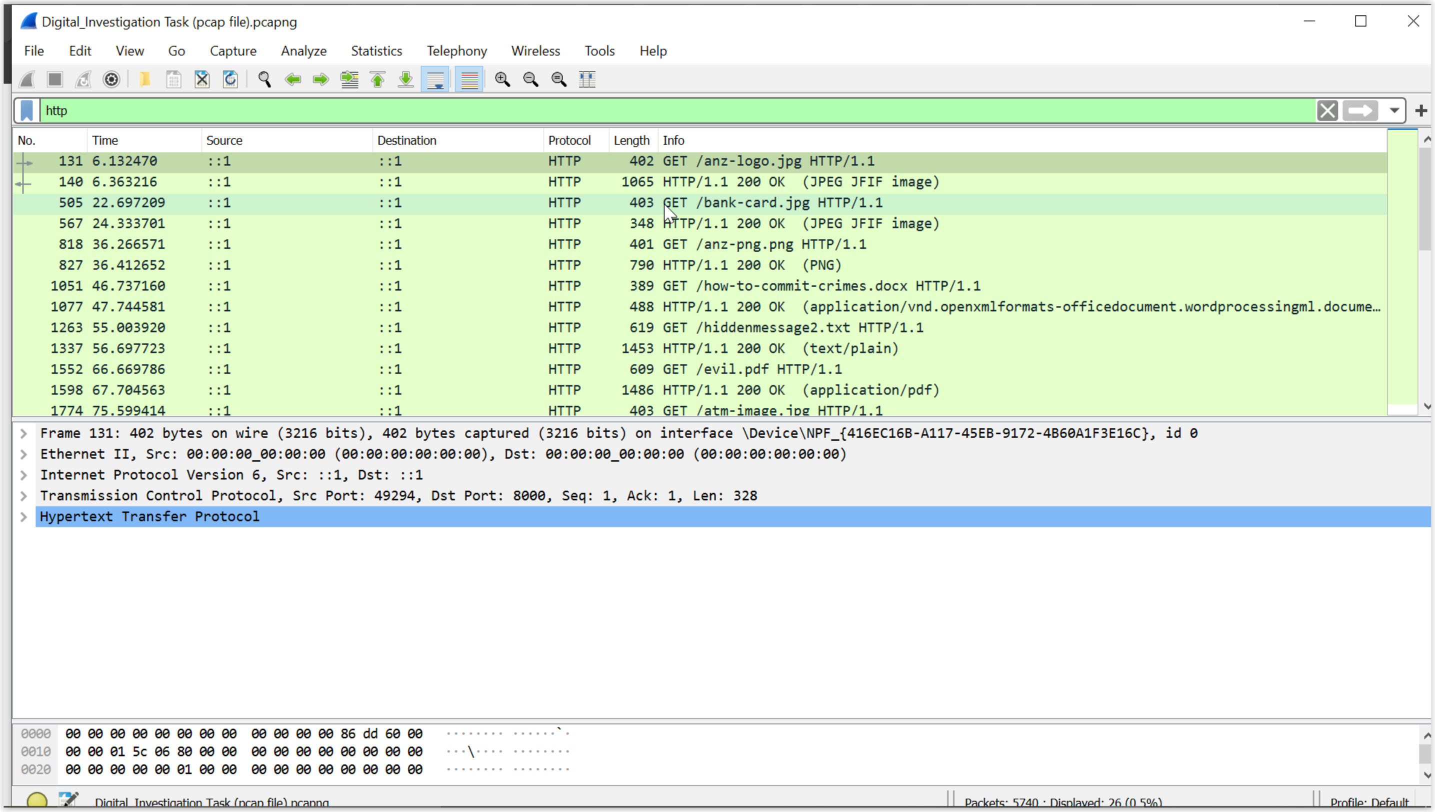
Provide a report on your findings from the pcap file and outline what processes / the steps you followed to achieve this. Here are each of your sub-tasks with additional instructions. Please record your findings under each sub-task title.

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.*

Open pcap file in wireshark to investigate
Filter http traffic and get anz.jpg
Left Click->Follow->TCP Stream
View data as raw data
In search bar find ffd8 and ffd9 and copy all hex data in between
Open hex editor HxD tool open new file and paste
Save as a jpg file



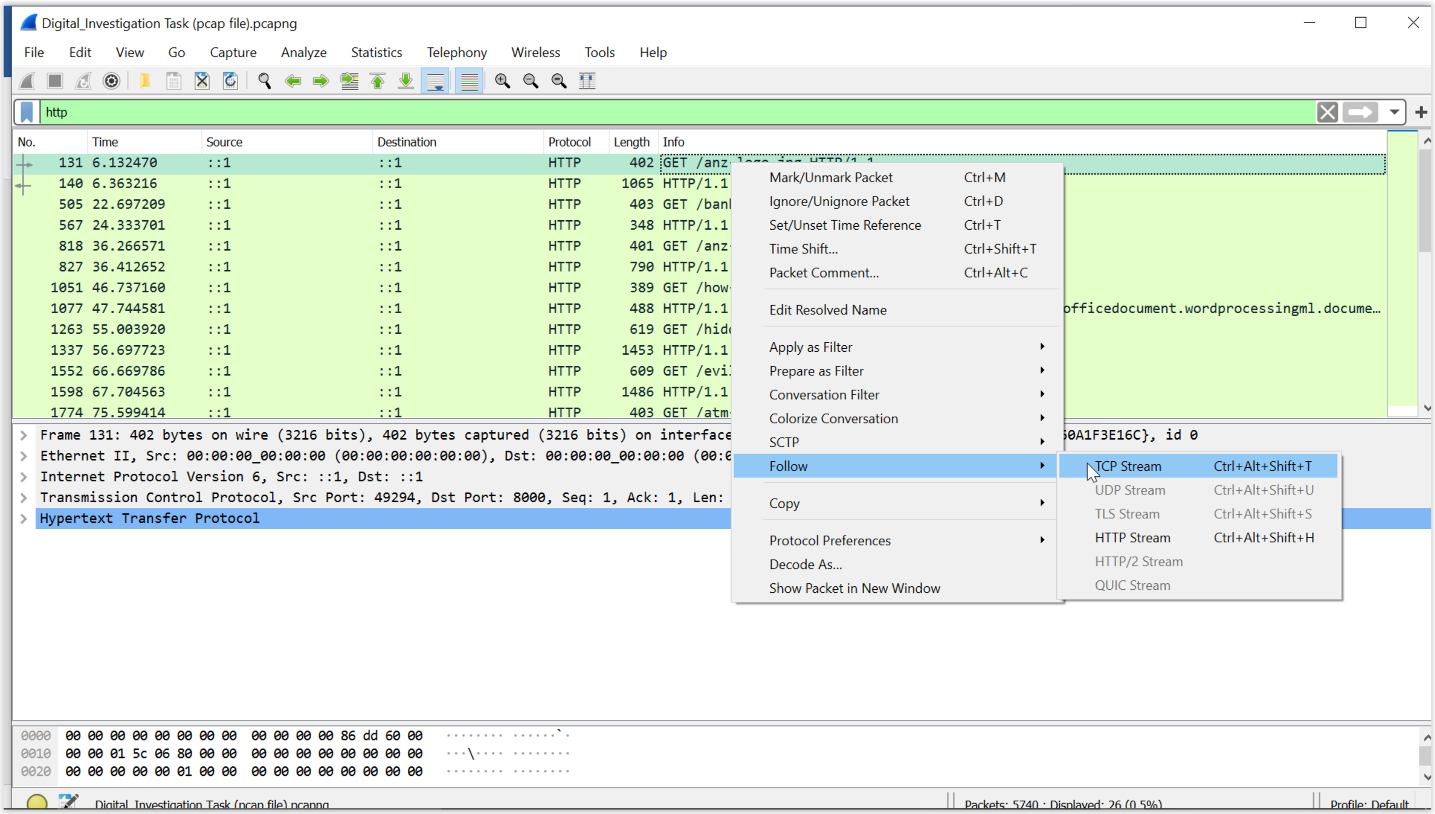
```
http
```

```
No.     Time        Source   Destination   Protocol   Length 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.docume…
  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
```

```
> Frame 131: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits) on interface \Device\NPF_{416EC16B-A117-45EB-9172-4B60A1F3E16C}, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 49294, Dst Port: 8000, Seq: 1, Ack: 1, Len: 328
> Hypertext Transfer Protocol
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 86 dd 60 00   ········ ······`·
0010  00 00 01 5c 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   ········ ········
```

```
Digital_Investigation Task (pcap file).pcapng     Packets: 5740 · Displayed: 26 (0.5%)     Profile: Default
```


Digital_Investigation Task (pcap file).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
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
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream

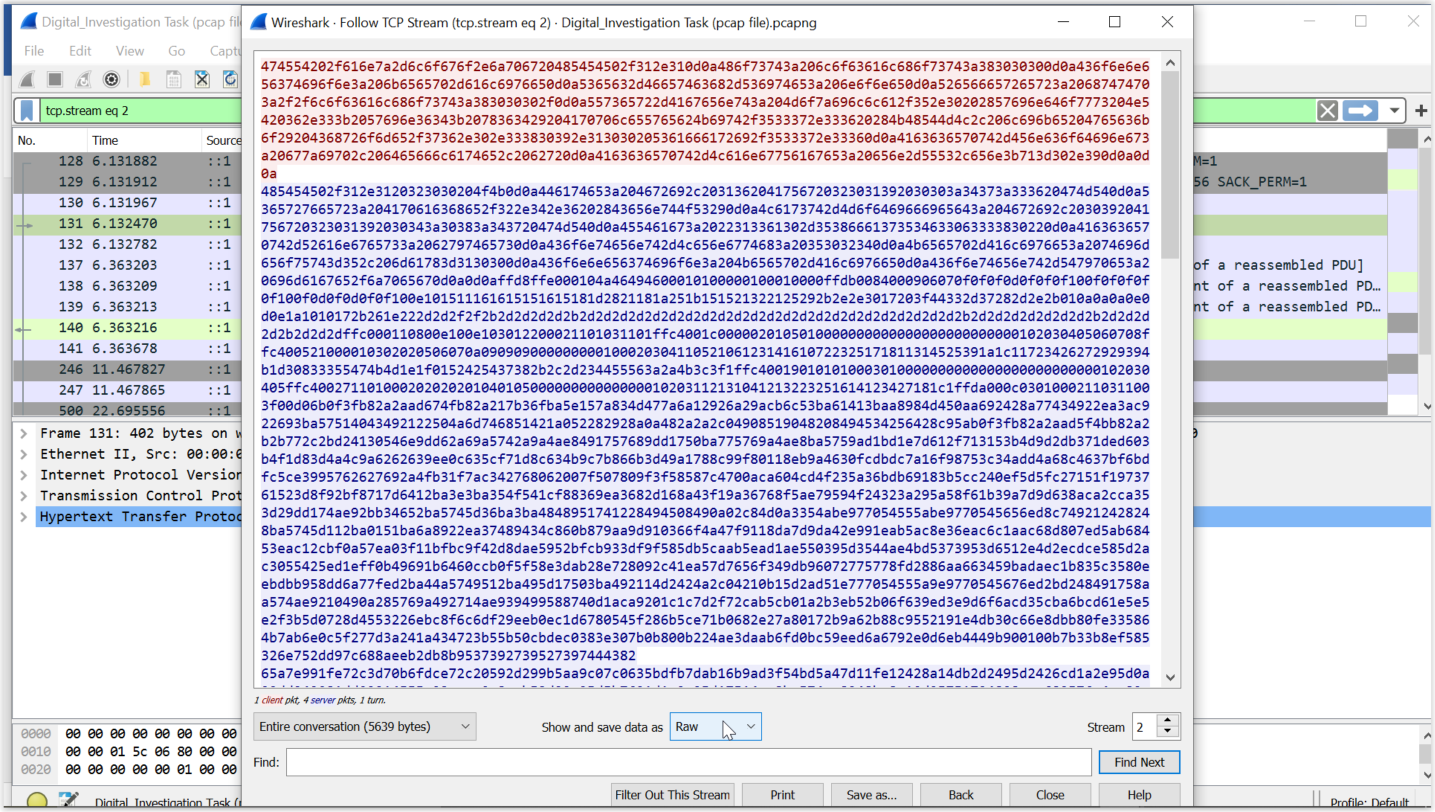
http

```
No.   Time       Source   Destination   Protocol  Length  Info
 131  6.132470   ::1      ::1           HTTP       402  GET /anz
 140  6.363216   ::1      ::1           HTTP      1065  HTTP/1.1
 505  22.697209  ::1      ::1           HTTP       403  GET /ban
 567  24.333701  ::1      ::1           HTTP       348  HTTP/1.1
 818  36.266571  ::1      ::1           HTTP       401  GET /anz
 827  36.412652  ::1      ::1           HTTP       790  HTTP/1.1
1051  46.737160  ::1      ::1           HTTP       389  GET /how
1077  47.744581  ::1      ::1           HTTP       488  HTTP/1.1 officedocument.wordprocessingml.docume…
1263  55.003920  ::1      ::1           HTTP       619  GET /hid
1337  56.697723  ::1      ::1           HTTP      1453  HTTP/1.1
1552  66.669786  ::1      ::1           HTTP       609  GET /evi
1598  67.704563  ::1      ::1           HTTP      1486  HTTP/1.1
1774  75.599414  ::1      ::1           HTTP       403  GET /atm
```

```
> Frame 131: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits) on interface …0A1F3E16C}, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:0
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 49294, Dst Port: 8000, Seq: 1, Ack: 1, Len:
> Hypertext Transfer Protocol
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 86 dd 60 00   ········ ······`·
0010  00 00 01 5c 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   ········ ········
```

Digital_Investigation Task (pcap file).pcapng | Packets: 5740 · Displayed: 26 (0.5%) | Profile: Default


Digital_Investigation Task (pcap fil
File Edit View Go Captu
Wireshark · Follow TCP Stream (tcp.stream eq 2) · Digital_Investigation Task (pcap file).pcapng
Filter Out This Stream
Print
Save as...
Back
Close
Help
Find Next

tcp.stream eq 2

```
No.   Time       Source
 128  6.131882   ::1
 129  6.131912   ::1
 130  6.131967   ::1
 131  6.132470   ::1
 132  6.132782   ::1
 137  6.363203   ::1
 138  6.363209   ::1
 139  6.363213   ::1
 140  6.363216   ::1
 141  6.363678   ::1
 246  11.467827  ::1
 247  11.467865  ::1
 500  22.695556  ::1
```

```
M=1
56 SACK_PERM=1
of a reassembled PDU]
nt of a reassembled PD…
nt of a reassembled PD…
```

```
> Frame 131: 402 bytes on w
> Ethernet II, Src: 00:00:0
> Internet Protocol Versio
> Transmission Control Prot
> Hypertext Transfer Protoc
```

```
0000  00 00 00 00 00 00 00 00
0010  00 00 01 5c 06 80 00 00
0020  00 00 00 00 00 01 00 00
```

```
474554202f616e7a2d6c6f676f2e6a706720485454502f312e310d0a486f73743a206c6f63616c686f73743a383030300d0a436f6e6e
56374696f6e3a206b6565702d616c6976650d0a5365632d46657463682d536974653a206e6f6e650d0a526566657265723a2068747470
3a2f2f6c6f63616c686f73743a383030302f0d0a557365722d4167656e743a204d6f7a696c6c612f352e3020285769e646f7773204e5
420362e333b2057696e36343b207836342920417070c655765624b69742f3533372e33362028b4b48544d4c2c206c696b65204765636b
6f29204368726f6d652f37362e302e333830392e3130302053616672692f3533372e33360d0a416363657074d456e636f64696e673
a20677a69702c206465666c6174652c2062720d0a4163636570742d4c616e67756167653a20656e2d55532c656e3b713d302e390d0a0d
0a
485454502f312e3120323030204f4b0d0a446174653a204672692c2031362041756720323031392030303a34373a333620474d540d0a5
365727665723a204170616368652f322e342e36202843656e744f53290d0a4c6173742d4d6f6469666965643a204672692c2030392041
7567203230313920303343a30383a343720474d540d0a455461673a2022313361302d353866613735346330633333830220d0a416363657
0742d52616e6765733a2062797465730d0a436f6e74656e742d4c656e6774683a20353032340d0a4b6565702d416c6976653a2074696d
656f75743d352c206d61783d3130300d0a436f6e6e656374696f6e3a204b6565702d416c6976650d0a436f6e74656e742d547970653a2
0696d6167652f6a7065670d0a0d0affd8ffe000104a46494600010100000100010000ffdb0084000906070f0f0f0d0f0f0f100f0f0f0f
0f100f0d0f0d0f0f100e101511161615151615181d2821181a251b151521322125292b2e2e3017203f44332d37282d2e2b010a0a0a0e0
d0e1a1010172b261e222d2d2f2f2b2d2d2d2d2b2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2b2d2d2d2d2d2d2d2b2d2d2d
2d2b2d2d2dffc000110800e100e103012200021101031101ffc4001c000002010501000000000000000000000000102030405060708f
fc4005210000103020205060709090900000000010002030411052106123141610722325171811314525391a1c11723426272929394
b1d30833355474b4d1e1f0152425437382b2c2d234455563a2a4b3c3f1ffc40019010101000301000000000000000000000000102030
405ffc4002711010002020202010401050000000000000000010203112131041213223251614123427181c1ffda000c0301000211031100
3f00d06b0f3fb82a2aad674fb82a217b36fba5e157a834d477a6a12926a29acb6c53ba61413baa8984d450aa692428a77434922ea3ac9
22693ba57514043492122504a6d746851421a052282928a0a482a2a2c04908519048208494534256428c95ab0f3fb82a2aad5f4bb82a2
b2b772c2bd24130546e9dd62a69a5742a9a4ae8491757689dd1750ba775769a4ae8ba5759ad1bd1e7d612f713153b4d9d2db371ded603
b4f1d83d4a4c9a6262639ee0c635cf71d8c634b9c7b866b3d49a1788c99f80118eb9a4630fcdbdc7a16f98753c34add4a68c4637bf6bd
fc5ce3995762627692a4fb31f7ac342768062007f507809f3f58587c4700aca604cd4f235a36bdb69183b5cc240ef5d5fc27151f19737
61523d8f92bf8717d6412ba3e3ba354f541cf88369ea3682d168a43f19a36768f5ae79594f24323a295a58f61b39a7d9d638aca2cca35
3d29dd174ae92bb34652ba5745d36ba3ba4848951741228494508490a02c84d0a3354abe977054555abe9770545656ed8c74921242824
8ba5745d112ba0151ba6a8922ea37489434c860b879aa9d910366f4a47f9118da7d9da42e991eab5ac8e36eac6c1aac68d807ed5ab684
53eac12cbf0a57ea03f11bfbc9f42d8dae5952bfcb933df9f585db5caab5ead1ae550395d3544ae4bd5373953d6512e4d2ecdce585d2a
c3055425ed1eff0b49691b6460ccb0f5f58e3dab28e728092c41ea57d7656f349db96072775778fd2886aa663459badaec1b835c3580e
ebdbb958dd6a77fed2ba44a5749512ba495d17503ba492114d2424a2c04210b15d2ad51e777054555a9e9770545676ed2bd248491758a
a574ae9210490a285769a492714ae939499588740d1aca9201c1c7d2f72cab5cb01a2b3eb52b06f639ed3e9d6f6acd35cba6bcd61e5e5
e2f3b5d0728d4553226ebc8f6c6df29eeb0ec1d6780545f286b5ce71b0682e27a80172b9a62b88c9552191e4db30c66e8dbb80fe33586
4b7ab6e0c5f277d3a241a434723b55b50cbdec0383e307b0b800b224ae3daab6fd0bc59eed6a6792e0d6eb4449b900100b7b33b8ef585
326e752dd97c688aeeb2db8b9537392739527397444382
65a7e991fe72c3d70b6fdce72c20592d299b5aa9c07c0635bdfb7dab16b9ad3f54bd5a47d11fe12428a14db2d2495d2426cd1a2e95d0a
```

1 client pkt, 4 server pkts, 1 turn.

Entire conversation (5639 bytes)

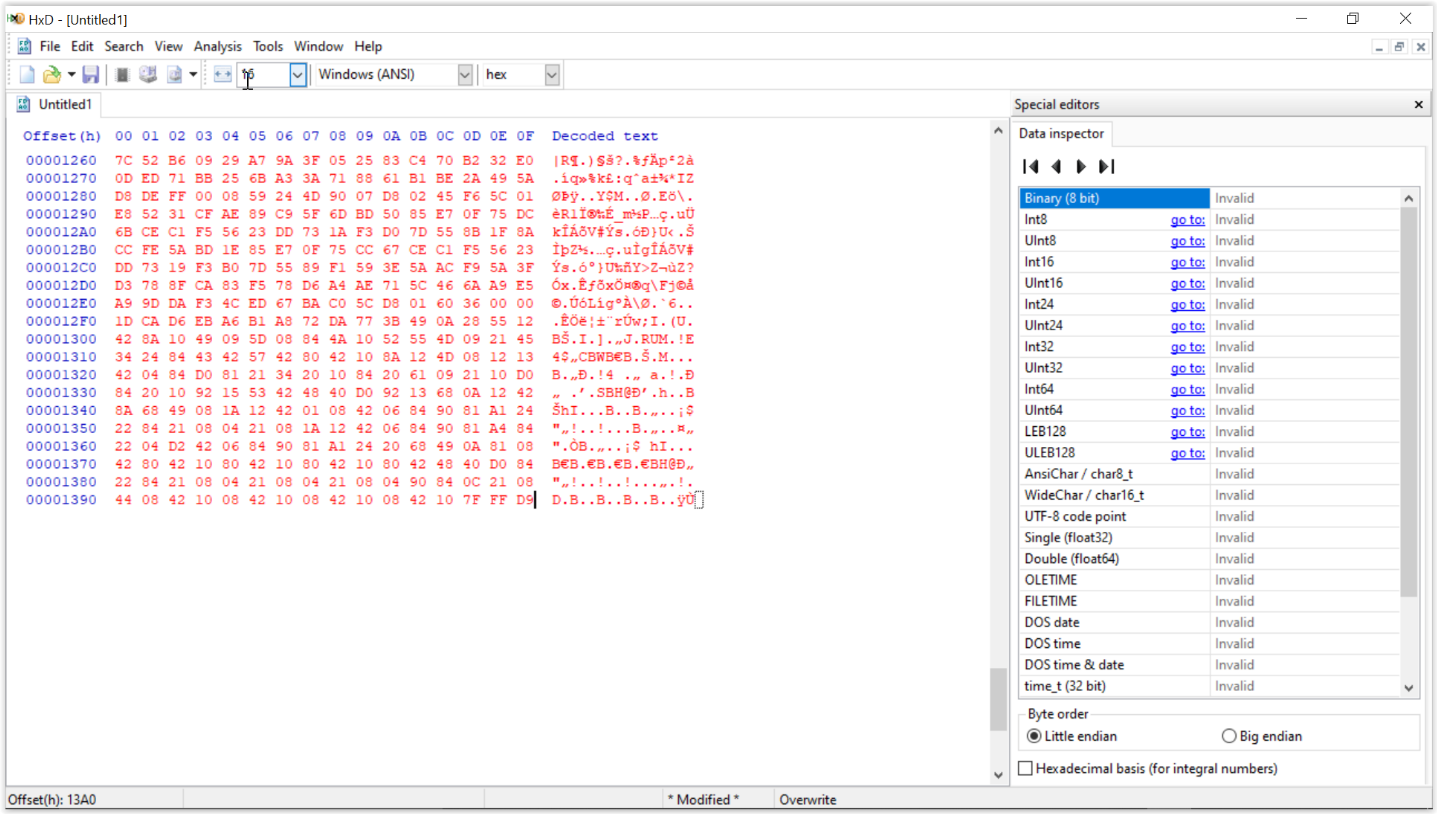
Show and save data as: Raw

Stream: 2

Find:

Digital_Investigation Task (

Profile: Default



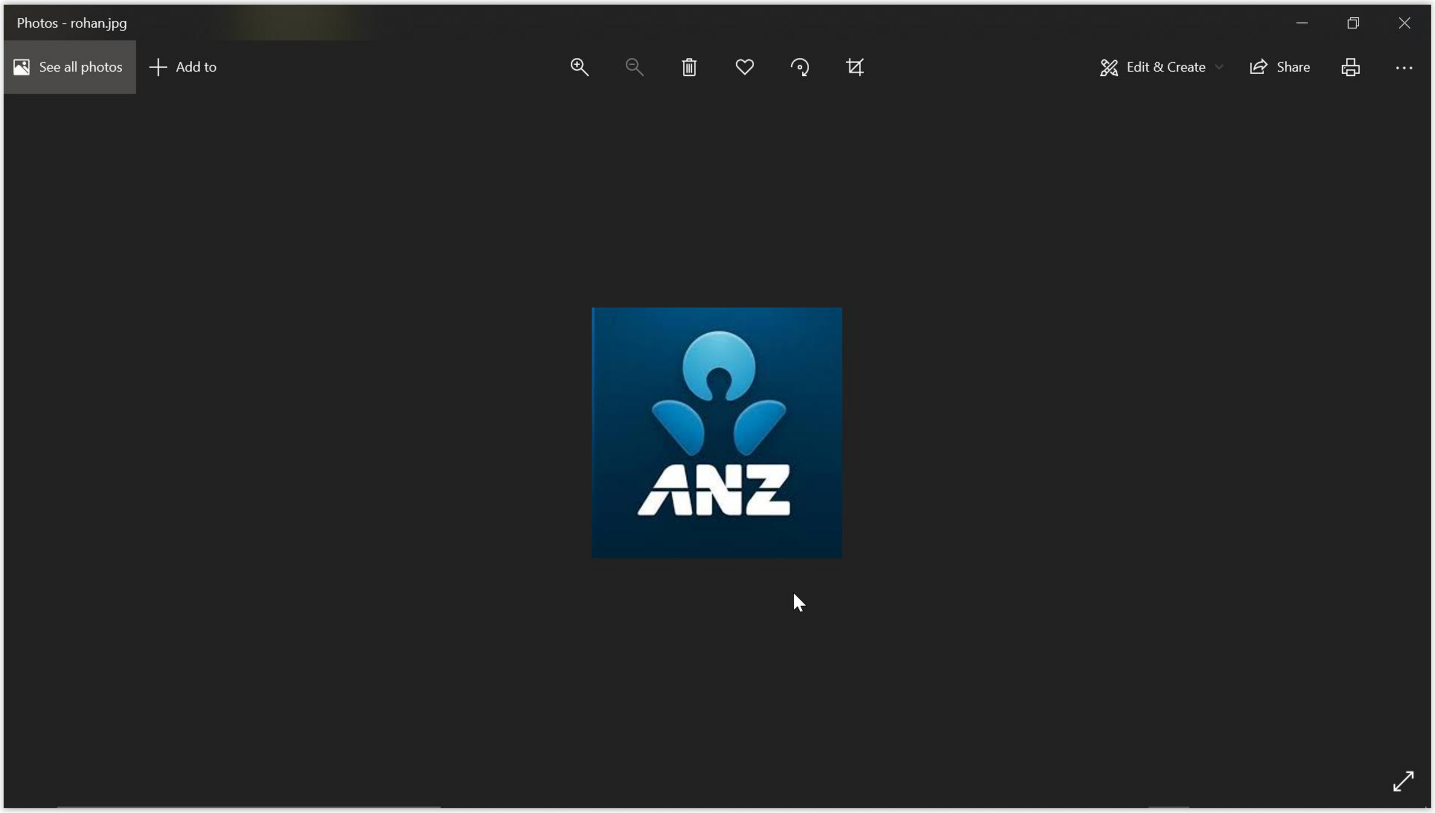
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00001260  7C 52 B6 09 29 A7 9A 3F 05 25 83 C4 70 B2 32 E0  |R¶.)§š?.%ƒÄp²2à
00001270  0D ED 71 BB 25 6B A3 3A 71 88 61 B1 BE 2A 49 5A  .íq»%k£:qˆa±¾*IZ
00001280  D8 DE FF 00 08 59 24 4D 90 07 D8 02 45 F6 5C 01  ØÞÿ..Y$M..Ø.Eö\.
00001290  E8 52 31 CF AE 89 C9 5F 6D BD 50 85 E7 0F 75 DC  èR1Ï®‰É_m½P…ç.uÜ
000012A0  6B CE C1 F5 56 23 DD 73 1A F3 D0 7D 55 8B 1F 8A  kÎÁõV#Ýs.óÐ}U‹.Š
000012B0  CC FE 5A BD 1E 85 E7 0F 75 CC 67 CE C1 F5 56 23  ÌþZ½.…ç.uÌgÎÁõV#
000012C0  DD 73 19 F3 B0 7D 55 89 F1 59 3E 5A AC F9 5A 3F  Ýs.ó°}U‰ñY>Z¬ùZ?
000012D0  D3 78 8F CA 83 F5 78 D6 A4 AE 71 5C 46 6A A9 E5  Óx.ÊƒõxÖ¤®q\Fj©å
000012E0  A9 9D DA F3 4C ED 67 BA C0 5C D8 01 60 36 00 00  ©.ÚóLígºÀ\Ø.`6..
000012F0  1D CA D6 EB A6 B1 A8 72 DA 77 3B 49 0A 28 55 12  .ÊÖë¦±¨rÚw;I.(U.
00001300  42 8A 10 49 09 5D 08 84 4A 10 52 55 4D 09 21 45  BŠ.I.].„J.RUM.!E
00001310  34 24 84 43 42 57 42 80 42 10 8A 12 4D 08 12 13  4$„CBWB€B.Š.M...
00001320  42 04 84 D0 81 21 34 20 10 84 20 61 09 21 10 D0  B.„Ð.!4 .„ a.!.Ð
00001330  84 20 10 92 15 53 42 48 40 D0 92 13 68 0A 12 42  „ .’.SBH@Ð’.h..B
00001340  8A 68 49 08 1A 12 42 01 08 42 06 84 90 81 A1 24  ŠhI...B..B.„..¡$
00001350  22 84 21 08 04 21 08 1A 12 42 06 84 90 81 A4 84  "„!..!...B.„..¤„
00001360  22 04 D2 42 06 84 90 81 A1 24 20 68 49 0A 81 08  ".ÒB.„..¡$ hI...
00001370  42 80 42 10 80 42 10 80 42 10 80 42 48 40 D0 84  B€B.€B.€B.€BH@Ð„
00001380  22 84 21 08 04 21 08 04 21 08 04 90 84 0C 21 08  "„!..!..!...„.!.
00001390  44 08 42 10 08 42 10 08 42 10 08 42 10 7F FF D9  D.B..B..B..B..ÿÙ
```

Binary (8 bit)		Invalid
Int8	go to:	Invalid
UInt8	go to:	Invalid
Int16	go to:	Invalid
UInt16	go to:	Invalid
Int24	go to:	Invalid
UInt24	go to:	Invalid
Int32	go to:	Invalid
UInt32	go to:	Invalid
Int64	go to:	Invalid
UInt64	go to:	Invalid
LEB128	go to:	Invalid
ULEB128	go to:	Invalid
AnsiChar / char8_t		Invalid
WideChar / char16_t		Invalid
UTF-8 code point		Invalid
Single (float32)		Invalid
Double (float64)		Invalid
OLETIME		Invalid
FILETIME		Invalid
DOS date		Invalid
DOS time		Invalid
DOS time & date		Invalid
time_t (32 bit)		Invalid

Byte order
● Little endian ○ Big endian

□ Hexadecimal basis (for integral numbers)

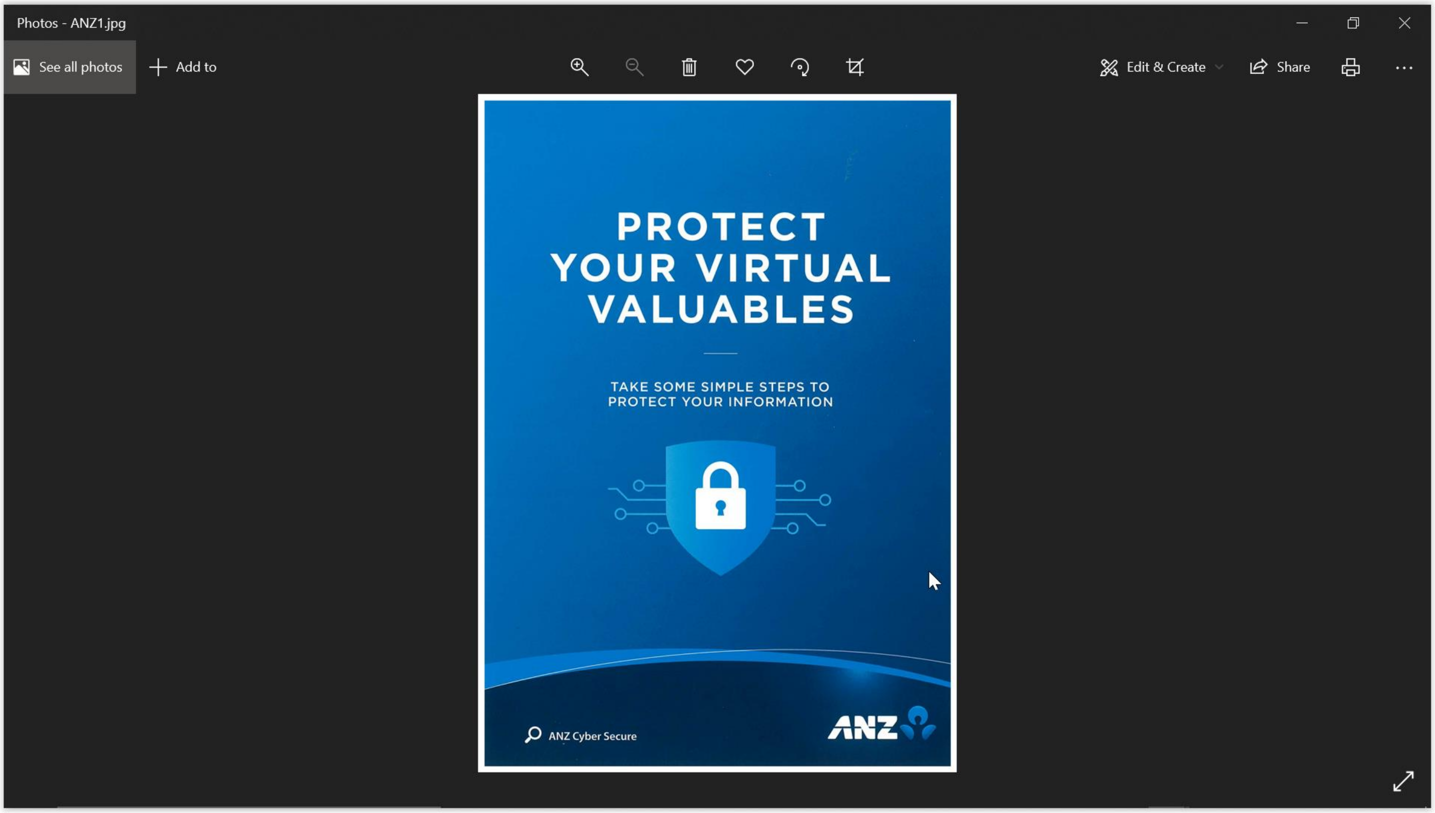
Offset(h): 13A0 * Modified * Overwrite



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.*

Second image is more detailed and comprehensive

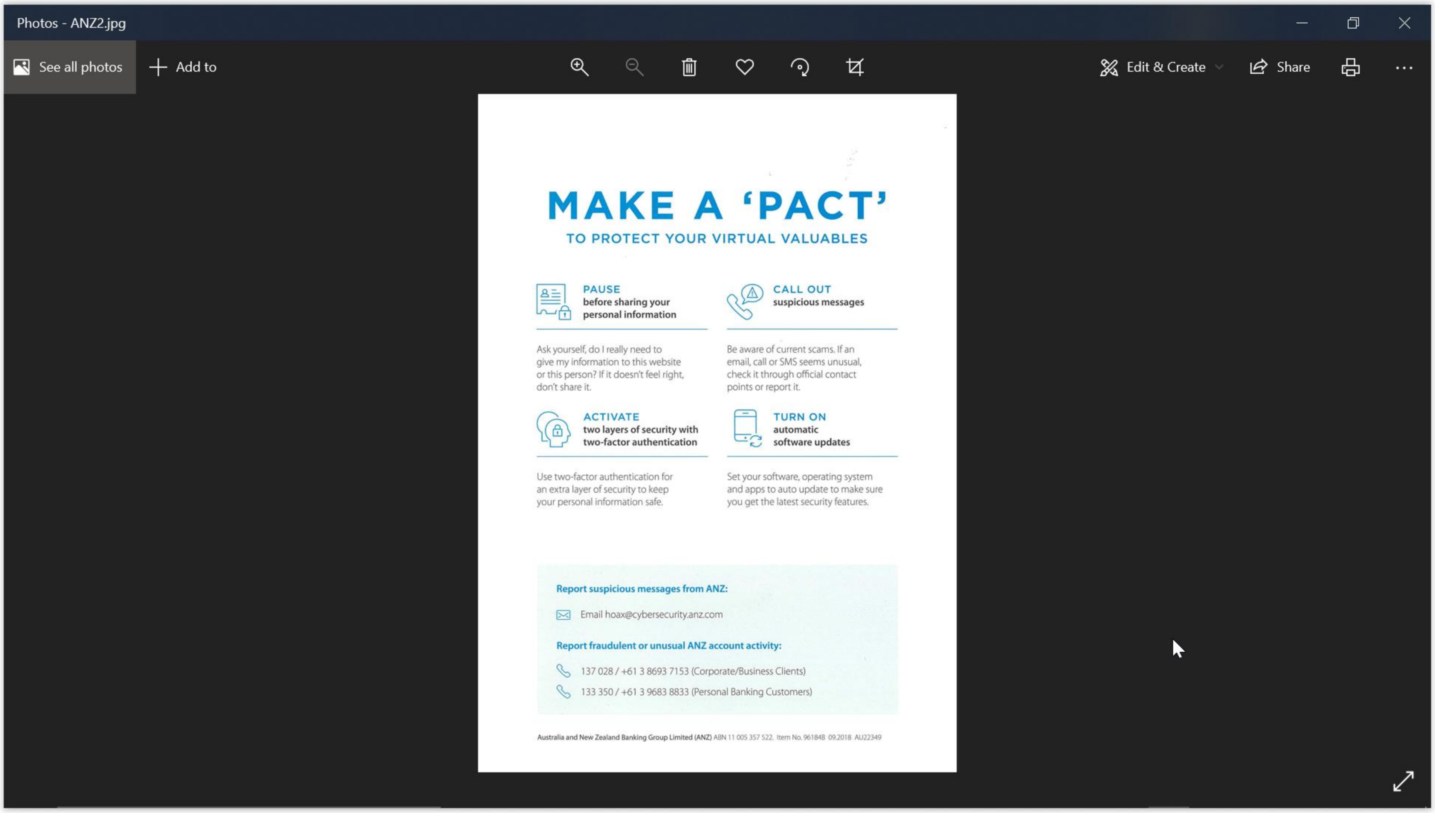


PROTECT YOUR VIRTUAL VALUABLES

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:

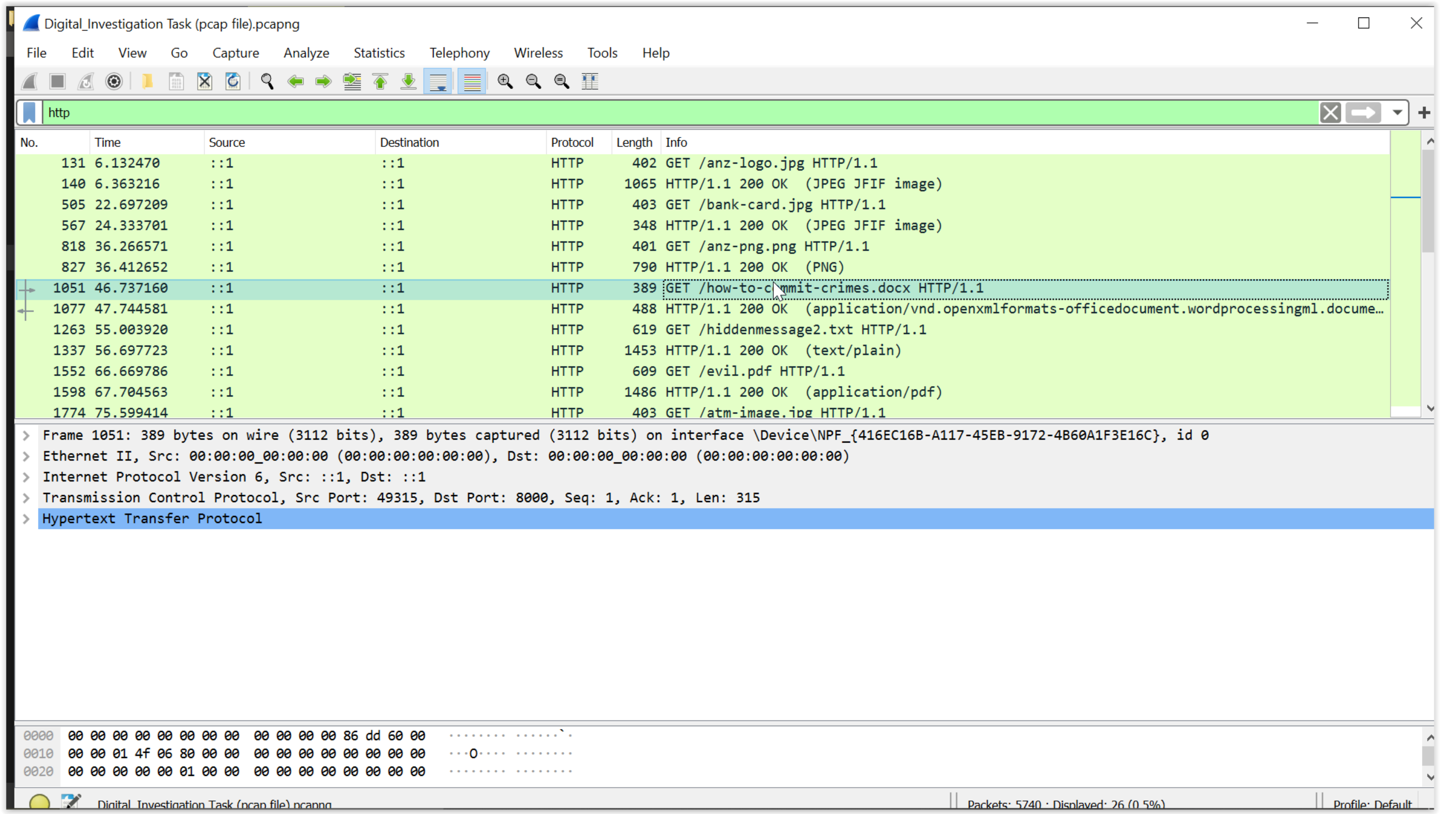
☎ 137 028 / +61 3 8693 7153 (Corporate/Business Clients)

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

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Item No. 961848 09.2018 AU22349

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.*


Digital_Investigation Task (pcap file).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

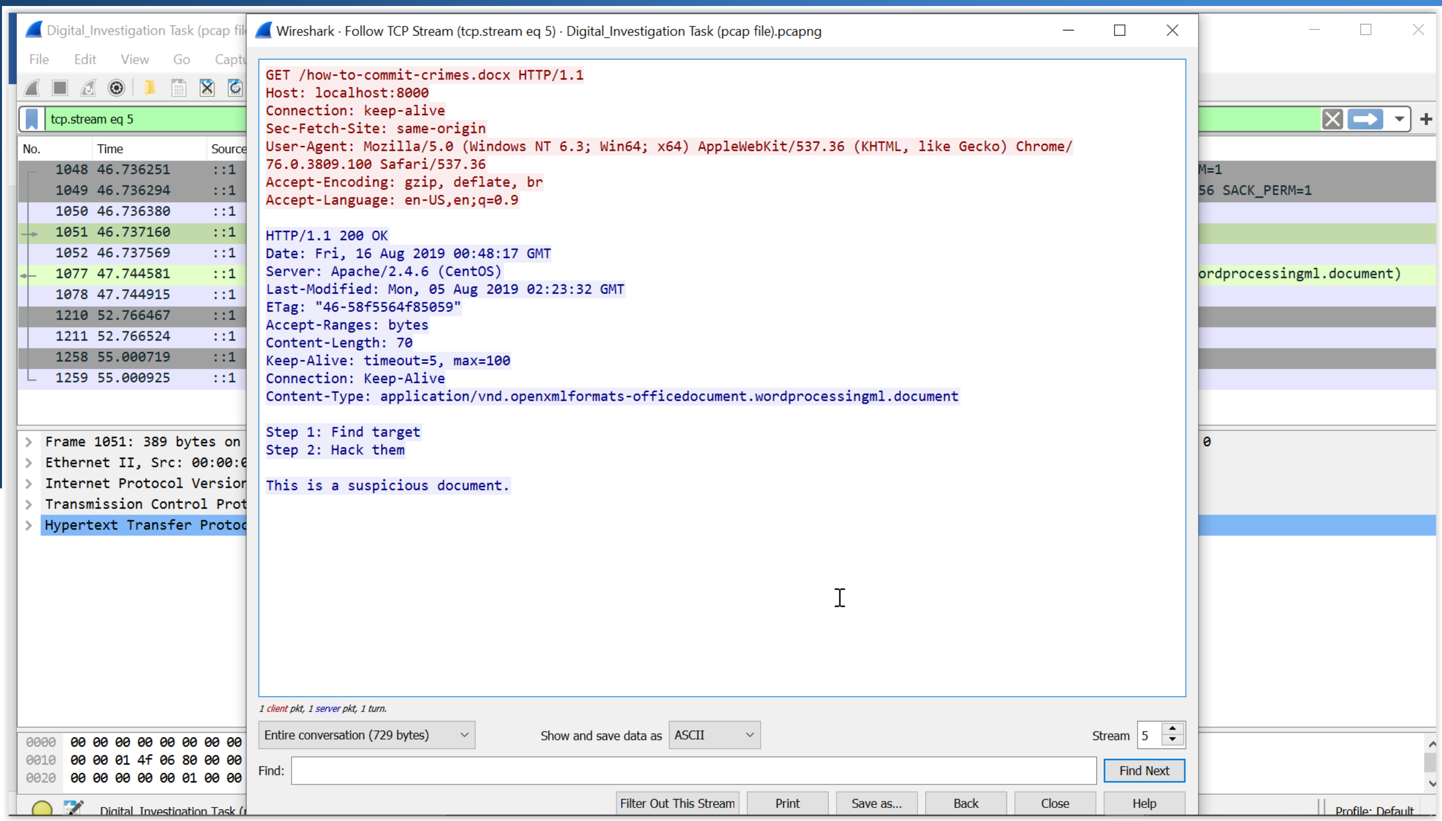
```
No.   Time       Source  Destination  Protocol  Length  Info
 131  6.132470   ::1     ::1          HTTP         402  GET /anz-logo.jpg HTTP/1.1
 140  6.363216   ::1     ::1          HTTP        1065  HTTP/1.1 200 OK  (JPEG JFIF image)
 505  22.697209  ::1     ::1          HTTP         403  GET /bank-card.jpg 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.docume…
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
```

```
> Frame 1051: 389 bytes on wire (3112 bits), 389 bytes captured (3112 bits) on interface \Device\NPF_{416EC16B-A117-45EB-9172-4B60A1F3E16C}, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 49315, Dst Port: 8000, Seq: 1, Ack: 1, Len: 315
> 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   ···O···· ········
0020  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Digital_Investigation Task (pcap file).pcapng | Packets: 5740 · Displayed: 26 (0.5%) | Profile: Default

Contents after opening TCP Stream

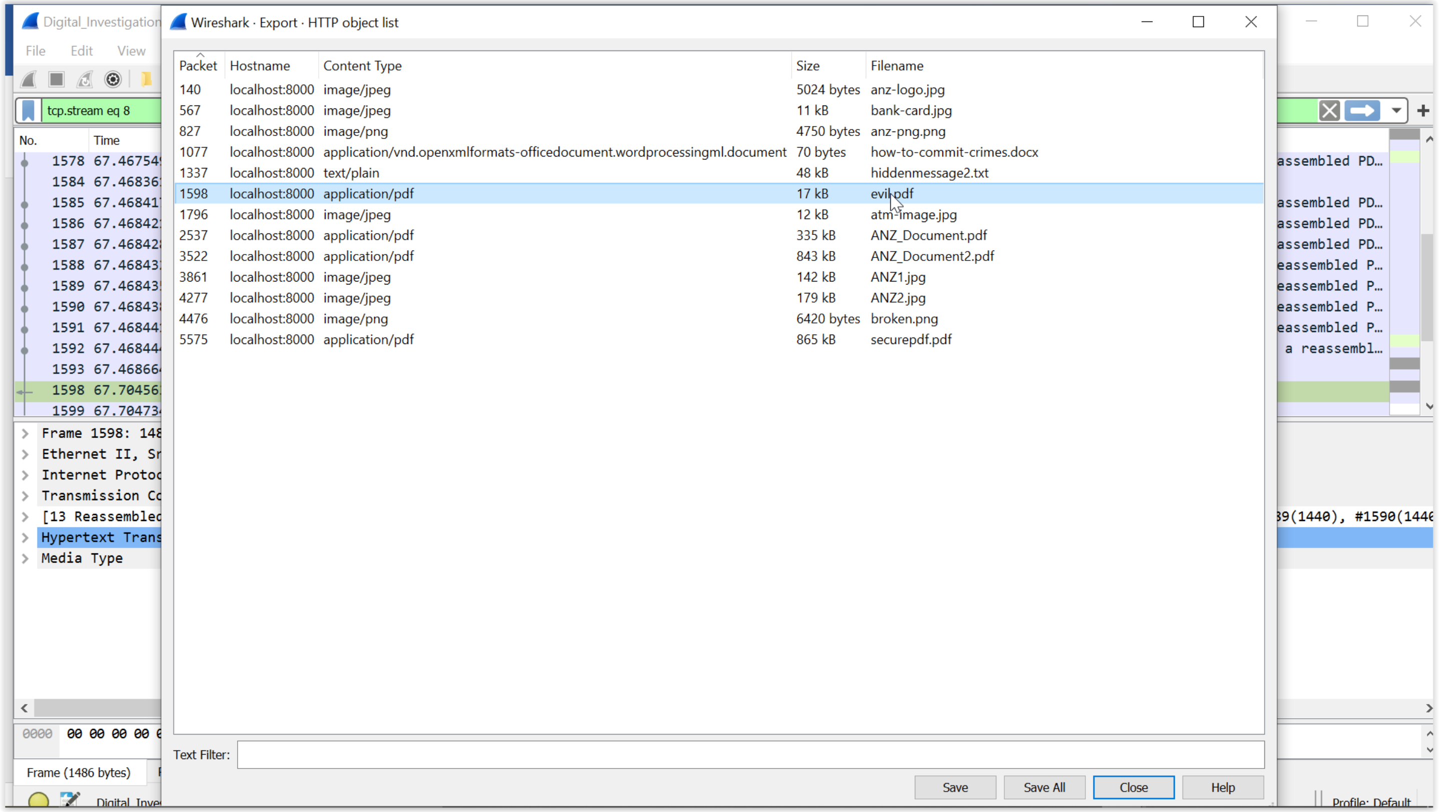

Wireshark · Follow TCP Stream (tcp.stream eq 5) · Digital_Investigation Task (pcap file).pcapng
tcp.stream eq 5
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (729 bytes)
Show and save data as
ASCII
Stream
5
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

```
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.
```

Sub-task 4:

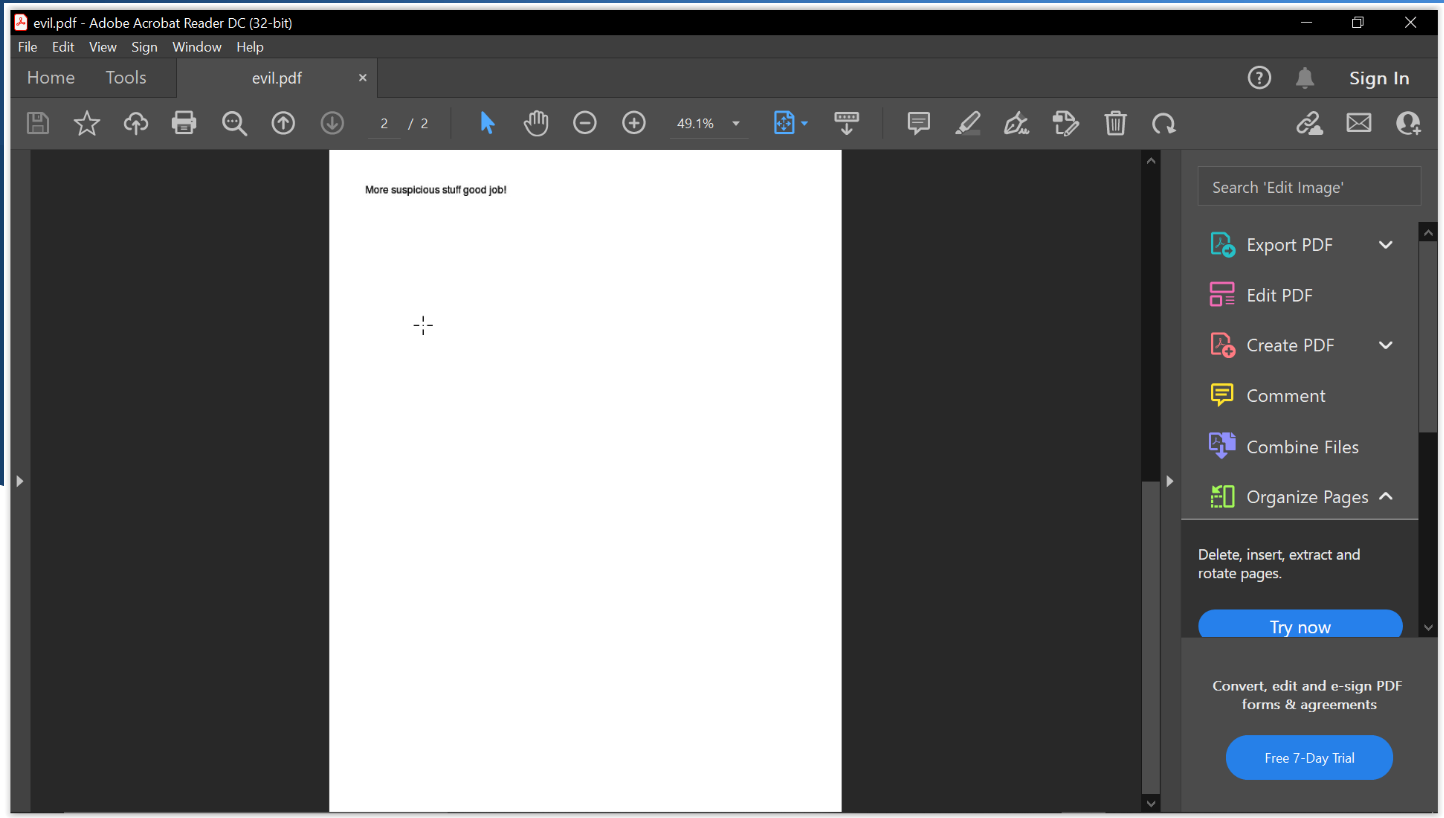
- *The user accessed 3 pdf documents: ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf*
- *Extract and view these documents. Include images of them in your report.*

File-> Export Objects-> HTTP



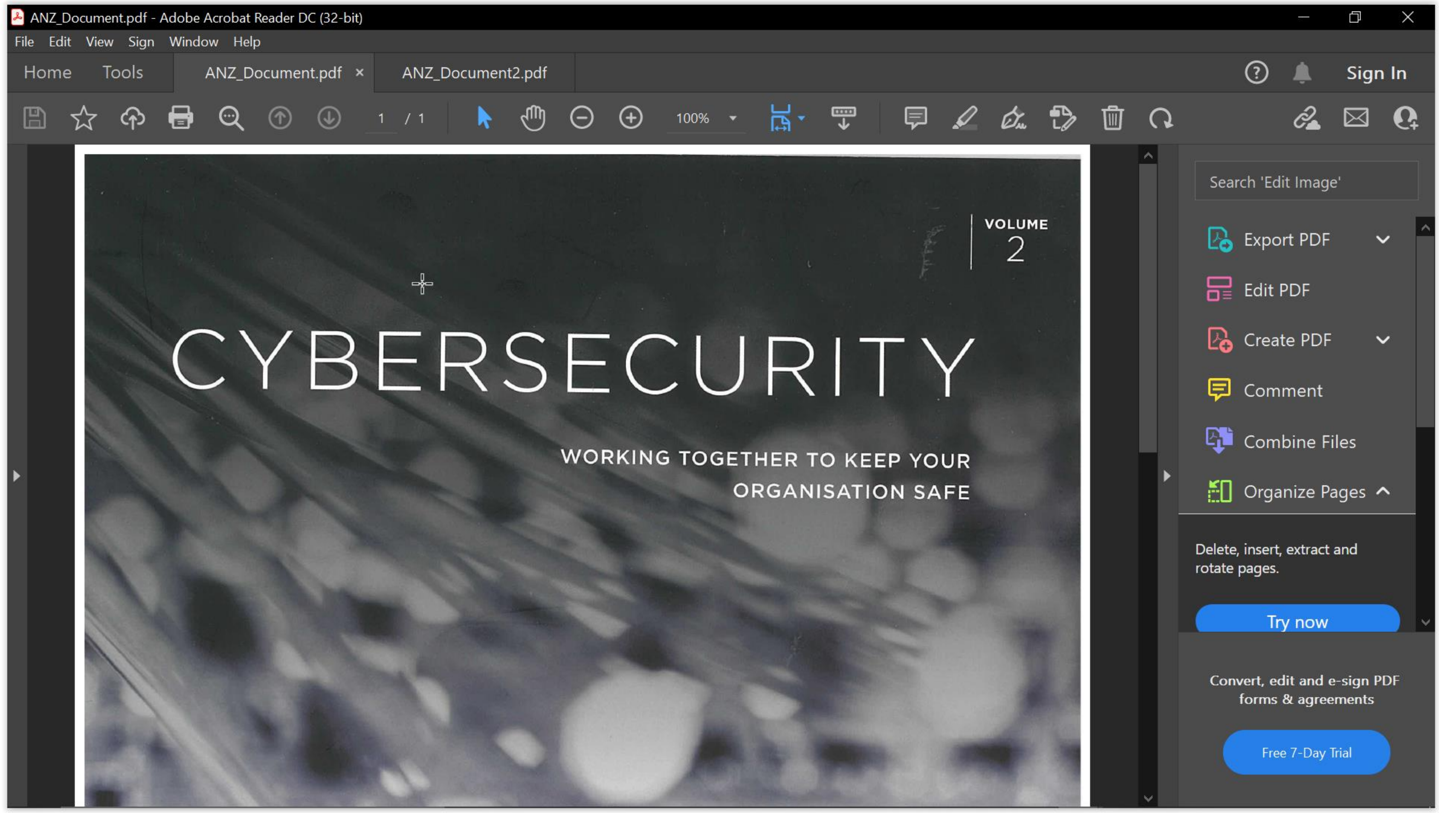
Packet	Hostname	Content Type	Size	Filename
140	localhost:8000	image/jpeg	5024 bytes	anz-logo.jpg
567	localhost:8000	image/jpeg	11 kB	bank-card.jpg
827	localhost:8000	image/png	4750 bytes	anz-png.png
1077	localhost:8000	application/vnd.openxmlformats-officedocument.wordprocessingml.document	70 bytes	how-to-commit-crimes.docx
1337	localhost:8000	text/plain	48 kB	hiddenmessage2.txt
1598	localhost:8000	application/pdf	17 kB	evil.pdf
1796	localhost:8000	image/jpeg	12 kB	atm-image.jpg
2537	localhost:8000	application/pdf	335 kB	ANZ_Document.pdf
3522	localhost:8000	application/pdf	843 kB	ANZ_Document2.pdf
3861	localhost:8000	image/jpeg	142 kB	ANZ1.jpg
4277	localhost:8000	image/jpeg	179 kB	ANZ2.jpg
4476	localhost:8000	image/png	6420 bytes	broken.png
5575	localhost:8000	application/pdf	865 kB	securepdf.pdf

Evil.pdf


evil.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools evil.pdf
2 / 2
49.1%
Sign In
Search 'Edit Image'
Export PDF
Edit PDF
Create PDF
Comment
Combine Files
Organize Pages
Delete, insert, extract and rotate pages.
Try now
Convert, edit and e-sign PDF forms & agreements
Free 7-Day Trial

More suspicious stuff good job!

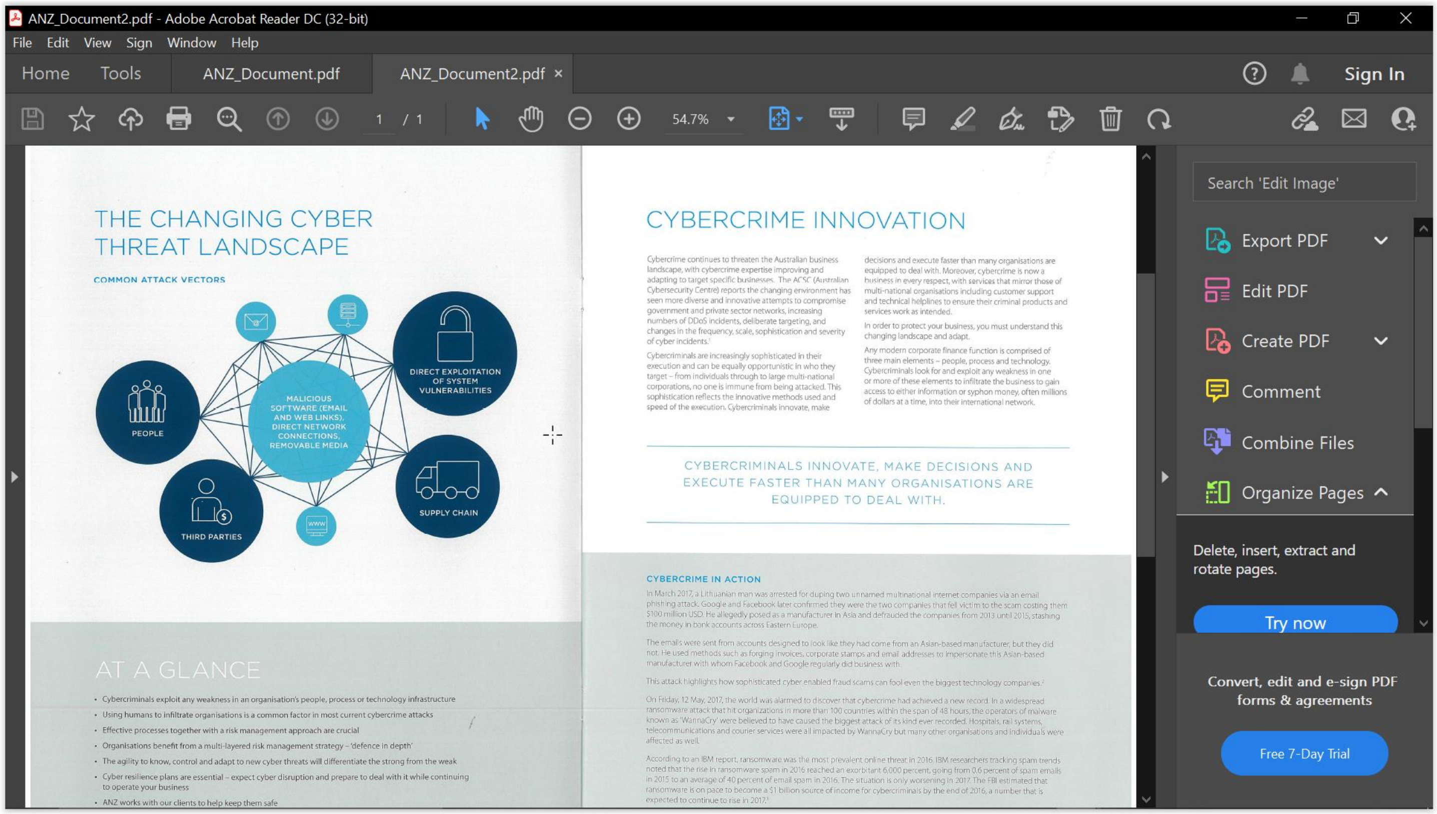
ANZ_Document.pdf


ANZ_Document.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools ANZ_Document.pdf ANZ_Document2.pdf
1 / 1
100%
Sign In
Search 'Edit Image'
Export PDF
Edit PDF
Create PDF
Comment
Combine Files
Organize Pages
Delete, insert, extract and rotate pages.
Try now
Convert, edit and e-sign PDF forms & agreements
Free 7-Day Trial

VOLUME 2

CYBERSECURITY

WORKING TOGETHER TO KEEP YOUR ORGANISATION SAFE


ANZ_Document2.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home
Tools
ANZ_Document.pdf
ANZ_Document2.pdf ×
Sign In
1 / 1
54.7%
Search 'Edit Image'
Export PDF
Edit PDF
Create PDF
Comment
Combine Files
Organize Pages
Delete, insert, extract and rotate pages.
Try now
Convert, edit and e-sign PDF forms & agreements
Free 7-Day Trial
COMMON ATTACK VECTORS
PEOPLE
MALICIOUS SOFTWARE (EMAIL AND WEB LINKS), DIRECT NETWORK CONNECTIONS, REMOVABLE MEDIA
DIRECT EXPLOITATION OF SYSTEM VULNERABILITIES
SUPPLY CHAIN
THIRD PARTIES
www

THE CHANGING CYBER THREAT LANDSCAPE

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.

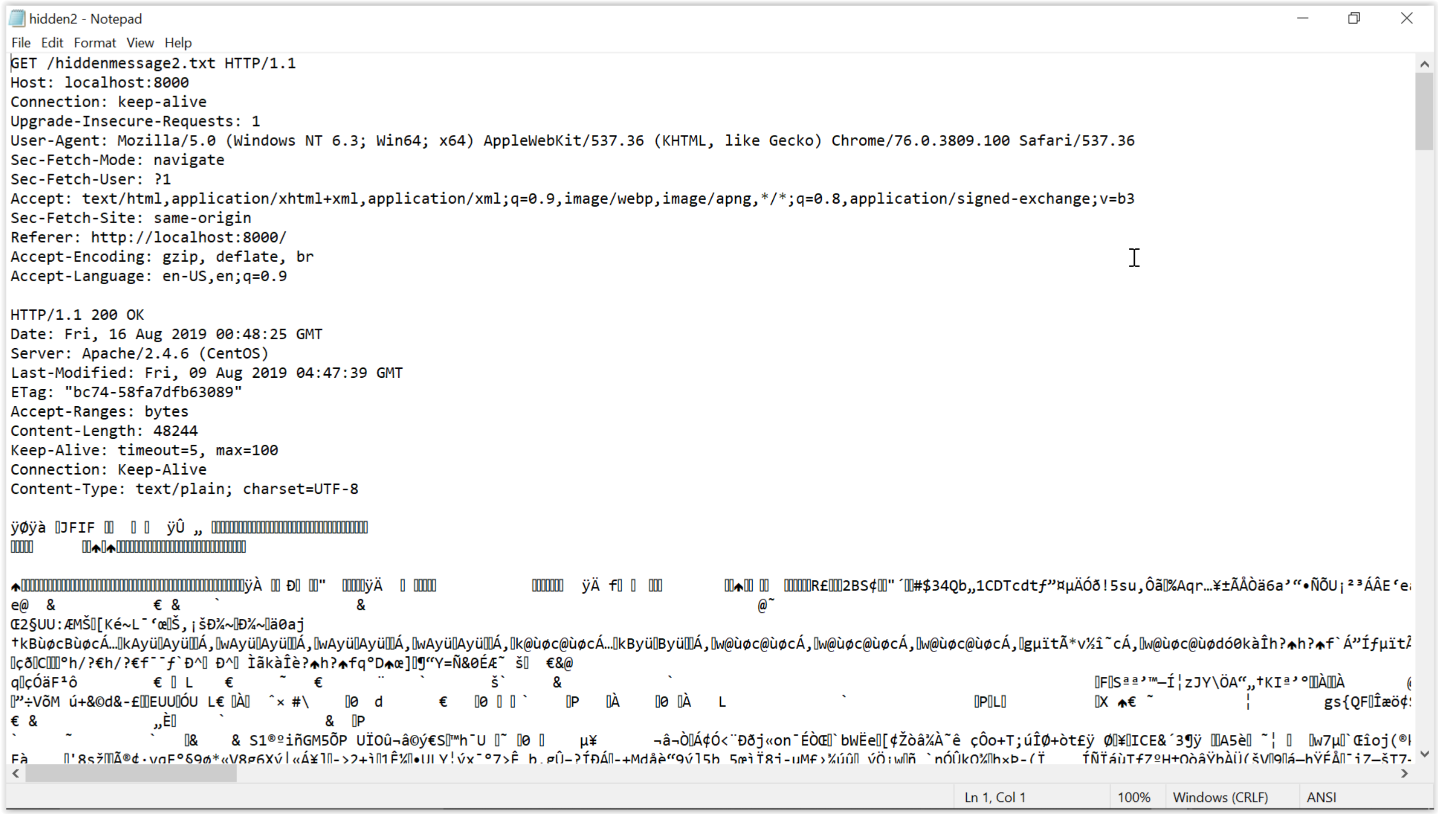
This attack highlights how sophisticated cyber enabled fraud scams can fool even the biggest technology companies.[2]

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]

Sub-task 5:

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

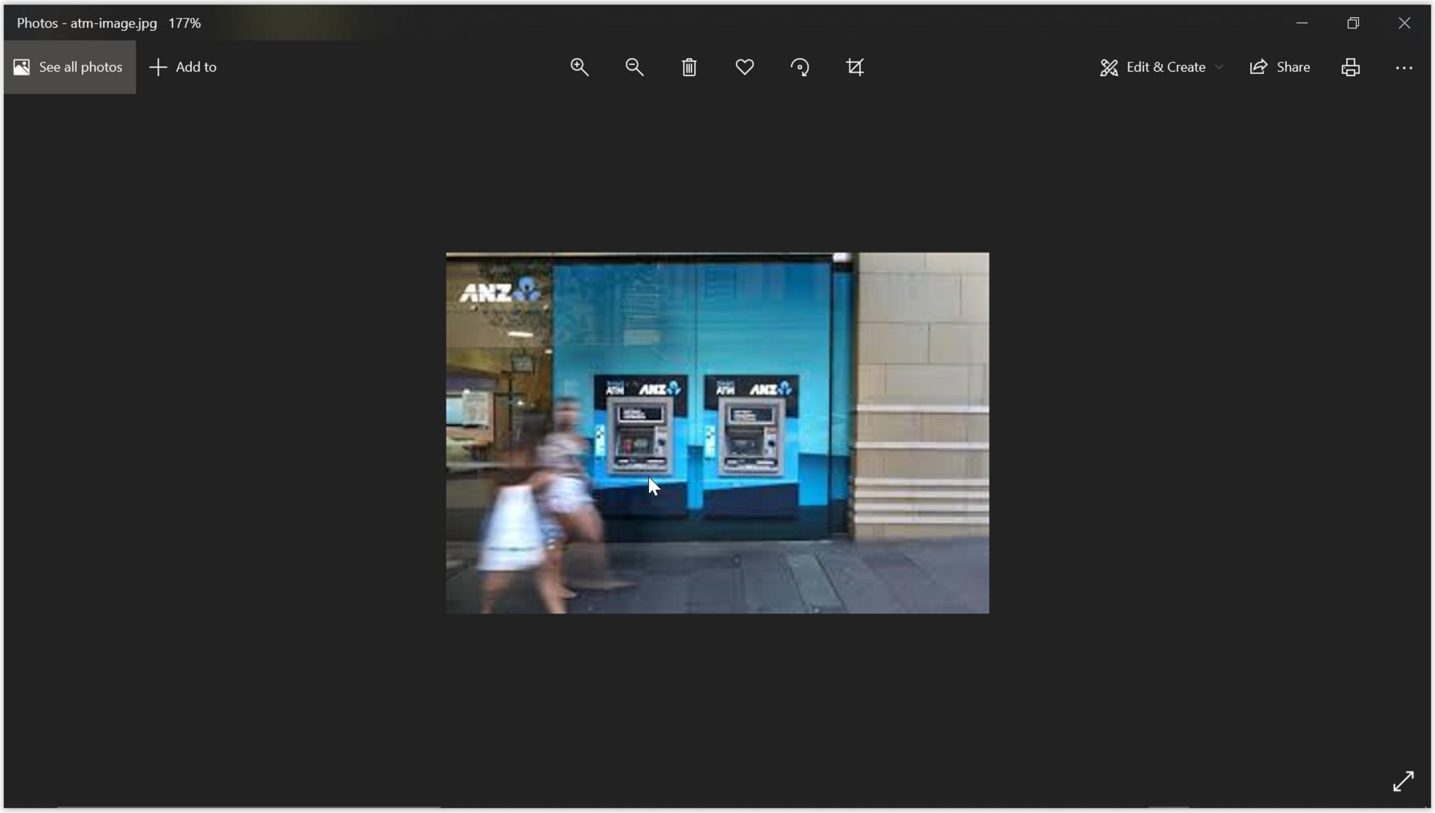


```
GET /hiddenmessage2.txt HTTP/1.1
Host: localhost:8000
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;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

ÿØÿà ▯JFIF ▯▯  ▯ ▯  ÿÛ „ ▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯
▯▯▯▯▯      ▯▯↑▯↑▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯

↑▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯ÿÀ ▯▯ Ð▯ ▯▯"  ▯▯▯▯ÿÄ  ▯ ▯▯▯▯          ▯▯▯▯▯▯▯  ÿÄ f▯ ▯ ▯▯▯        ▯▯↑▯▯ ▯▯  ▯▯▯▯▯R£▯▯▯2BS¢▯▯"´▯▯#$34Qb„1CDTcdtƒ”¤µÄÓð!5su,Ôã▯%Aqr…¥±ÃÅÒä6a’“•ÑÕU¡²³ÁÂE‘e
e@  &           € &    `                 &                   @˜
Œ2§UU:ÆMŠ▯[Ké~L¯‘œ▯Š,¡šÐ¾~▯Ð¾~▯ä0aj
†kBùøcBùøcÁ…▯kAyü▯Ayü▯▯Á,▯wAyü▯Ayü▯▯Á,▯wAyü▯Ayü▯▯Á,▯wAyü▯Ayü▯▯Á,▯k@ùøc@ùøcÁ…▯kByü▯Byü▯▯Á,▯w@ùøc@ùøcÁ,▯w@ùøc@ùøcÁ,▯w@ùøc@ùøcÁ,▯gµïtÃ*v½î˜cÁ,▯w@ùøc@ùødó0kàÎh?↑h?↑f`Á”Íƒµït
▯çð▯C▯▯▯°h/?€h/?€f¯¯ƒ`Ð^▯ Ð^▯ Ìãkàîè?↑h?↑fq°D↑œ]▯¶“Y=Ñ&0ÉÆ˜ š▯  €&@
q▯çÓäF¹ô        € ▯ L   €     ˜   €      ¨    `       š`     &          `                ▯F▯Sªª’™–Í¦zJY\ÖA“„†KIª’°▯▯À▯▯À       (
▯”÷VõM ú+&©d&-£▯▯EUU▯ÓU L€ ▯À▯  ˆ× #\    ▯0  d      €   ▯0 ▯ ▯`    ▯P   ▯À    ▯0 ▯À   L            `              ▯P▯L▯         ▯X ↑€ ˜         ¦          gs{QF▯Îæö¢
€ &             „È▯    `              &  ▯P
`     ˜           `    ▯&    & S1®ºiñGM5ÕP UÏOû¬â©ý€S▯™h¯U ▯˜ ▯0 ▯    µ¥       ¬â¬Ò▯Á¢Ó<¨Ððj«on¯ÉÒŒ▯`bWËe▯[¢Žòâ¾À˜ê çÔo+T;úÎØ+òt£ÿ Ø▯¥▯ICE&´3¶ÿ ▯▯A5è▯ ˜¦ ▯  ▯w7µ▯`Œîoj(®
Fà    ▯'8sž▯▯Ã®¢·vgF°§9ø*«V8g6Xý|«Á¥]▯->2+ì▯1Ê½▯•ULY¦ýx¯°7>Ê b,gÛ-?ÍÐÁ▯-+Mdåè“9ý]5b 5œìÏ8j-uMf›¾úû▯ ýÖ¡w▯ñ `nÓÛkO%▯hxÞ-(Ï    ÍÑÏáùTfZºH+OòâŸbÀÜ(šV▯9▯á–hŸÉÅ▯¯jZ–šT7-
```

Sub-task 6:

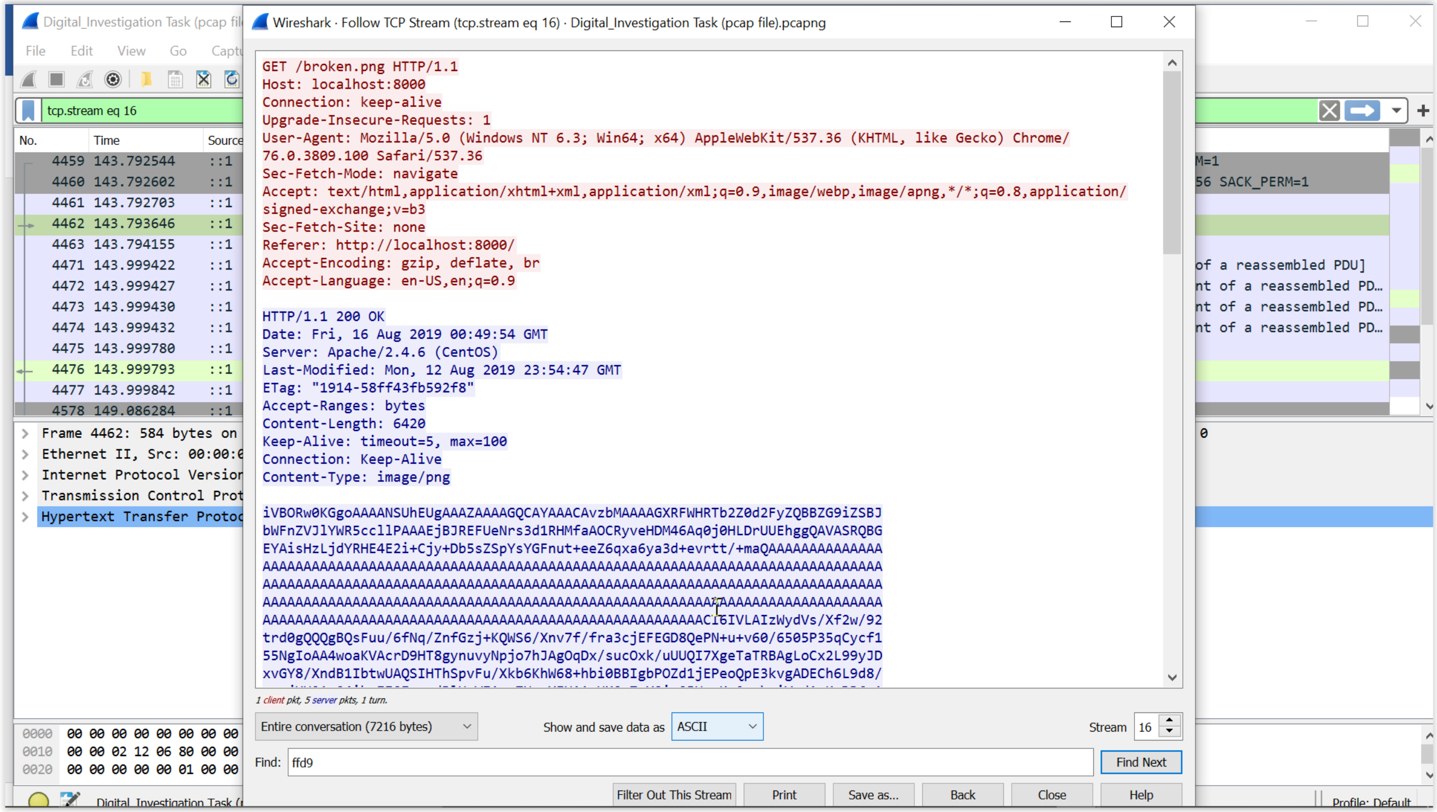
- *The user accessed an image called "atm-image.jpg"*
- *Identify what is different about this traffic and include everything in your report.*

Some coulding be conductinf reconnaissance and planning an attack on anz atms.



Sub-task 7:

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



Digital_Investigation Task (pcap fil

Wireshark · Follow TCP Stream (tcp.stream eq 16) · Digital_Investigation Task (pcap file).pcapng

tcp.stream eq 16

```
No.   Time        Source
4459 143.792544   ::1
4460 143.792602   ::1
4461 143.792703   ::1
4462 143.793646   ::1
4463 143.794155   ::1
4471 143.999422   ::1
4472 143.999427   ::1
4473 143.999430   ::1
4474 143.999432   ::1
4475 143.999780   ::1
4476 143.999793   ::1
4477 143.999842   ::1
4578 149.086284   ::1
```

```
> Frame 4462: 584 bytes on
> Ethernet II, Src: 00:00:0
> Internet Protocol Versior
> Transmission Control Prot
> Hypertext Transfer Protoc
```

```
0000  00 00 00 00 00 00 00 00
0010  00 00 02 12 06 80 00 00
0020  00 00 00 00 00 01 00 00
```

```
GET /broken.png 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
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: none
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 00:49:54 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Mon, 12 Aug 2019 23:54:47 GMT
ETag: "1914-58ff43fb592f8"
Accept-Ranges: bytes
Content-Length: 6420
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png
```

```
iVBORw0KGgoAAAANSUhEUgAAAZAAAAGQCAYAAACAvzbMAAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJ
bWFnZVJlYWR5ccllPAAAEjBJREFUeNrs3d1RHMfaAOCRyveHDM46Aq0j0HLDrUUEhggQAVASRQBG
EYAisHzLjdYRHE4E2i+Cjy+Db5sZSpYsYGFnut+eeZ6qxa6ya3d+evrtt/+maQAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACI6IVLAIzWydVs/Xf2w/92
trd0gQQQgBQsFuu/6fNq/ZnfGzj+KQWS6/Xnv7f/fra3cjEFEGD8QePN+u+v60/6505P35qCycf1
55NgIoAA4woaKVAcrD9HT8gynuvyNpjo7hJAgOqDx/sucOxk/uUUQI7XgeTaTRBAgLoCx2L99yJD
xvGY8/XndB1IbtwUAQSIHThSpvFu/fmtwZ/P87sdm/Xkb6hW68+bsXkOelpEBRUUDQoSI2nAVc7zw
```

1 client pkt, 5 server pkts, 1 turn.

Entire conversation (7216 bytes)

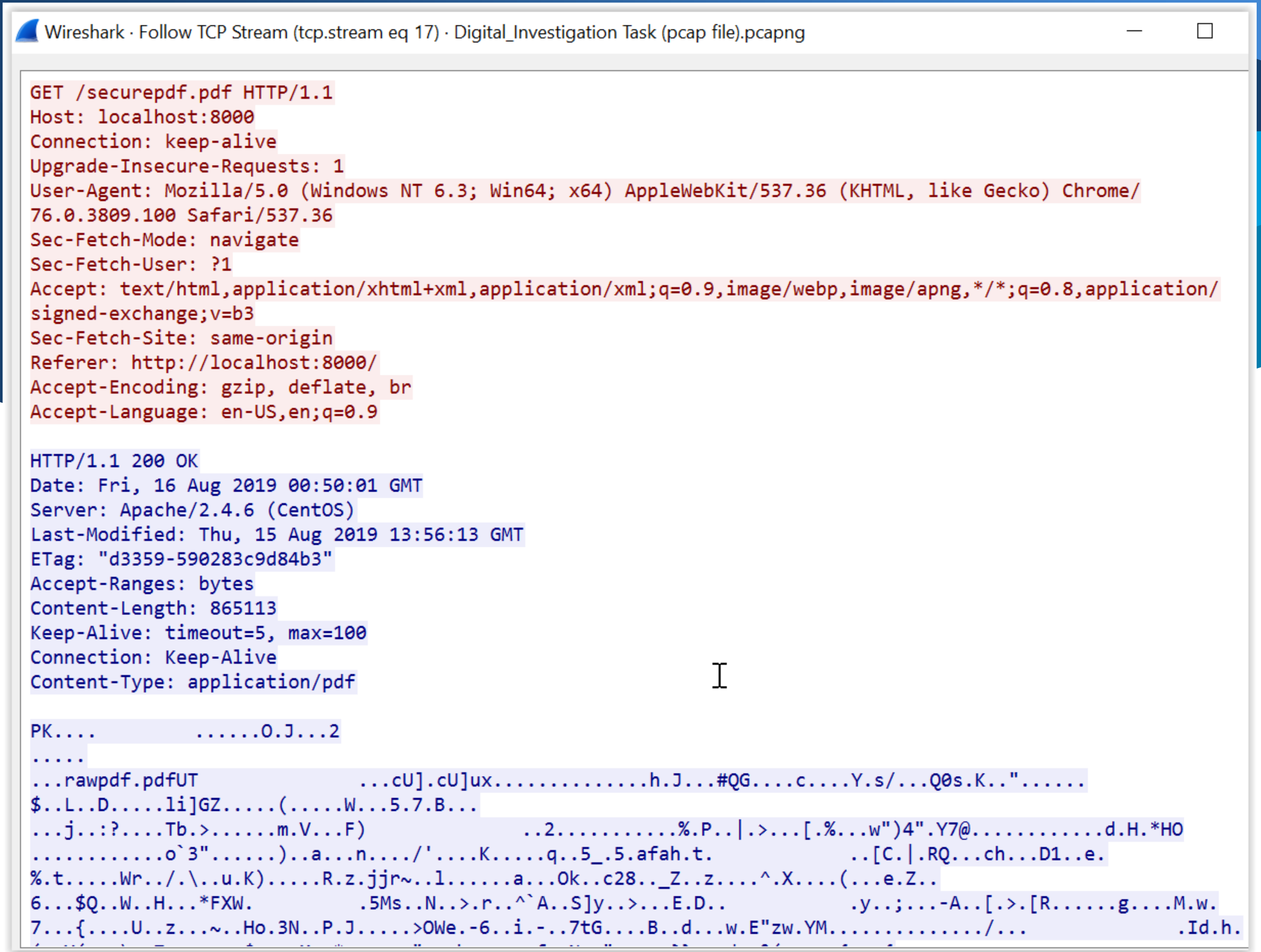
Show and save data as: ASCII

Stream: 16

Find: ffd9

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.*



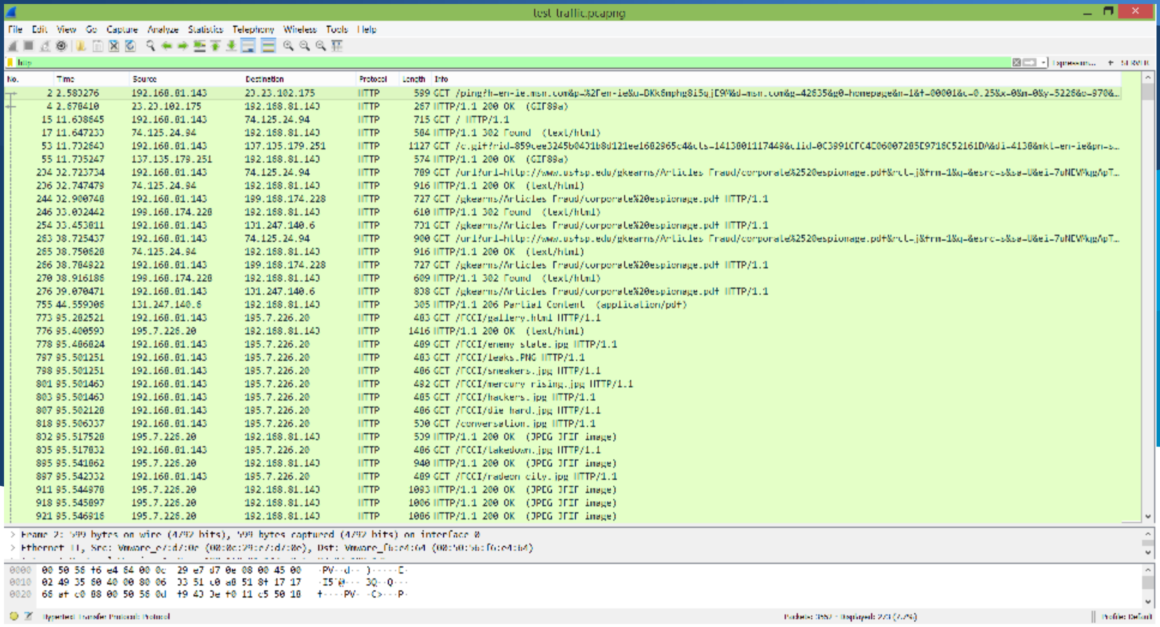
Wireshark · Follow TCP Stream (tcp.stream eq 17) · Digital_Investigation Task (pcap file).pcapng

```
GET /securepdf.pdf 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 00:50:01 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Thu, 15 Aug 2019 13:56:13 GMT
ETag: "d3359-590283c9d84b3"
Accept-Ranges: bytes
Content-Length: 865113
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/pdf

PK....         ......O.J...2
.....
...rawpdf.pdfUT              ...cU].cU]ux..............h.J...#QG....c....Y.s/...Q0s.K.."......
$..L..D.....li]GZ.....(.....W...5.7.B...
...j..:?....Tb.>......m.V...F)             ..2...........%.P..|.>...[.%...w")4".Y7@...........d.H.*HO
...........o`3"......)..a...n..../'....K.....q..5_.5.afah.t.             ..[C.|.RQ...ch...D1..e.
%.t.....Wr../.\..u.K).....R.z.jjr~..l......a...Ok..c28.._Z..z....^.X....(...e.Z..
6...$Q..W..H...*FXW.          .5Ms..N..>.r..^`A..S]y..>...E.D..           .y..;...-A..[.>.[R......g....M.w.
7...{....U..z...~..Ho.3N..P.J.....>OWe.-6..i.-..7tG....B..d...w.E"zw.YM............../...          .Id.h.
```

Packet Capture Analysis:

I have analysed the provided packet capture file using the free network analysis tool Wireshark. I was able to put “http” into the filter field in order to filter the network traffic to only see HTTP packets.

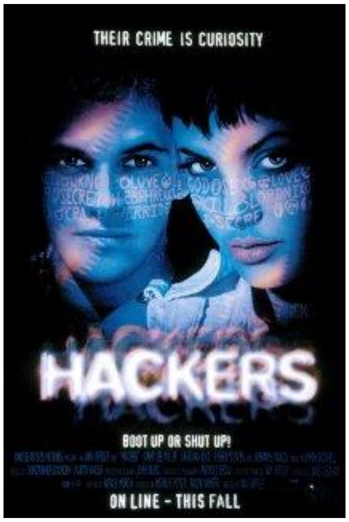
This view let me see some interesting http GET requests, which indicate that the user specifically requests information, including one for hackers.jpg



```
test traffic.pcapng

No.   Time        Source           Destination      Protocol  Length Info
   2  2.580276    192.168.81.143   23.23.102.175    HTTP       589 GET /ping?h=en-ie.msn.com&p=%2Fen-ie&u=DKk6mphg8i5qjE9M&d=msn.com&g=42635&g0=homepage&n=1&t=00001&c=0.25&x=0&m=0&y=5226&o=970&…
   4  2.670410    23.23.102.175    192.168.81.143   HTTP       267 HTTP/1.1 200 OK  (GIF89a)
  15  11.638645   192.168.81.143   74.125.24.94     HTTP       715 GET / HTTP/1.1
  17  11.647233   74.125.24.94     192.168.81.143   HTTP       584 HTTP/1.1 302 Found  (text/html)
  53  11.732643   192.168.81.143   137.135.179.251  HTTP      1127 GET /c.gif?rid=859cee3245b0431b8d121ee1682965c4&cts=1413801117448&cid=0C3891CFC4E06007285E9716C52161DA&di=4130&mkt=en-ie&pn=s…
  55  11.735247   137.135.179.251  192.168.81.143   HTTP       574 HTTP/1.1 200 OK  (GIF89a)
 234  32.723734   192.168.81.143   74.125.24.94     HTTP       709 GET /url?url=http://www.ustsp.edu/gkearns/Articles Fraud/corporate%2520espionage.pdf&rct=j&frm=1&q=&esrc=s&sa=U&ei=7uNEVMqgApT…
 236  32.747479   74.125.24.94     192.168.81.143   HTTP       916 HTTP/1.1 200 OK  (text/html)
 244  32.900748   192.168.81.143   199.168.174.228  HTTP       727 GET /gkearns/Articles Fraud/corporate%20espionage.pdf HTTP/1.1
 246  33.032442   199.168.174.228  192.168.81.143   HTTP       610 HTTP/1.1 302 Found  (text/html)
 254  33.453811   192.168.81.143   131.247.140.6    HTTP       731 GET /gkearns/Articles Fraud/corporate%20espionage.pdf HTTP/1.1
 263  38.725437   192.168.81.143   74.125.24.94     HTTP       900 GET /url?url=http://www.ustsp.edu/gkearns/Articles Fraud/corporate%2520espionage.pdf&rct=j&frm=1&q=&esrc=s&sa=U&ei=7uNEVMqgApT…
 265  38.750828   74.125.24.94     192.168.81.143   HTTP       916 HTTP/1.1 200 OK  (text/html)
 266  38.784922   192.168.81.143   199.168.174.228  HTTP       727 GET /gkearns/Articles Fraud/corporate%20espionage.pdf HTTP/1.1
 270  38.916186   199.168.174.228  192.168.81.143   HTTP       609 HTTP/1.1 302 Found  (text/html)
 276  39.070471   192.168.81.143   131.247.140.6    HTTP       838 GET /gkearns/Articles Fraud/corporate%20espionage.pdf HTTP/1.1
 755  44.559306   131.247.140.6    192.168.81.143   HTTP       305 HTTP/1.1 206 Partial Content  (application/pdf)
 773  95.282521   192.168.81.143   195.7.226.20     HTTP       403 GET /FCCI/gallery.html HTTP/1.1
 776  95.400593   195.7.226.20     192.168.81.143   HTTP      1416 HTTP/1.1 200 OK  (text/html)
 778  95.406824   192.168.81.143   195.7.226.20     HTTP       409 GET /FCCI/enemy state.jpg HTTP/1.1
 797  95.501251   192.168.81.143   195.7.226.20     HTTP       403 GET /FCCI/leaks.PNG HTTP/1.1
 798  95.501251   192.168.81.143   195.7.226.20     HTTP       406 GET /FCCI/sneakers.jpg HTTP/1.1
 801  95.501463   192.168.81.143   195.7.226.20     HTTP       492 GET /FCCI/mercury rising.jpg HTTP/1.1
 803  95.501463   192.168.81.143   195.7.226.20     HTTP       405 GET /FCCI/hackers.jpg HTTP/1.1
 807  95.502128   192.168.81.143   195.7.226.20     HTTP       406 GET /FCCI/die hard.jpg HTTP/1.1
 818  95.506337   192.168.81.143   195.7.226.20     HTTP       530 GET /conversation.jpg HTTP/1.1
 832  95.517528   195.7.226.20     192.168.81.143   HTTP       539 HTTP/1.1 200 OK  (JPEG JFIF image)
 835  95.517832   192.168.81.143   195.7.226.20     HTTP       406 GET /FCCI/takedown.jpg HTTP/1.1
 895  95.541062   195.7.226.20     192.168.81.143   HTTP       940 HTTP/1.1 200 OK  (JPEG JFIF image)
 897  95.542332   192.168.81.143   195.7.226.20     HTTP       409 GET /FCCI/radeon city.jpg HTTP/1.1
 911  95.544878   195.7.226.20     192.168.81.143   HTTP      1083 HTTP/1.1 200 OK  (JPEG JFIF image)
 918  95.545097   195.7.226.20     192.168.81.143   HTTP      1006 HTTP/1.1 200 OK  (JPEG JFIF image)
 921  95.546816   195.7.226.20     192.168.81.143   HTTP      1006 HTTP/1.1 200 OK  (JPEG JFIF image)

> Frame 2: 599 bytes on wire (4792 bits), 599 bytes captured (4792 bits) on interface 0
> Ethernet II, Src: Vmware_e7:d7:0e (00:0c:29:e7:d7:0e), Dst: Vmware_f6:e4:64 (00:50:56:f6:e4:64)

0000  00 50 56 f6 e4 64 00 0c  29 e7 d7 0e 08 00 45 00   .PV..d.. ).....E.
0010  02 49 35 60 40 00 80 06  33 51 c0 a8 51 8f 17 17   .I5`@... 3Q..Q...
0020  66 af c0 08 00 50 56 0d  f9 43 3e f0 11 c5 50 18   f....PV. .C>...P.

Hypertext Transfer Protocol: Protocol    Packets: 3557 · Displayed: 231 (7.7%)    Profile: Default
```

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 recognizeable in ASCII by the string 'JFIF' near the start.
The ASCII view shows that the second image is called Radeon_city.jpg.

The next step taken was carving out the images from the tcp stream, which I did by taking all the hex from FFD8 to FFD9 and copying it into the hex editor program HxD. I then saved the file as a jpg and opened it, resulting in the image below.



I followed the same process for the second image.

Helpful Task Tips & Hints!

- Please note that the relevant traffic is all in http.

- When investigating packet capture files, you can filter the traffic using search terms to isolate certain types of traffic, for example using “http” in the search box, will only display http traffic.
- Once downloaded items have been identified, you will need to investigate them, and rebuild them forensically using a hex viewer.
- In order to rebuild the file you will need to carve out just that file’s hex data, and delete any other hex data surrounding it.

An essential part of solving some of these tasks is identifying what sort of file was downloaded by identifying its *file signature.* A file signature is some data at the start of a file that identifies what sort of file it is. These are usually viewed in hex form.

For example you can identify a jpeg image by its file signature. A jpeg will always start with the hex data “FFD8” and normally ends with the hex data “FFD9”.

Other files can be identified in the same way, with their own unique file signatures.

Please note that some of the downloads made by the user contain more than just the files mentioned in the task template.