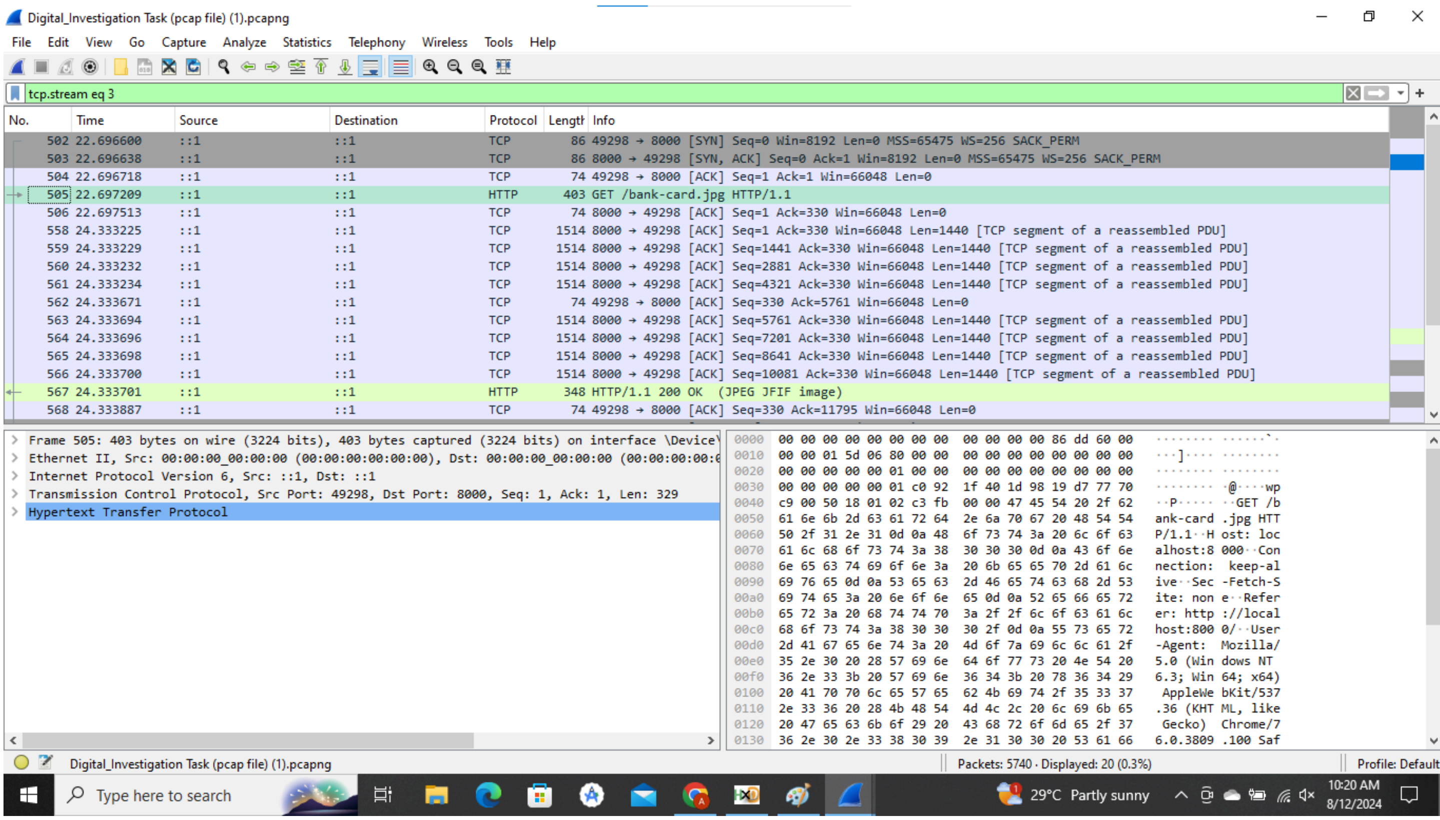
Sub-task 1:

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

Packet Capture Analysis:

I analyzed the provided packet capture file using Wireshark, a free network analysis tool. By applying the "http" filter, I was able to narrow down the traffic to display only HTTP packets. This allowed me to observe several notable HTTP GET requests, including one specifically requesting a file named **anz-logo.jpg and card.jpg .**

Further, I examined the associated TCP stream.



```
tcp.stream eq 3
```

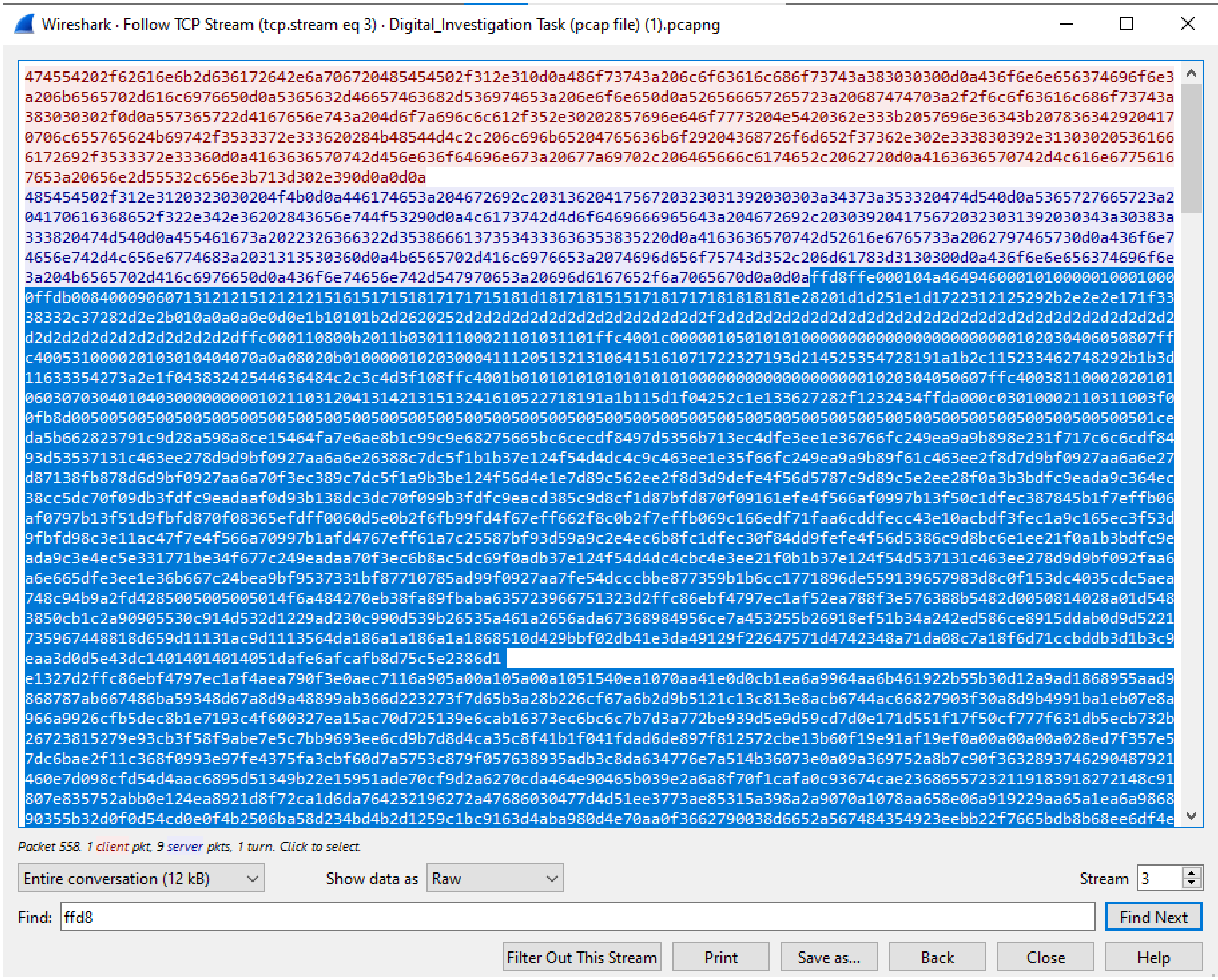
```
No.   Time       Source  Destination  Protocol Lengtl Info
  502 22.696600  ::1     ::1          TCP        86 49298 → 8000 [SYN] Seq=0 Win=8192 Len=0 MSS=65475 WS=256 SACK_PERM
  503 22.696638  ::1     ::1          TCP        86 8000 → 49298 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65475 WS=256 SACK_PERM
  504 22.696718  ::1     ::1          TCP        74 49298 → 8000 [ACK] Seq=1 Ack=1 Win=66048 Len=0
  505 22.697209  ::1     ::1          HTTP      403 GET /bank-card.jpg HTTP/1.1
  506 22.697513  ::1     ::1          TCP        74 8000 → 49298 [ACK] Seq=1 Ack=330 Win=66048 Len=0
  558 24.333225  ::1     ::1          TCP      1514 8000 → 49298 [ACK] Seq=1 Ack=330 Win=66048 Len=1440 [TCP segment of a reassembled PDU]
  559 24.333229  ::1     ::1          TCP      1514 8000 → 49298 [ACK] Seq=1441 Ack=330 Win=66048 Len=1440 [TCP segment of a reassembled PDU]
  560 24.333232  ::1     ::1          TCP      1514 8000 → 49298 [ACK] Seq=2881 Ack=330 Win=66048 Len=1440 [TCP segment of a reassembled PDU]
  561 24.333234  ::1     ::1          TCP      1514 8000 → 49298 [ACK] Seq=4321 Ack=330 Win=66048 Len=1440 [TCP segment of a reassembled PDU]
  562 24.333671  ::1     ::1          TCP        74 49298 → 8000 [ACK] Seq=330 Ack=5761 Win=66048 Len=0
  563 24.333694  ::1     ::1          TCP      1514 8000 → 49298 [ACK] Seq=5761 Ack=330 Win=66048 Len=1440 [TCP segment of a reassembled PDU]
  564 24.333696  ::1     ::1          TCP      1514 8000 → 49298 [ACK] Seq=7201 Ack=330 Win=66048 Len=1440 [TCP segment of a reassembled PDU]
  565 24.333698  ::1     ::1          TCP      1514 8000 → 49298 [ACK] Seq=8641 Ack=330 Win=66048 Len=1440 [TCP segment of a reassembled PDU]
  566 24.333700  ::1     ::1          TCP      1514 8000 → 49298 [ACK] Seq=10081 Ack=330 Win=66048 Len=1440 [TCP segment of a reassembled PDU]
  567 24.333701  ::1     ::1          HTTP      348 HTTP/1.1 200 OK  (JPEG JFIF image)
  568 24.333887  ::1     ::1          TCP        74 49298 → 8000 [ACK] Seq=330 Ack=11795 Win=66048 Len=0
```

```
> Frame 505: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface \Device\
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:0
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 49298, Dst Port: 8000, Seq: 1, Ack: 1, Len: 329
> Hypertext Transfer Protocol
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 86 dd 60 00   ········ ······`·
0010  00 00 01 5d 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 92  1f 40 1d 98 19 d7 77 70   ········ ·@····wp
0040  c9 00 50 18 01 02 c3 fb  00 00 47 45 54 20 2f 62   ··P····· ··GET /b
0050  61 6e 6b 2d 63 61 72 64  2e 6a 70 67 20 48 54 54   ank-card .jpg HTT
0060  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 6c 6f 63   P/1.1··H ost: loc
0070  61 6c 68 6f 73 74 3a 38  30 30 30 0d 0a 43 6f 6e   alhost:8 000··Con
0080  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0090  69 76 65 0d 0a 53 65 63  2d 46 65 74 63 68 2d 53   ive··Sec -Fetch-S
00a0  69 74 65 3a 20 6e 6f 6e  65 0d 0a 52 65 66 65 72   ite: non e··Refer
00b0  65 72 3a 20 68 74 74 70  3a 2f 2f 6c 6f 63 61 6c   er: http ://local
00c0  68 6f 73 74 3a 38 30 30  30 2f 0d 0a 55 73 65 72   host:800 0/··User
00d0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00e0  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT 
00f0  36 2e 33 3b 20 57 69 6e  36 34 3b 20 78 36 34 29   6.3; Win 64; x64)
0100  20 41 70 70 6c 65 57 65  62 4b 69 74 2f 35 33 37    AppleWe bKit/537
0110  2e 33 36 20 28 4b 48 54  4d 4c 2c 20 6c 69 6b 65   .36 (KHT ML, like
0120  20 47 65 63 6b 6f 29 20  43 68 72 6f 6d 65 2f 37    Gecko)  Chrome/7
0130  36 2e 30 2e 33 38 30 39  2e 31 30 30 20 53 61 66   6.0.3809 .100 Saf
```

Digital_Investigation Task (pcap file) (1).pcapng | Packets: 5740 · Displayed: 20 (0.3%) | Profile: Default

The data within the TCP stream indicated that this GET request actually downloaded many images, as evidenced by the presence of more than one sets of headers and footers for a .jpg file. The headers and footers are identified by the hex values FFD8 and FFD9, respectively, and the images are recognizable in ASCII by the 'JFIF' string near the beginning.



Wireshark · Follow TCP Stream (tcp.stream eq 3) · Digital_Investigation Task (pcap file) (1).pcapng

```
474554202f62616e6b2d636172642e6a706720485454502f312e310d0a486f73743a206c6f63616c686f73743a383030300d0a436f6e6e656374696f6e3
a206b6565702d616c6976650d0a5365632d46657463682d536974653a206e6f6e650d0a526566657265723a20687474703a2f2f6c6f63616c686f73743a
383030302f0d0a557365722d4167656e743a204d6f7a696c6c612f352e30202857696e646f7773204e5420362e333b2057696e36343b207836342920417
0706c655765624b69742f3533372e333620284b48544d4c2c206c696b65204765636b6f29204368726f6d652f37362e302e333830392e31303020536166
6172692f3533372e33360d0a4163636570742d456e636f64696e673a20677a69702c206465666c6174652c2062720d0a4163636570742d4c616e6775616
7653a20656e2d55532c656e3b713d302e390d0a0d0a
485454502f312e3120323030204f4b0d0a446174653a204672692c2031362041756720323031392030303a34373a353320474d540d0a5365727665723a2
04170616368652f322e342e36202843656e744f53290d0a4c6173742d4d6f6469666965643a204672692c2030392041756720323031392030343a30383a
333820474d540d0a455461673a2022326366322d35386661373534333636353835220d0a4163636570742d52616e6765733a2062797465730d0a436f6e7
4656e742d4c656e6774683a2031313530360d0a4b6565702d416c6976653a2074696d656f75743d352c206d61783d3130300d0a436f6e6e656374696f6e
3a204b6565702d416c6976650d0a436f6e74656e742d547970653a20696d6167652f6a7065670d0a0d0affd8ffe000104a46494600010100000100010000
0ffdb0084000906071312121512121215161517151817171715181d181718151517181717181818181e28201d1d251e1d1722312125292b2e2e2e171f33
38332c37282d2e2b010a0a0a0e0d0e1b10101b2d2620252d2d2d2d2d2d2d2d2d2d2d2d2d2f2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2
d2d2d2d2d2d2d2d2d2d2dffc000110800b2011b03011100021101031101ffc4001c000001050101010000000000000000000000000102030406050807ff
c400531000020103010404070a0a08020b010000010203000411120513213106415161071722327193d214525354728191a1b2c115233462748292b1b3d
11633354273a2e1f04383242544636484c2c3c4d3f108ffc4001b01010101010101010100000000000000000001020304050607ffc40038110002020101
0603070304010403000000000102110312041314213151324161052271819 1a1b115d1f04252c1e133627282f1232434ffda000c03010002110311003f0
0fb8d00500500500500500500500500500500500500500500500500500500500500500500500500500500500500500500500500500500500500501ce
da5b662823791c9d28a598a8ce15464fa7e6ae8b1c99c9e68275665bc6cecdf8497d5356b713ec4dfe3ee1e36766fc249ea9a9b898e231f717c6c6cdf84
93d53537131c463ee278d9d9bf0927aa6a6e26388c7dc5f1b1b37e124f54d4dc4c9c463ee1e35f66fc249ea9a9b89f61c463ee2f8d7d9bf0927aa6a6e27
d87138fb878d6d9bf0927aa6a70f3ec389c7dc5f1a9b3be124f56d4e1e7d89c562ee2f8d3d9defe4f56d5787c9d89c5e2ee28f0a3b3bdfc9eada9c364ec
38cc5dc70f09db3fdfc9eadaaf0d93b138dc3dc70f099b3fdfc9eacd385c9d8cf1d87bfd870f09161efe4f566af0997b13f50c1dfec387845b1f7effb06
af0797b13f51d9fbfd870f08365efdff0060d5e0b2f6fb99fd4f67eff662f8c0b2f7effb069c166edf71faa6cddfecc43e10acbdf3fec1a9c165ec3f53d
9fbfd98c3e11ac47f7e4f566a70997b1afd4767eff61a7c25587bf93d59a9c2e4ec6b8fc1dfec30f84dd9fefe4f56d5386c9d8bc6e1ee21f0a1b3bdfc9e
ada9c3e4ec5e331771be34f677c249eadaa70f3ec6b8ac5dc69f0adb37e124f54d4dc4cbc4e3ee21f0b1b37e124f54d537131c463ee278d9d9bf092faa6
a6e665dfe3ee1e36b667c24bea9bf9537331bf87710785ad99f0927aa7fe54dcccbbe877359b1b6cc1771896de559139657983d8c0f153dc4035cdc5aea
748c94b9a2fd4285005005005014f6a484270eb38fa89fbaba635723966751323d2ffc86ebf4797ec1af52ea788f3e576388b5482d0050814028a01d548
3850cb1c2a90905530c914d532d1229ad230c990d539b26535a461a2656ada67368984956ce7a453255b26918ef51b34a242ed586ce8915ddab0d9d5221
735967448818d659d11131ac9d1113564da186a1a186a1a1868510d429bbf02db41e3da49129f22647571d4742348a71da08c7a18f6d71ccbddb3d1b3c9
eaa3d0d5e43dc14014014014051dafe6afcafb8d75c5e2386d1
e1327d2ffc86ebf4797ec1af4aea790f3e0aec7116a905a00a105a00a1051540ea1070aa41e0d0cb1ea6a9964aa6b461922b55b30d12a9ad1868955aad9
868787ab667486ba59348d67a8d9a48899ab366d223273f7d65b3a28b226cf67a6b2d9b5121c13c813e8acb6744ac66827903f30a8d9b4991ba1eb07e8a
966a9926cfb5dec8b1e7193c4f600327ea15ac70d725139e6cab16373ec6bc6c7b7d3a772be939d5e9d59cd7d0e171d551f17f50cf777f631db5ecb732b
26723815279e93cb3f58f9abe7e5c7bb9693ee6cd9b7d8d4ca35c8f41b1f041fdad6de897f812572cbe13b60f19e91af19ef0a00a00a00a028ed7f357e5
7dc6bae2f11c368f0993e97fe4375fa3cbf60d7a5753c879f057638935adb3c8da634776e7a514b36073e0a09a369752a8b7c90f363289374629048792 1
460e7d098cfd54d4aac6895d51349b22e15951ade70cf9d2a6270cda464e90465b039e2a6a8f70f1cafa0c93674cae23686557232119183918272148c91
807e835752abb0e124ea8921d8f72ca1d6da764232196272a47686030477d4d51ee3773ae85315a398a2a9070a1078aa658e06a919229aa65a1ea6a9868
90355b32d0f0d54cd0e0f4b2506ba58d234bd4b2d1259c1bc9163d4aba980d4e70aa0f3662790038d6652a567484354923eebb22f7665bdb8b68ee6df4e
```

Packet 558. 1 client pkt, 9 server pkts, 1 turn. Click to select.

Entire conversation (12 kB)

Show data as Raw

Stream 3

Find: ffd8

and the extracted image is for anz-logo.jpg is given below

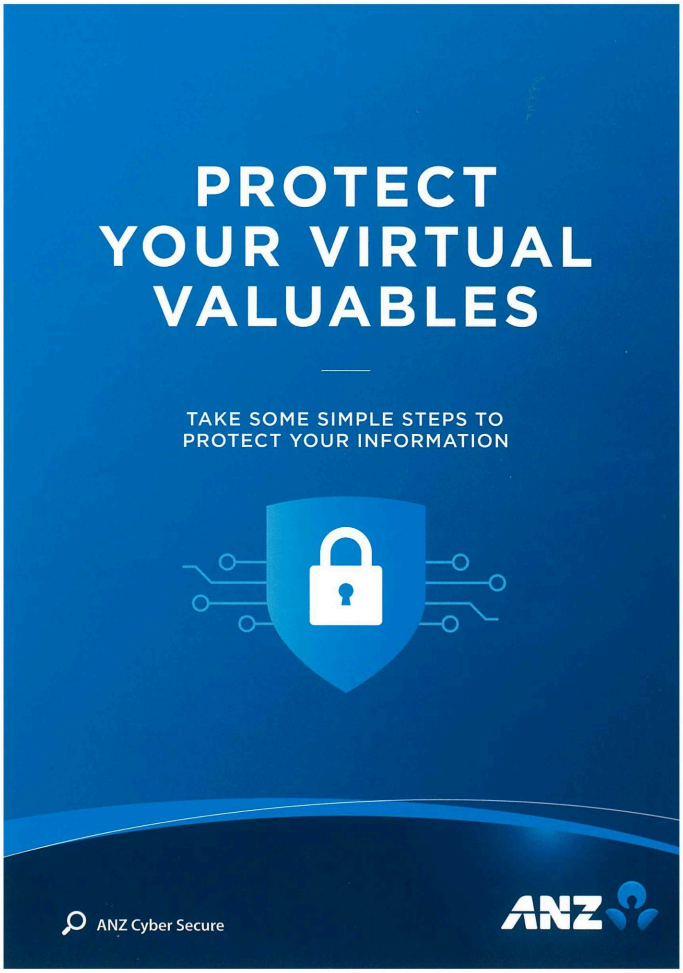
anz–logo.jpg

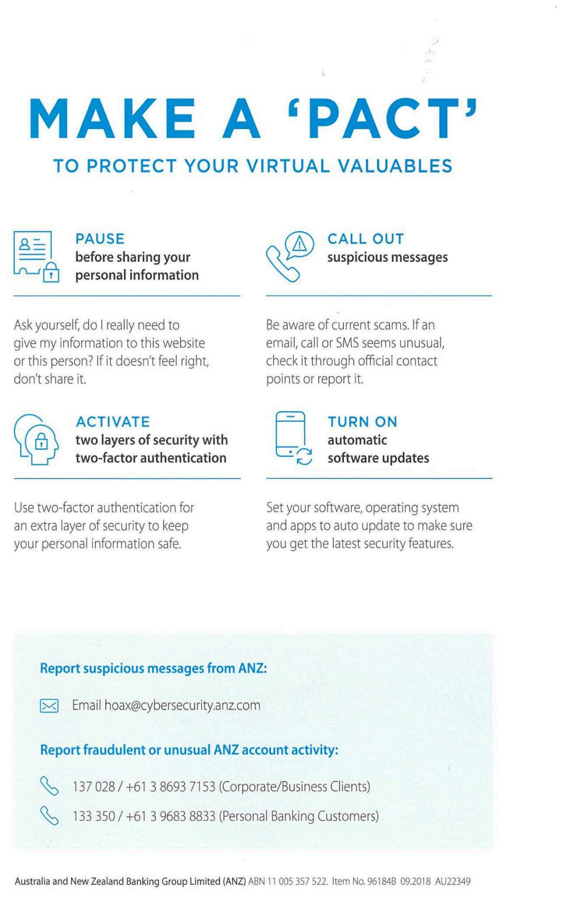
and for the second image i followed the same process and the image for card.jpg is given below

card.jpg

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.*


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



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

ANZ1.jpg **ANZ2.jpg**

There are many headers and footers in these images

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.*

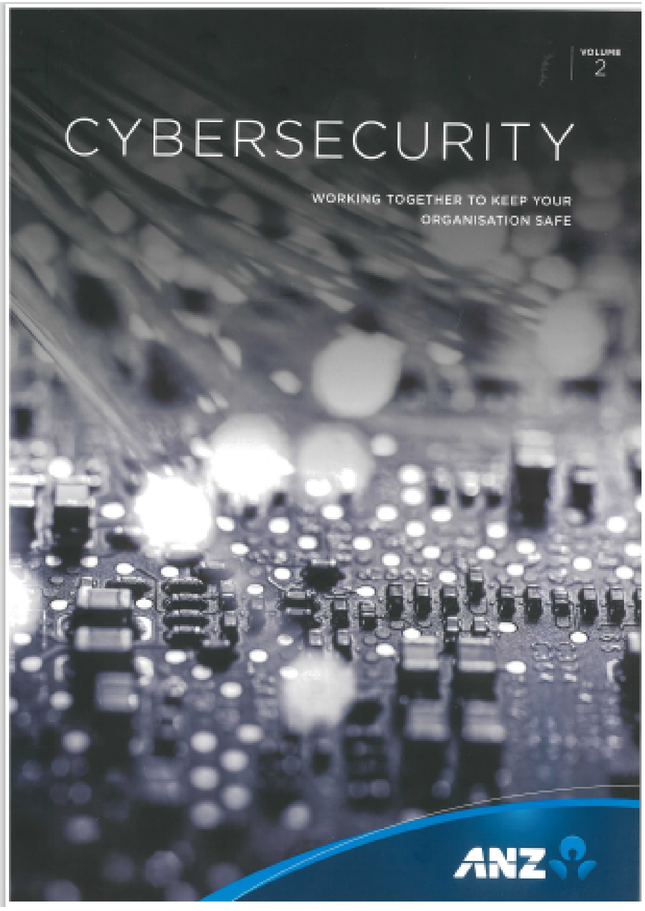
The contents of this docx file is given below

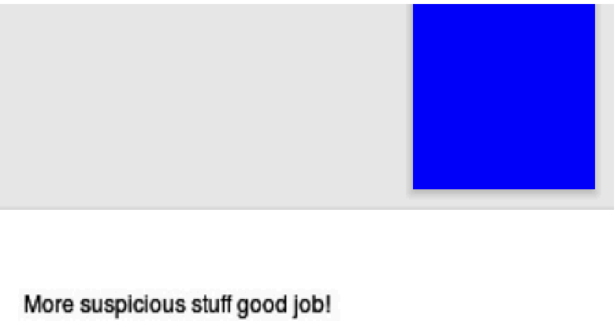
Step 1: Find target
Step 2: Hack them

This is a suspicious document.

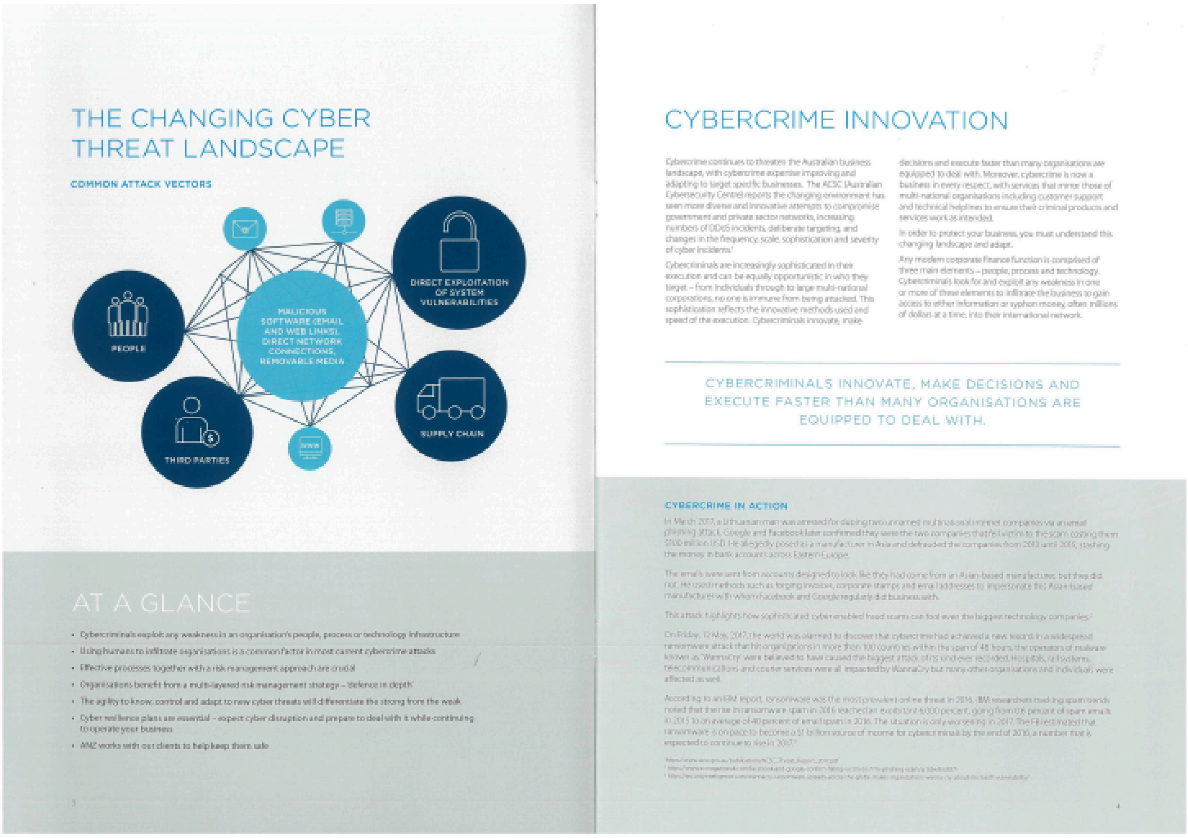
Sub-task 4:

- *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.*




More suspicious stuff good job!

ANZ_Document.pdf ***Evil.pdf***



THE CHANGING CYBER THREAT LANDSCAPE

COMMON ATTACK VECTORS

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

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] [illegible]
[3] [illegible]

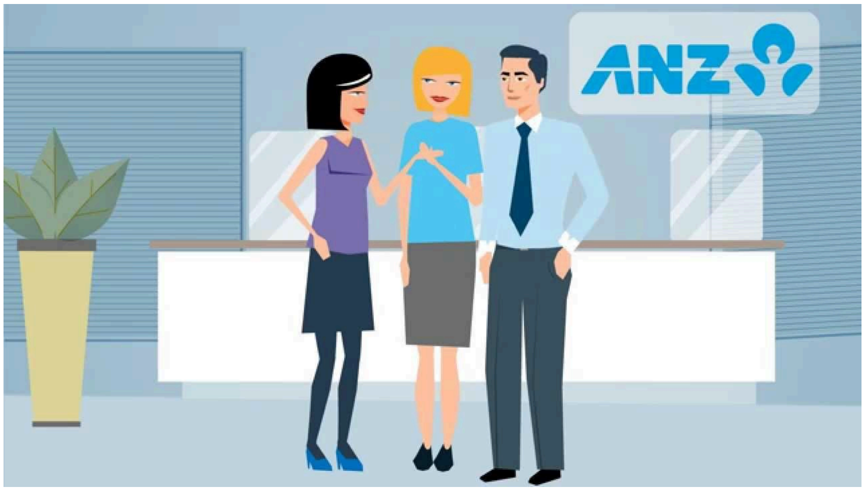
4

ANZ_Document2.pdf

Sub-task 5:

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

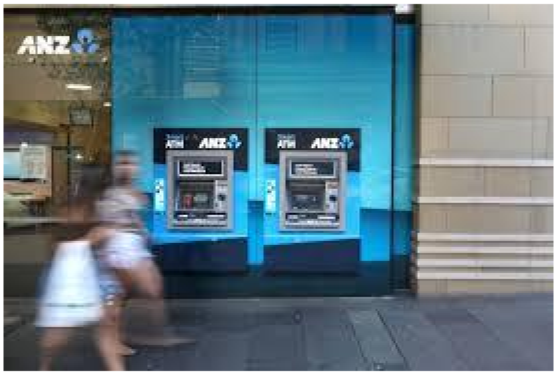
That's not a txt file but a jpg file so they are trying to deceive us b showing that they viewed the txt file but actually they say the jpg which is given below



hiddentext2

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.*

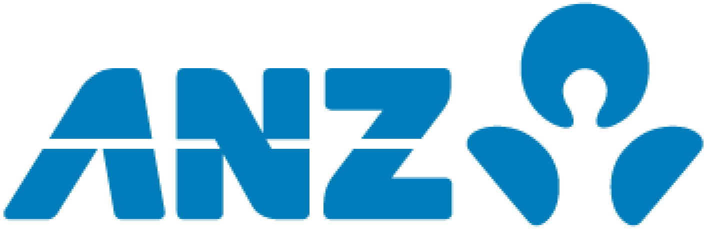


atm-image.jpg

The headers and footers are identified by the hex values FFD8 and FFD9, respectively, and the image is recognizable in ASCII by the ‘JFIF’ string near the beginning.

Sub-task 7:

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



broken.png

There is no png file so i view the data in ascii form then decode it from an online toll 64 bit decoder then paste the data hxd and view this image.

Sub-task 8:

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

The password is secure for the pdf file and we retrieve two images from this secured.pdf 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 prompted for a password. The password ‘secure’ shown in the tcp stream worked, and the PDF opened. It was the first two pages to a guide for internet banking.

YOUR GUIDE TO
ANZ INTERNET BANKING

TABLE OF CONTENTS