhatRnej9eh
J9CJ6De1CX6D9GMCUMQZmjNlh7lggFoOlYhmYGJuLlWKVWDW2F2uCv/QVrAvrxT7iRJyOM3E7uF7D8EScg+fhc/
FyfD2+E6/HT+NX8Ad4H/
6VQCPoE2wJngQWYQIhkzCdUEKoJGwnHCacgc9ON+EdkUhkEC2JbvDZSyFmEWcRy4kbifuIJ4idxEfEfhKJpEuyJXmT
YkhsUj6phLSOtJt0nHSZ1E36oKSsZKTkqBSilKokVCpSqlTapXRM6bLSU6UBshrZnOxJjiFzyTPJy8g15CbyJXI3eY
CiTrGkeFMSKFmUBZS1lL2UM5S7lDfKysomyh7K45UFyvOV1yrvVz6n/
ED5I1WDakMNpE6iSqlLqTuoJ6i3qG9oNJoFzY+WSsunLaXV0k7R7tM+qNBVxqiwVLgq81SqVOpVLqu8VCWrmqv6q05

The header of this PNG file is like the header of the broken.png file, which demonstrates that the BASE64 algorithm encoded this file.

As a result, I have used the online Cyberchef program to decode the message in the picture below.

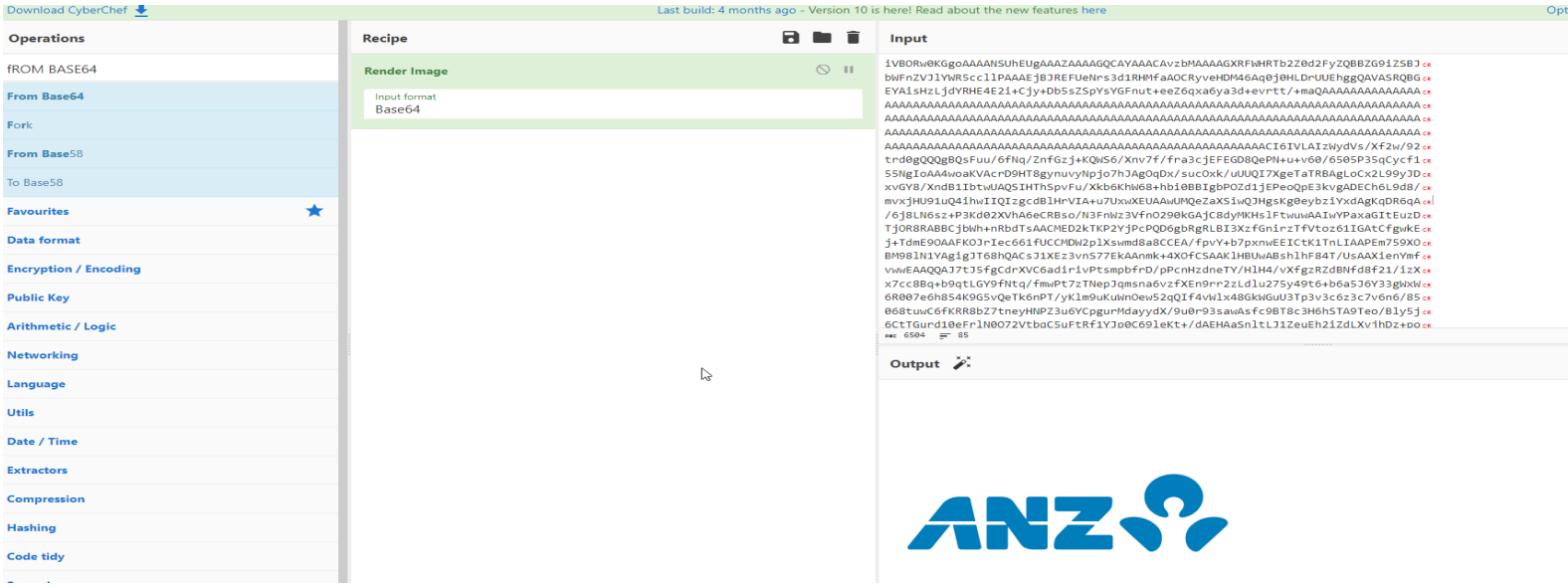


Image 13: The conversion of the BASE64 code into the image.

X. Investigation of securepdf.pdf.

After following the stream of securepdf.pdf, the hex signature of the file was analysed, and it showed that the header of the signature was 504b0304. Consequently, this was known as the signature of the zip file, not the pdf file. Therefore, the hex content was extracted, analysed, and saved in zip format by the HxD program.

However, the PDF file extraction required a password, which was analysed at the end of the message. As mentioned previously, some files within the traffic can contain more messages.

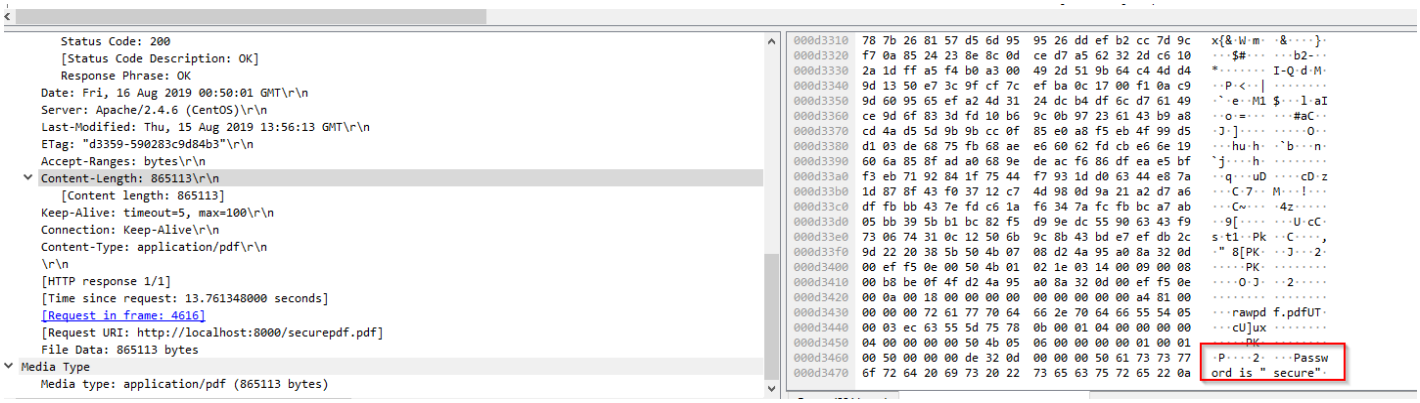


Figure 13: Password for PDF file extraction.

YOUR GUIDE TO ANZ INTERNET BANKING

TABLE OF CONTENTS

Image 14: The content of rawpdf.pdf