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.

Time

First packet:	2019-08-15 18:47:34
Last packet:	2019-08-15 18:50:26
Elapsed:	00:02:51

Capture

Hardware:	Intel(R) Core(TM) i7-5700HQ CPU @ 2.70GHz (with SSE4.2)
OS:	64-bit Windows 8.1, build 9600
Application:	Dumpcap (Wireshark) 3.0.3 (v3.0.3-0-g6130b92b0ec6)

Interfaces

- *This image shows the timeline of the when the pcap was captured. The capture lasted for 2mins 51secs.*

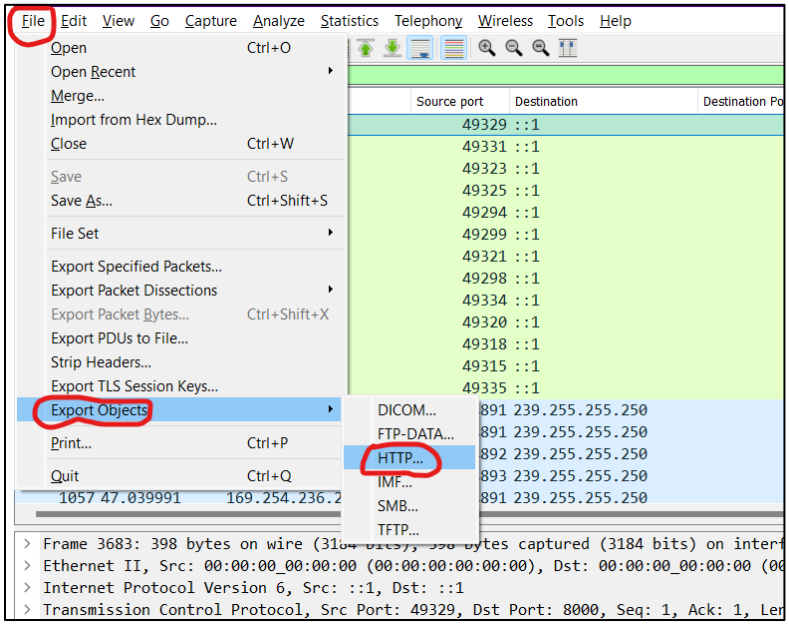
Sub-task 1:

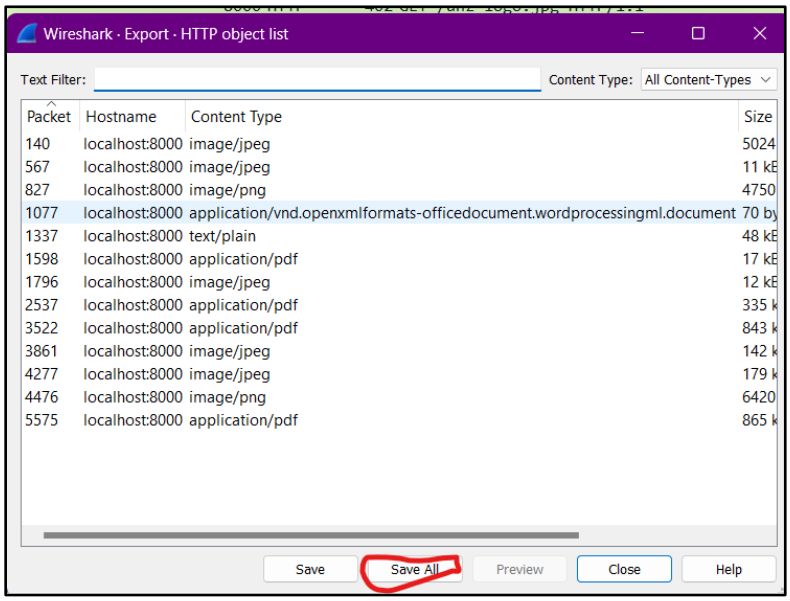
http.request

No.	Time	Source	Source port	Destination	Destination Port	Protocol	Length	Info
3683	119.921282	::1	49329	::1	8000	HTTP	398	GET /ANZ1.jpg HTTP/1.1
4074	132.661982	::1	49331	::1	8000	HTTP	398	GET /ANZ2.jpg HTTP/1.1
2085	89.620153	::1	49323	::1	8000	HTTP	617	GET /ANZ_Document.pdf HTTP/1.1
2662	103.007294	::1	49325	::1	8000	HTTP	618	GET /ANZ_Document2.pdf HTTP/1.1
131	6.132470	::1	49294	::1	8000	HTTP	402	GET /anz-logo.jpg HTTP/1.1
818	36.266571	::1	49299	::1	8000	HTTP	401	GET /anz-png.png HTTP/1.1
1774	75.599414	::1	49321	::1	8000	HTTP	403	GET /atm-image.jpg HTTP/1.1
505	22.697209	::1	49298	::1	8000	HTTP	403	GET /bank-card.jpg HTTP/1.1
4462	143.793646	::1	49334	::1	8000	HTTP	584	GET /broken.png HTTP/1.1
1552	66.669786	::1	49320	::1	8000	HTTP	609	GET /evil.pdf HTTP/1.1
1263	55.003920	::1	49318	::1	8000	HTTP	619	GET /hiddenmessage2.txt HTTP/1.1
1051	46.737160	::1	49315	::1	8000	HTTP	389	GET /how-to-commit-crimes.docx HTTP/1.1
4616	150.748121	::1	49335	::1	8000	HTTP	614	GET /securepdf.pdf HTTP/1.1

Time (format as specified)

- *anz-logo.jpg and bank-card.jpg are two images that show up in the user's network traffic.*
  Ans: I did a "HTTP.Request" and then clicked on file → export objects → HTTP





I was able to download every file I needed for this project.

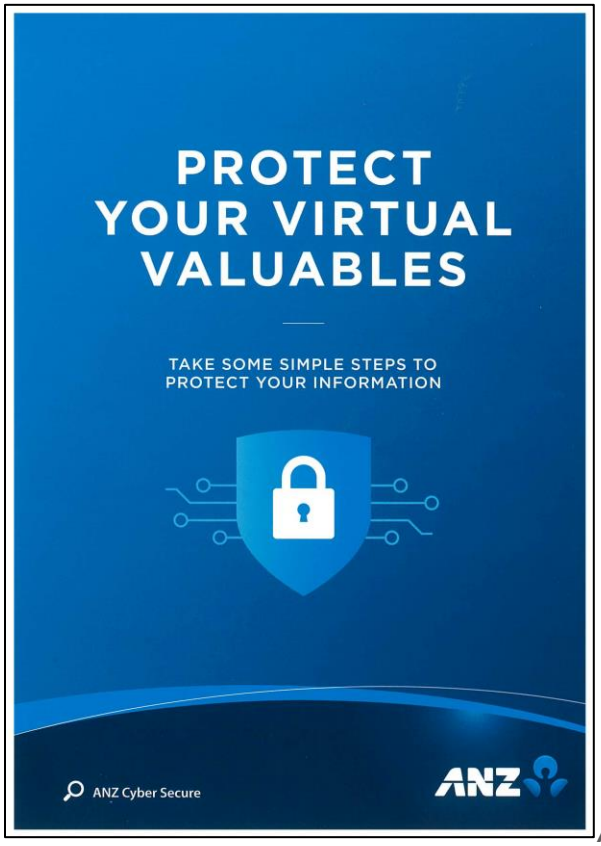
- *Extract these images from the pcap file and attach them to your report.*

Bank card

ANZ -logo

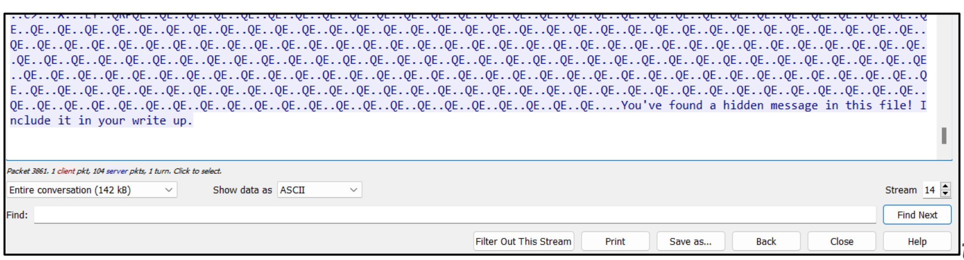
Sub-task 2:

- *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

ANZ1.jpg

ANZ2.jpg



tcp stream for ANZ1.jpg

I was able to find "You've found a hidden message in this file! Include it in your write up." When you scroll down after you've opened the tcp stream

Sub-task 3:

- *The user downloaded a suspicious document called "how-to-commit-crimes.docx"*

I tried opening the document but it wasn't opening and the I went back to wireshark to analyze the packet and below is what I found.

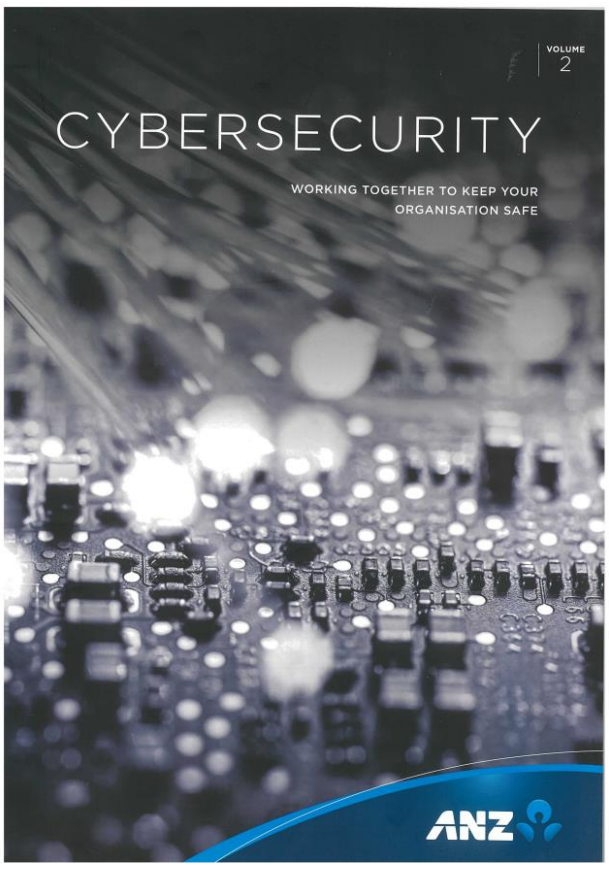
- *Find the contents of this file and include it in your report.*

```
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 Sa
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.
```

I made use of the tcp stream and this is what I found.

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 have included them in the images below



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

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]

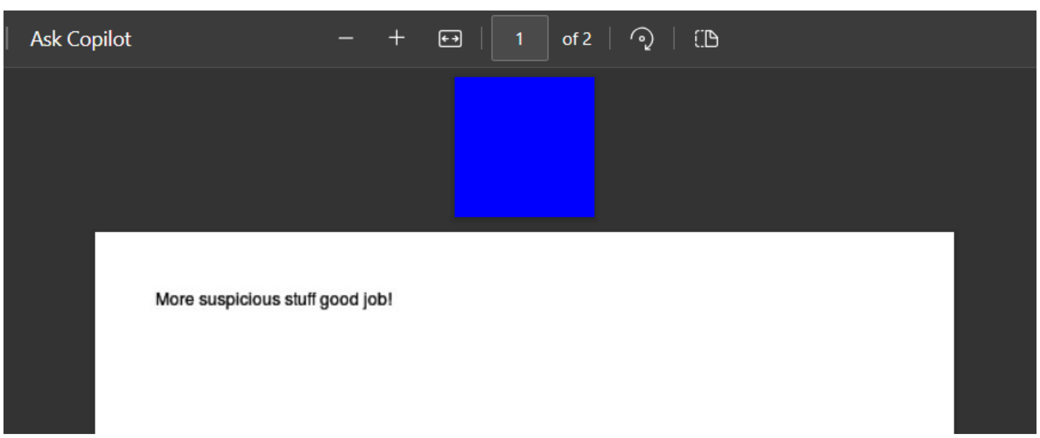
On Friday, 12 May, 2017, the world was alarmed to discover that cybercrime had achieved a new record. In a widespread ransomware attack that hit organizations in more than 100 countries within the span of 48 hours, the operators of malware known as 'WannaCry' were believed to have caused the biggest 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]

3

4

ANZ_Document2.pdf



Evil.pdf

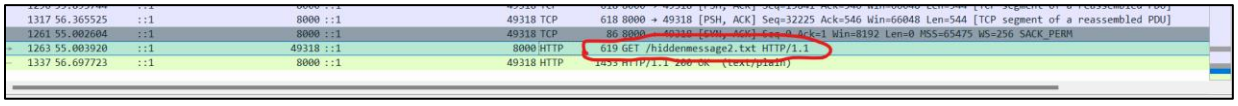
Sub-task 5:

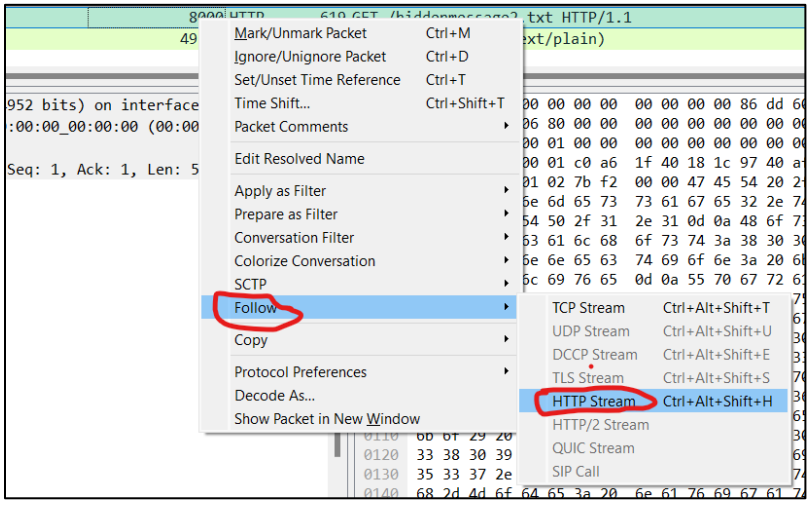
- *The user also accessed a file called "hiddenmessage2.txt"*

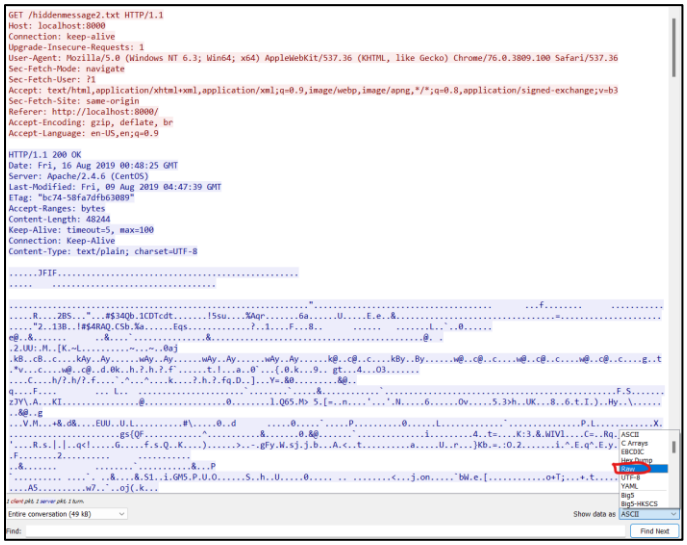
hiddenmessage2.txt

This was what I saw when I opened the "hiddenmessage2.txt" file. I had to go back to my wireshark and extract the file using HXD and from the JFIF I circled in the txt file, you can tell that it's probably a JPEG file.

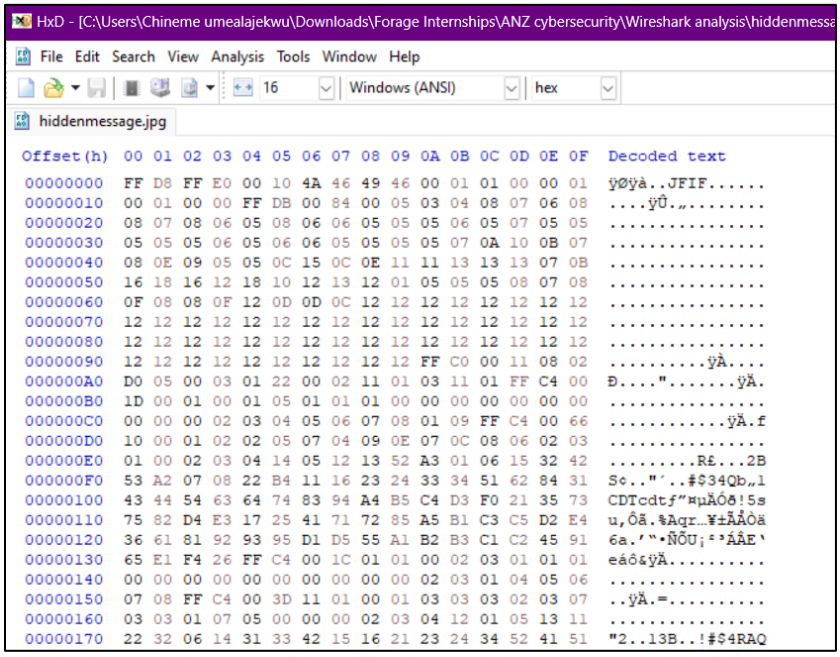
Here's the step I followed to extract the image from HXD




Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call


GET /hiddenmessage2.txt HTTP/1.1
Host: localhost:8000
Connection: keep-alive
Upgrade-Insecure-Requests: 1
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
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: http://localhost:8000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
HTTP/1.1 200 OK
Date: Fri, 16 Aug 2019 00:48:25 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Fri, 09 Aug 2019 04:47:39 GMT
ETag: "bc74-58fa7dfb63089"
Accept-Ranges: bytes
Content-Length: 48244
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain; charset=UTF-8

Change it to RAW to be able to transport to HXD
And search for 'FFD8' and 'FFD9' and then copy from both ends



Here is the Hex file and im going to save it as .jpg

- *What is the contents of this file? Include it in your report*

Here is the content of the file

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.*

Sub-task 7:

- *The network traffic shows that the user accessed the image "broken.png"*
  Yes, the user accessed it.
- *Extract and include the image in your report.*
  I was able to extract the file initially and then it wasn't opening. I went back to wireshark and opened the http stream of the packet and changed it to RAW file. I was able to figure out its in BASE64 encoding and I needed to decode it.
  I opened the website base64decode.org and I uploaded the file and was able to decode it on the website. After decoding, I was able to download the picture.

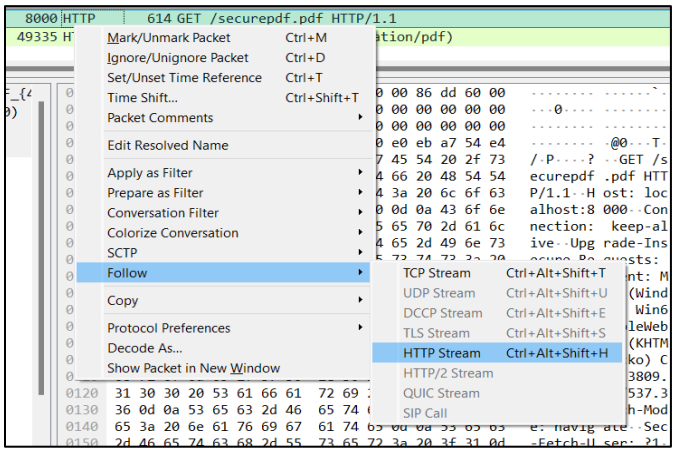
Here is an image of the file

Sub-task 8:

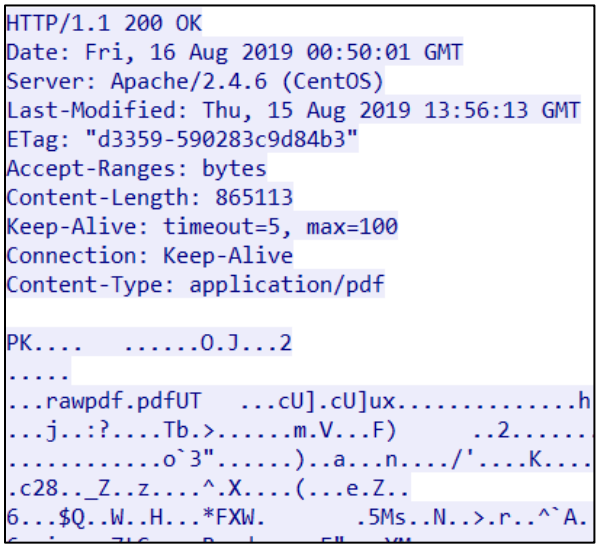
- *The user accessed one more document called securepdf.pdf*

→	4616	2019-08-16 00:50:05.048110	::1	49335	::1	8000	HTTP	614	GET /securepdf.pdf HTTP/1.1
←	5575	2019-08-16 00:50:18.809458	::1	8000	::1	49335	HTTP	554	HTTP/1.1 200 OK (application/pdf)

- *Access this document include an image of the pdf in your report. Detail the steps to access it.*



I followed the HTTP stream and I changed it from ASCII to RAW inorder for it to be ingested in HXD.



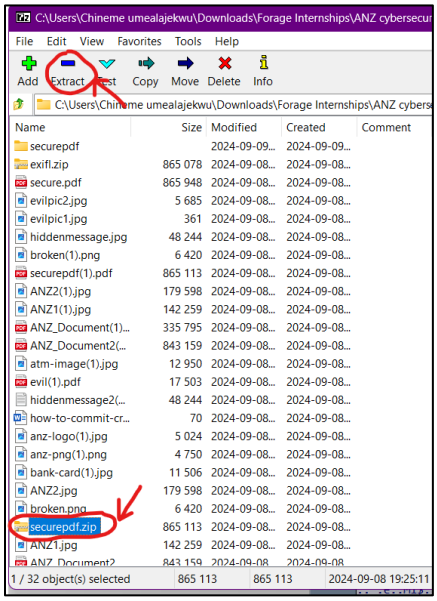
From this image I could tell that it is a .zip file as it started with PK. But with further analysis I was able to also see rawpdf.pdf wehich indicates the actuall pdf doc that is inside the zipped file.

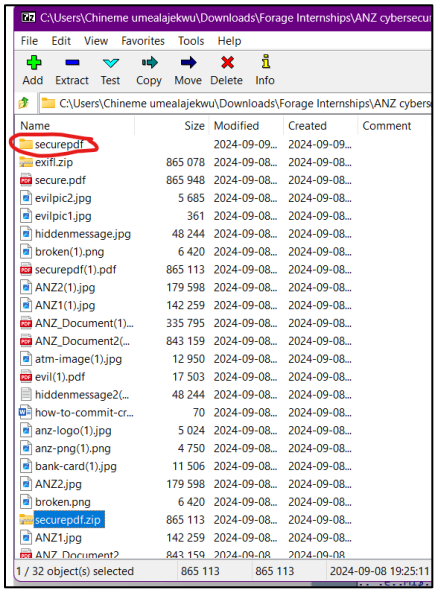
I saved this file in my device just like I did for others in the beginning

I had to change it to the .zip file inorder for it to run. Using your regular pdf reader wouldn't catch it. I made use of 7zip files and was able to extract the file.

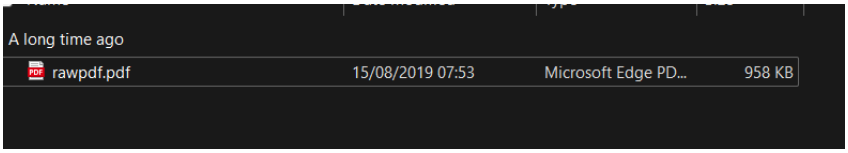
In addition to this, the zip file was passworded and we can see the password when we scroll down to the last tcp stream inforamtion.

```
.+...<D./CD.7...?..W..U.h...>....V..RO.      ..v_w.....a.g.-.6..A.3..)......U^..e}.
<.F.r@C6...e.I.a..q.U!N    .....TN..da...=. ~.n..tXE8..Q.....6.%...L./.~7Q
)U..b.U.
'.....]...K.....)V........J
.........:$W....M.~O6K.x{&.W.m..&....}..
.$#..
...b2-..*.......I-Q.d.M...P.<..|......
..`.e..M1$...l.aI..o.=......#aC...J.].........O.....hu.h..`b...n.`j....h..........
.!......C~....4z.......9[.......U.cC.s.t1..Pk..C....,." 8[PK...J...2
.....PK......     ......O.J...2
.....
.................rawpdf.pdfUT....cU]ux.............PK..........P....2
...Password is "secure"
```





Here is the extracted file



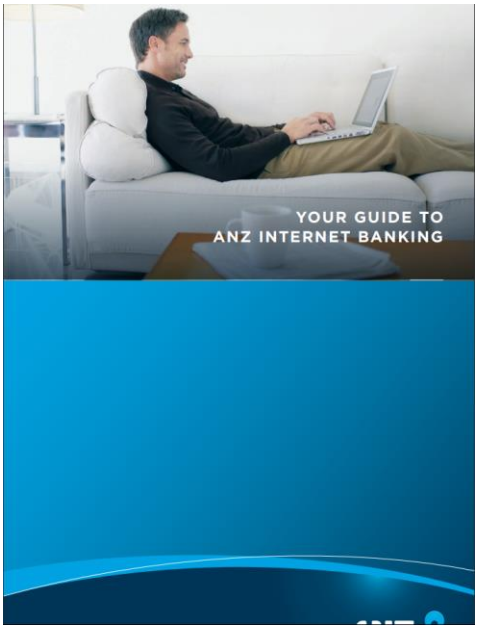


TABLE OF CONTENTS