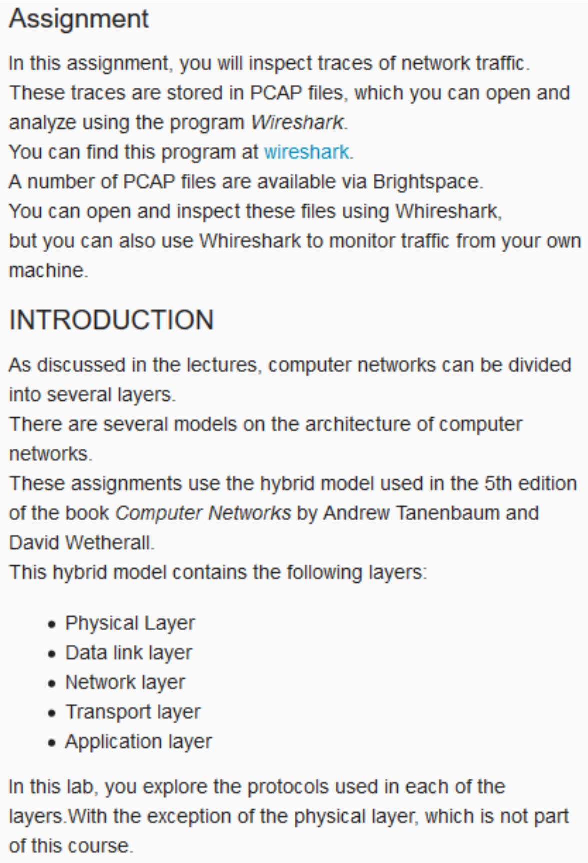
Assignment 4

Network Analysis Basics



Assignment

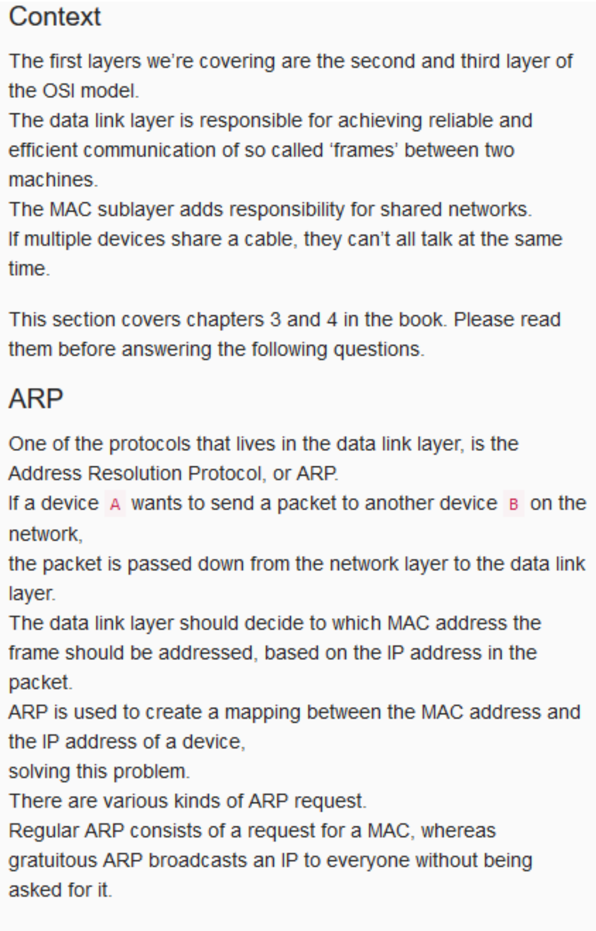
In this assignment, you will inspect traces of network traffic. These traces are stored in PCAP files, which you can open and analyze using the program *Wireshark*. You can find this program at wireshark. A number of PCAP files are available via Brightspace. You can open and inspect these files using Whireshark, but you can also use Whireshark to monitor traffic from your own machine.

INTRODUCTION

As discussed in the lectures, computer networks can be divided into several layers. There are several models on the architecture of computer networks. These assignments use the hybrid model used in the 5th edition of the book *Computer Networks* by Andrew Tanenbaum and David Wetherall. This hybrid model contains the following layers:

- Physical Layer
- Data link layer
- Network layer
- Transport layer
- Application layer

In this lab, you explore the protocols used in each of the layers.With the exception of the physical layer, which is not part of this course.



Context

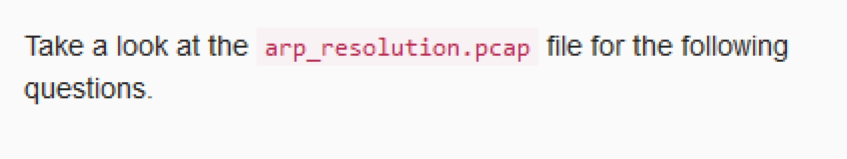
The first layers we're covering are the second and third layer of the OSI model. The data link layer is responsible for achieving reliable and efficient communication of so called 'frames' between two machines. The MAC sublayer adds responsibility for shared networks. If multiple devices share a cable, they can't all talk at the same time.

This section covers chapters 3 and 4 in the book. Please read them before answering the following questions.

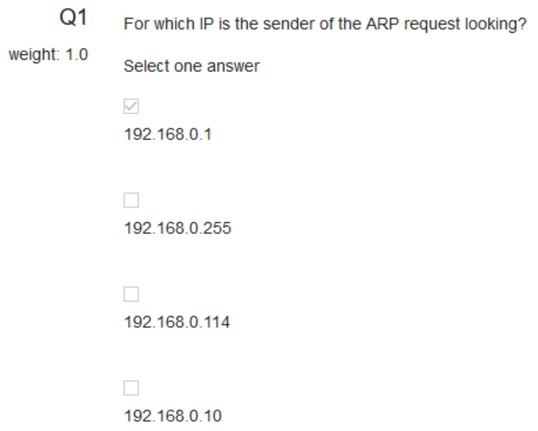
ARP

One of the protocols that lives in the data link layer, is the Address Resolution Protocol, or ARP. If a device `A` wants to send a packet to another device `B` on the network, the packet is passed down from the network layer to the data link layer. The data link layer should decide to which MAC address the frame should be addressed, based on the IP address in the packet. ARP is used to create a mapping between the MAC address and the IP address of a device, solving this problem. There are various kinds of ARP request. Regular ARP consists of a request for a MAC, whereas gratuitous ARP broadcasts an IP to everyone without being asked for it.

Data Link Layer:



Take a look at the `arp_resolution.pcap` file for the following questions.



Q1

weight: 1.0

For which IP is the sender of the ARP request looking?

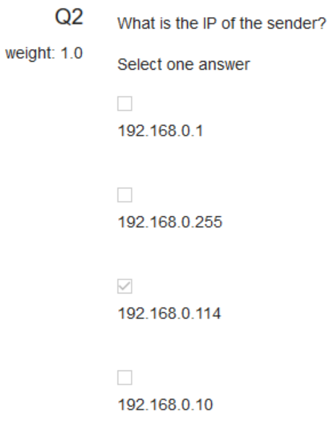
Select one answer

☑ 192.168.0.1

□ 192.168.0.255

□ 192.168.0.114

□ 192.168.0.10



Q2

weight: 1.0

What is the IP of the sender?

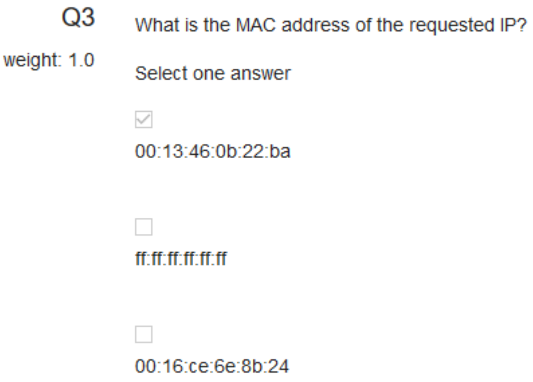
Select one answer

□ 192.168.0.1

□ 192.168.0.255

☑ 192.168.0.114

□ 192.168.0.10


Q3

weight: 1.0

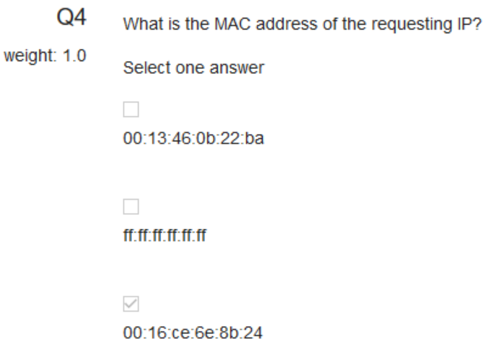
What is the MAC address of the requested IP?

Select one answer

☑ 00:13:46:0b:22:ba

□ ff:ff:ff:ff:ff:ff

□ 00:16:ce:6e:8b:24


Q4

weight: 1.0

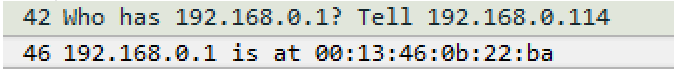
What is the MAC address of the requesting IP?

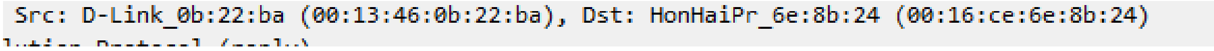
Select one answer

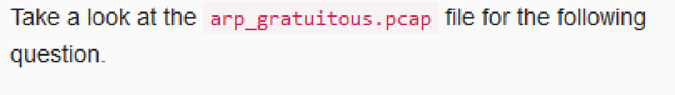
□ 00:13:46:0b:22:ba

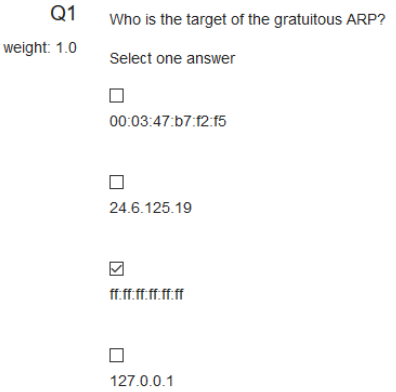
□ ff:ff:ff:ff:ff:ff

☑ 00:16:ce:6e:8b:24


```
42 Who has 192.168.0.1? Tell 192.168.0.114
46 192.168.0.1 is at 00:13:46:0b:22:ba
```


```
Src: D-Link_0b:22:ba (00:13:46:0b:22:ba), Dst: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
```


Take a look at the `arp_gratuitous.pcap` file for the following question.


Q1

weight: 1.0

Who is the target of the gratuitous ARP?

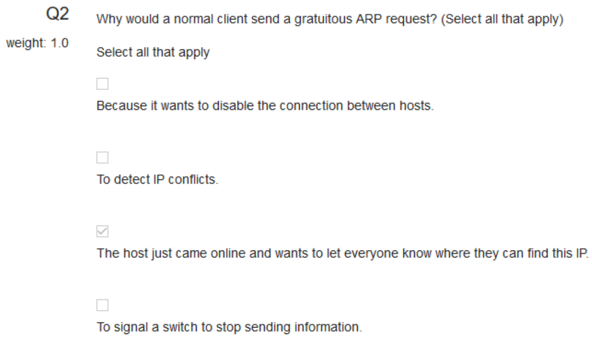
Select one answer

□ 00:03:47:b7:f2:f5

□ 24.6.125.19

☑ ff:ff:ff:ff:ff:ff

□ 127.0.0.1


Q2

weight: 1.0

Why would a normal client send a gratuitous ARP request? (Select all that apply)

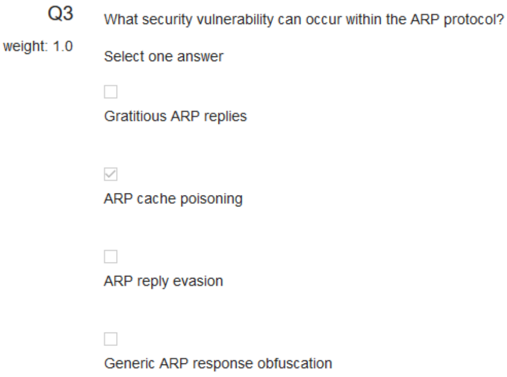
Select all that apply

□ Because it wants to disable the connection between hosts.

□ To detect IP conflicts.

☑ The host just came online and wants to let everyone know where they can find this IP.

□ To signal a switch to stop sending information.


Q3

weight: 1.0

What security vulnerability can occur within the ARP protocol?

Select one answer

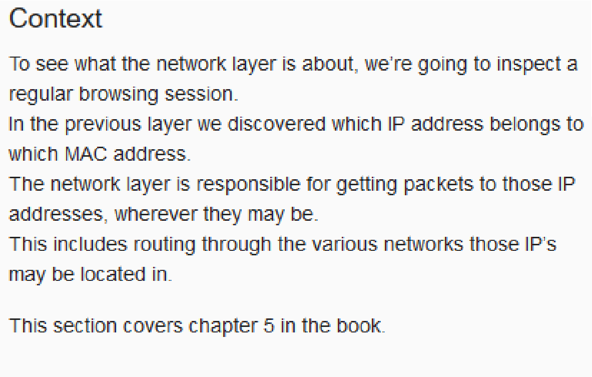
□ Gratitious ARP replies

☑ ARP cache poisoning

□ ARP reply evasion

□ Generic ARP response obfuscation

Network Layer:



Context

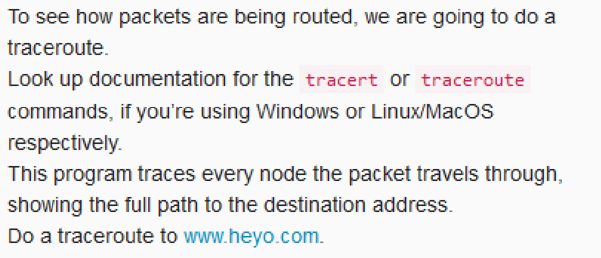
To see what the network layer is about, we're going to inspect a regular browsing session.

In the previous layer we discovered which IP address belongs to which MAC address.

The network layer is responsible for getting packets to those IP addresses, wherever they may be.

This includes routing through the various networks those IP's may be located in.

This section covers chapter 5 in the book.

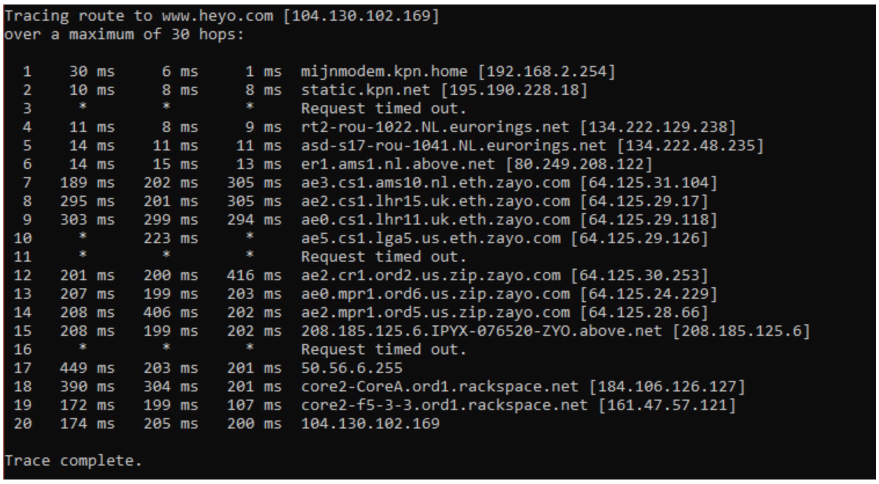


To see how packets are being routed, we are going to do a traceroute.

Look up documentation for the `tracert` or `traceroute` commands, if you're using Windows or Linux/MacOS respectively.

This program traces every node the packet travels through, showing the full path to the destination address.

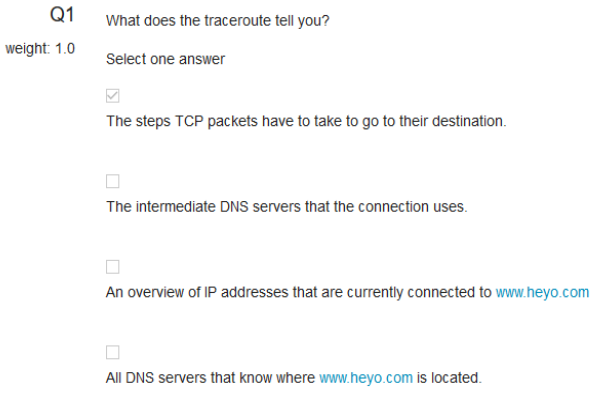
Do a traceroute to www.heyo.com.



```
Tracing route to www.heyo.com [104.130.102.169]
over a maximum of 30 hops:

  1    30 ms     6 ms     1 ms  mijnmodem.kpn.home [192.168.2.254]
  2    10 ms     8 ms     8 ms  static.kpn.net [195.190.228.18]
  3     *        *        *     Request timed out.
  4    11 ms     8 ms     9 ms  rt2-rou-1022.NL.eurorings.net [134.222.129.238]
  5    14 ms    11 ms    11 ms  asd-s17-rou-1041.NL.eurorings.net [134.222.48.235]
  6    14 ms    15 ms    13 ms  er1.ams1.nl.above.net [80.249.208.122]
  7   189 ms   202 ms   305 ms  ae3.cs1.ams10.nl.eth.zayo.com [64.125.31.104]
  8   295 ms   201 ms   305 ms  ae2.cs1.lhr15.uk.eth.zayo.com [64.125.29.17]
  9   303 ms   299 ms   294 ms  ae0.cs1.lhr11.uk.eth.zayo.com [64.125.29.118]
 10     *      223 ms     *     ae5.cs1.lga5.us.eth.zayo.com [64.125.29.126]
 11     *        *        *     Request timed out.
 12   201 ms   200 ms   416 ms  ae2.cr1.ord2.us.zip.zayo.com [64.125.30.253]
 13   207 ms   199 ms   203 ms  ae0.mpr1.ord6.us.zip.zayo.com [64.125.24.229]
 14   208 ms   406 ms   202 ms  ae2.mpr1.ord5.us.zip.zayo.com [64.125.28.66]
 15   208 ms   199 ms   202 ms  208.185.125.6.IPYX-076520-ZYO.above.net [208.185.125.6]
 16     *        *        *     Request timed out.
 17   449 ms   203 ms   201 ms  50.56.6.255
 18   390 ms   304 ms   201 ms  core2-CoreA.ord1.rackspace.net [184.106.126.127]
 19   172 ms   199 ms   107 ms  core2-f5-3-3.ord1.rackspace.net [161.47.57.121]
 20   174 ms   205 ms   200 ms  104.130.102.169

Trace complete.
```



Q1

weight: 1.0

What does the traceroute tell you?

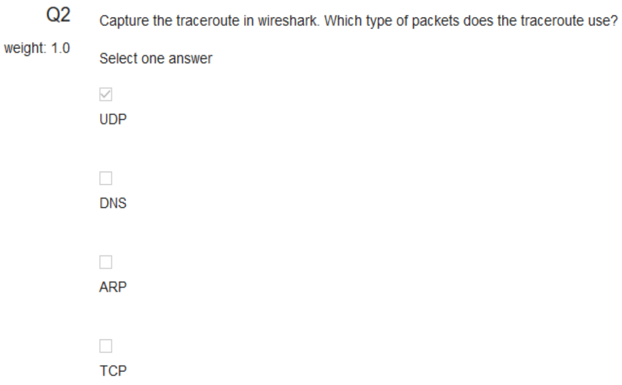
Select one answer

☑ The steps TCP packets have to take to go to their destination.

□ The intermediate DNS servers that the connection uses.

□ An overview of IP addresses that are currently connected to www.heyo.com

□ All DNS servers that know where www.heyo.com is located.



Q2

weight: 1.0

Capture the traceroute in wireshark. Which type of packets does the traceroute use?

Select one answer

☑ UDP

□ DNS

□ ARP

□ TCP

IPv4 vs IPv6

Soon, the supply of available IPv4 address will be depleted.
An alternative is already available in the form of IPv6.

Q1

weight: 1.0

Select all answers that are true with regards to IPv4 and IPv6.

Select all that apply

☑ IPv6 has more addresses than IPv4.

□ IPv4 is obsolete.

☑ The IPv6 header has less fields than the IPv4 header.

□ In IPv6, IP spoofing is not possible anymore.

Q2

weight: 1.0

How many addresses are in IPv4 and IPv6?

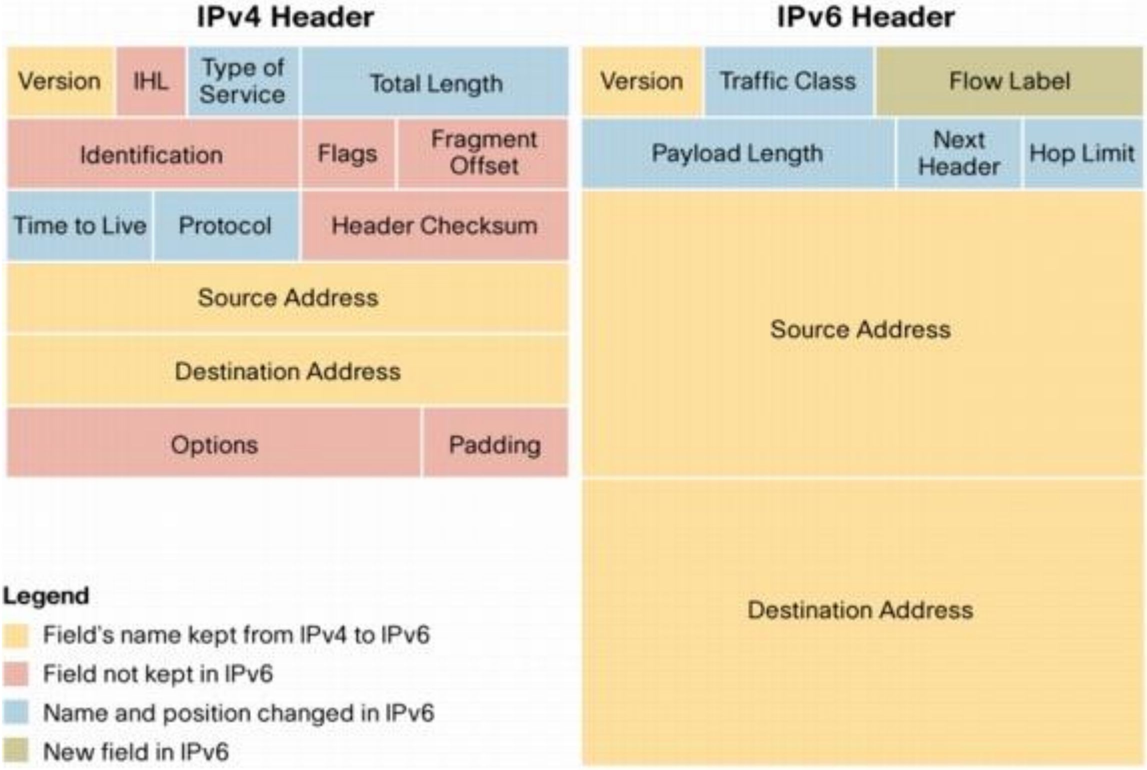
Select one answer

□ IPv4: 2147483648
IPv6: 4294967296

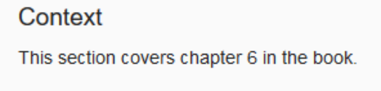
□ IPv4: 1.84467441e19
IPv6: 1.84467441e19

□ IPv4: 2194967296
IPv6: 1.84467441e19

☑ IPv4: 4294967296
IPv6: 3.40282367e38

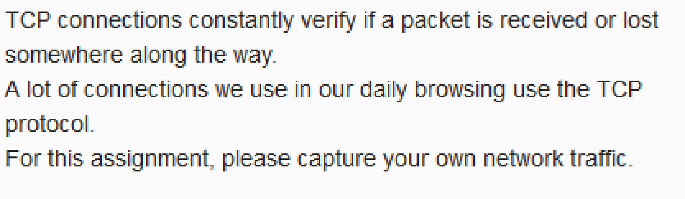


Transport Layer:

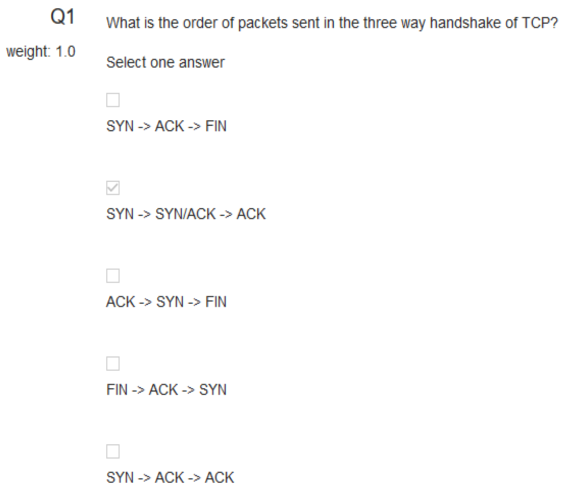


Context

This section covers chapter 6 in the book.



TCP connections constantly verify if a packet is received or lost somewhere along the way.
A lot of connections we use in our daily browsing use the TCP protocol.
For this assignment, please capture your own network traffic.



Q1

weight: 1.0

What is the order of packets sent in the three way handshake of TCP?

Select one answer

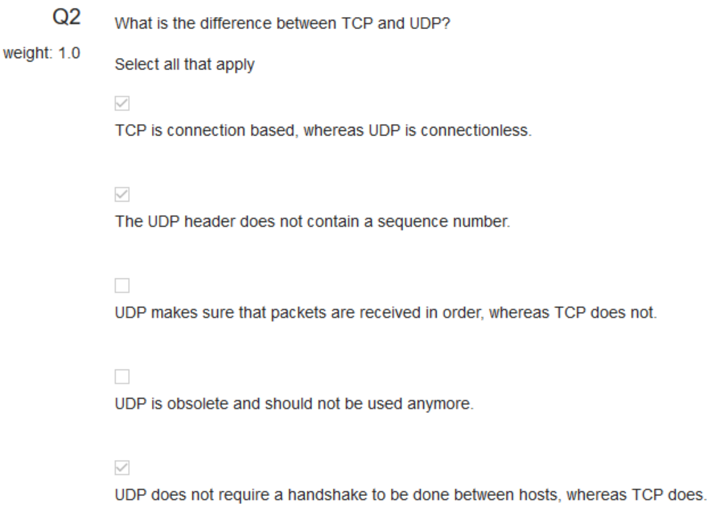
□ SYN -> ACK -> FIN

☑ SYN -> SYN/ACK -> ACK

□ ACK -> SYN -> FIN

□ FIN -> ACK -> SYN

□ SYN -> ACK -> ACK



Q2

weight: 1.0

What is the difference between TCP and UDP?

Select all that apply

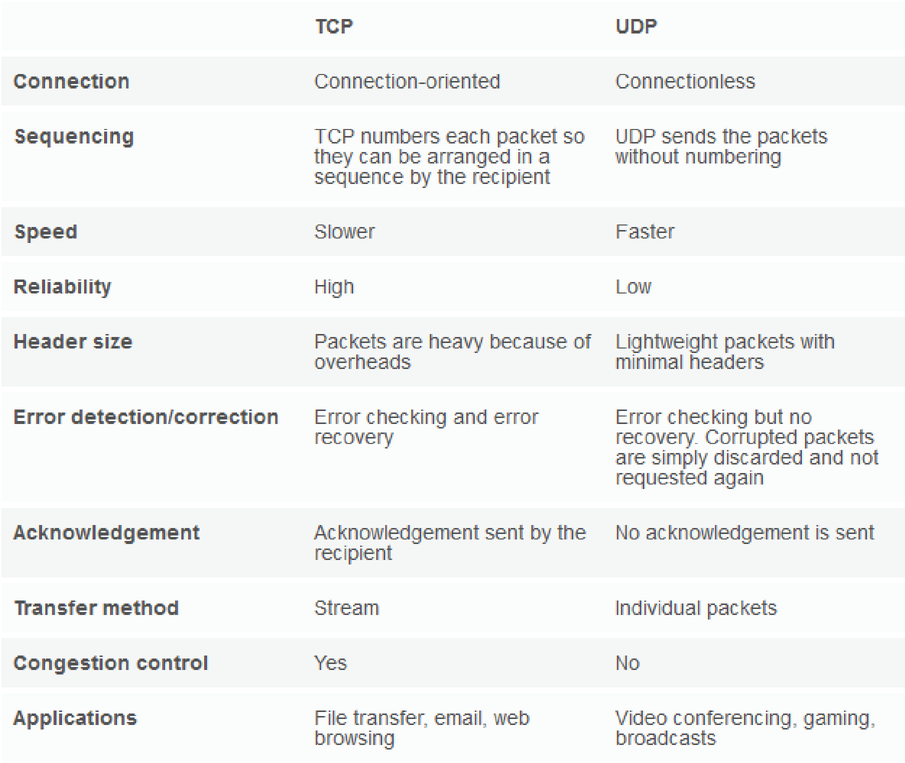
☑ TCP is connection based, whereas UDP is connectionless.

☑ The UDP header does not contain a sequence number.

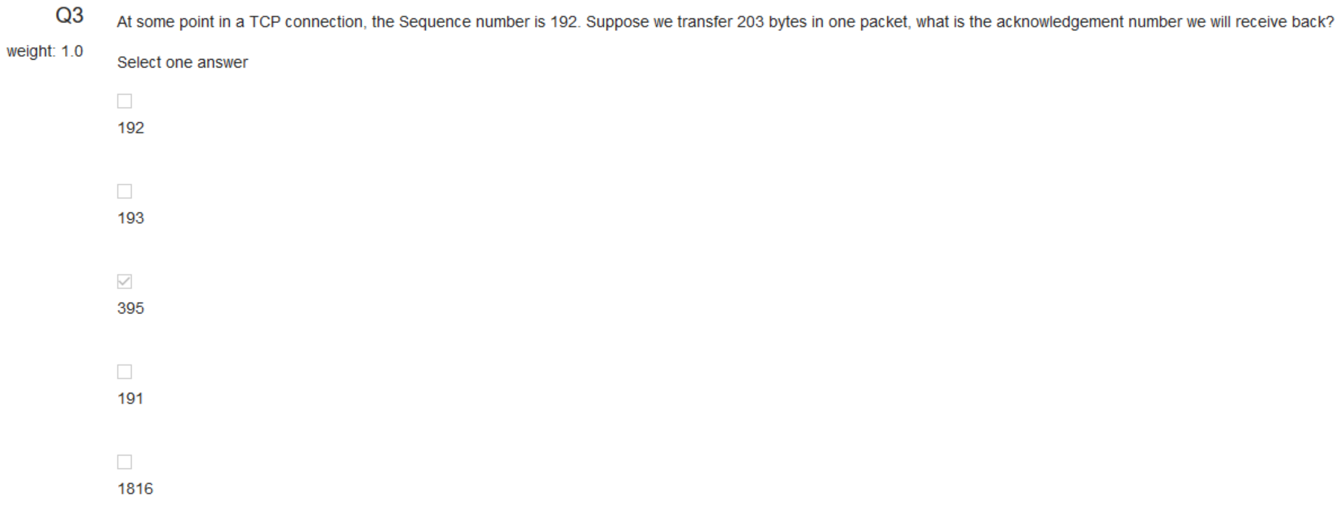
□ UDP makes sure that packets are received in order, whereas TCP does not.

□ UDP is obsolete and should not be used anymore.

☑ UDP does not require a handshake to be done between hosts, whereas TCP does.



	TCP	UDP
Connection	Connection-oriented	Connectionless
Sequencing	TCP numbers each packet so they can be arranged in a sequence by the recipient	UDP sends the packets without numbering
Speed	Slower	Faster
Reliability	High	Low
Header size	Packets are heavy because of overheads	Lightweight packets with minimal headers
Error detection/correction	Error checking and error recovery	Error checking but no recovery. Corrupted packets are simply discarded and not requested again
Acknowledgement	Acknowledgement sent by the recipient	No acknowledgement is sent
Transfer method	Stream	Individual packets
Congestion control	Yes	No
Applications	File transfer, email, web browsing	Video conferencing, gaming, broadcasts



Q3

weight: 1.0

At some point in a TCP connection, the Sequence number is 192. Suppose we transfer 203 bytes in one packet, what is the acknowledgement number we will receive back?

Select one answer

□ 192

□ 193

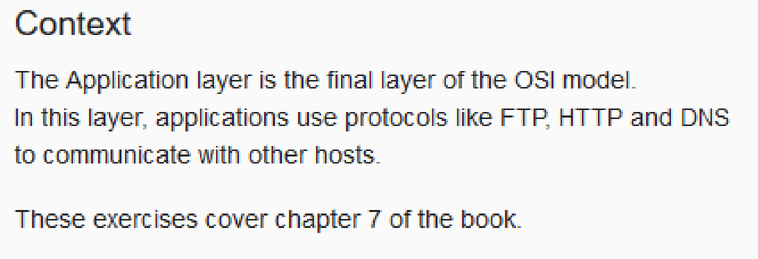
☑ 395

□ 191

□ 1816

Client: sequence number before: 192 after: 192 + 203 = 395
Server: acknowledgment: 395

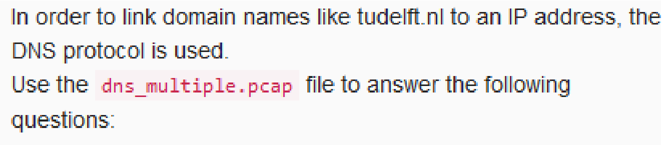
Application Layer:



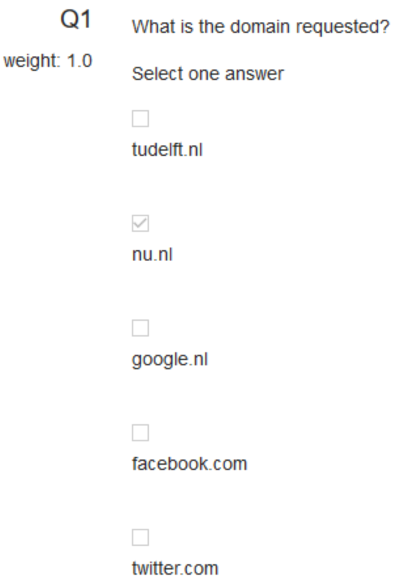
Context

The Application layer is the final layer of the OSI model.
In this layer, applications use protocols like FTP, HTTP and DNS to communicate with other hosts.

These exercises cover chapter 7 of the book.



In order to link domain names like tudelft.nl to an IP address, the DNS protocol is used.
Use the `dns_multiple.pcap` file to answer the following questions:



Q1

weight: 1.0

What is the domain requested?

Select one answer

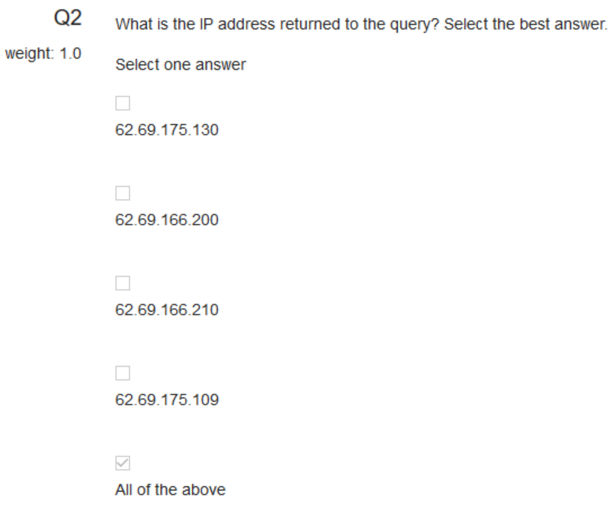
□ tudelft.nl

☑ nu.nl

□ google.nl

□ facebook.com

□ twitter.com



Q2

weight: 1.0

What is the IP address returned to the query? Select the best answer.

Select one answer

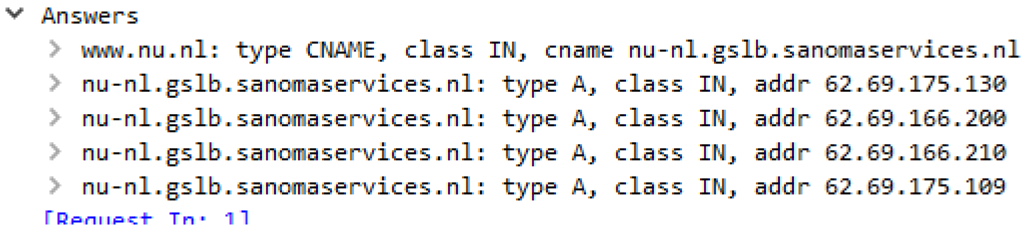
□ 62.69.175.130

□ 62.69.166.200

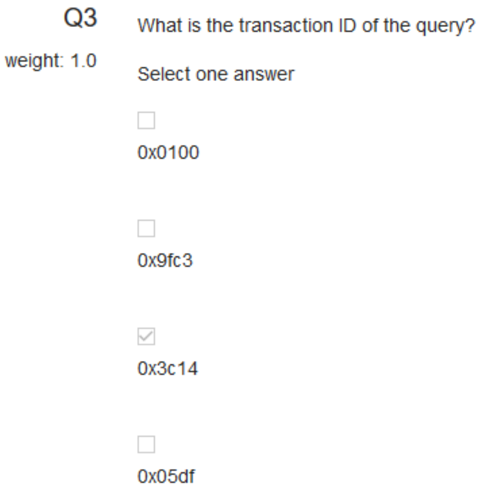
□ 62.69.166.210

□ 62.69.175.109

☑ All of the above



```
⌄ Answers
  › www.nu.nl: type CNAME, class IN, cname nu-nl.gslb.sanomaservices.nl
  › nu-nl.gslb.sanomaservices.nl: type A, class IN, addr 62.69.175.130
  › nu-nl.gslb.sanomaservices.nl: type A, class IN, addr 62.69.166.200
  › nu-nl.gslb.sanomaservices.nl: type A, class IN, addr 62.69.166.210
  › nu-nl.gslb.sanomaservices.nl: type A, class IN, addr 62.69.175.109
[Request In: 1]
```



Q3

weight: 1.0

What is the transaction ID of the query?

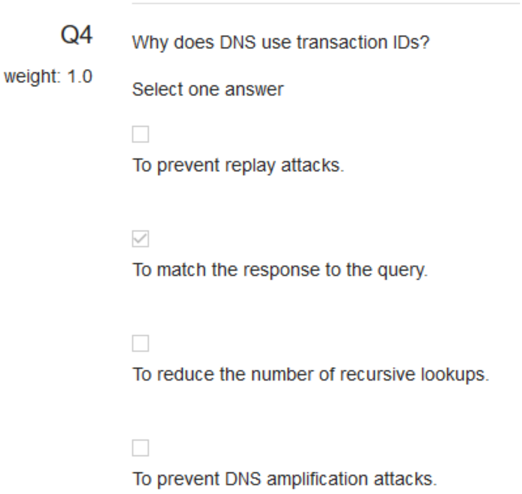
Select one answer

□ 0x0100

□ 0x9fc3

☑ 0x3c14

□ 0x05df



Q4

weight: 1.0

Why does DNS use transaction IDs?

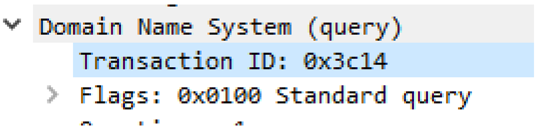
Select one answer

□ To prevent replay attacks.

☑ To match the response to the query.

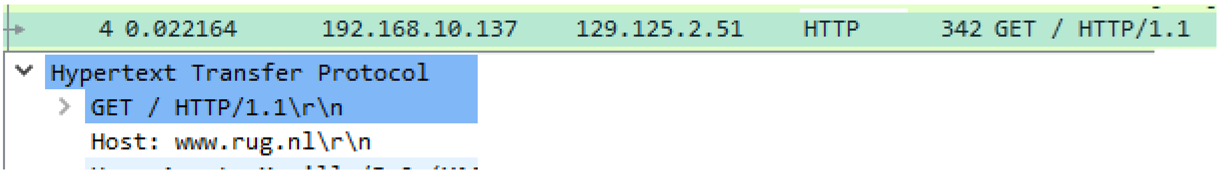
□ To reduce the number of recursive lookups.

□ To prevent DNS amplification attacks.



```
⌄ Domain Name System (query)
    Transaction ID: 0x3c14
  › Flags: 0x0100 Standard query
    Questions: 1
```

For the next exercise we'll be looking into the HTTP protocol.
See the `HTTP_browsing` PCAP.



```
4 0.022164     192.168.10.137    129.125.2.51    HTTP     342 GET / HTTP/1.1
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: www.rug.nl\r\n
```

Q1

weight: 1.0

What website is being visited?

Select one answer

□ tudelft.nl

□ google.com

☑ rug.nl

□ amazon.com

□ delaptophulp.nl

□ brightspace.tudelft.nl

□ outlook.com

Q2

weight: 1.0

What sort of HTTP method is used here?

Select one answer

□ POST

☑ GET

□ HEAD

□ PUT

□ GIVEME

□ SEARCH

□ OPTIONS

Q3

weight: 1.0

What does the 200 OK mean? Select the best answer.

Select one answer

☑ The request was successful.

□ The resource describing the result of the action is transmitted in the message body.

□ The entity headers are in the message body.

□ The message body contains the request message as received by the server.

Q4

weight: 1.0

Which IP is the 'client' and which IP the 'server'?

Select one answer

□ Client: 00:0c:29:23:4f:b6
Server: 00:50:56:e3:84:bd

□ Client: 129.125.2.51
Server: 192.168.10.137

☑ Client: 192.168.10.137
Server: 129.125.2.51

□ Client: 00:50:56:e3:84:bd
Server: 00:0c:29:23:4f:b6

Q5

weight: 1.0

What files are loaded in the PCAP?

Select all that apply

☑ responsive.js

☑ jquery.js

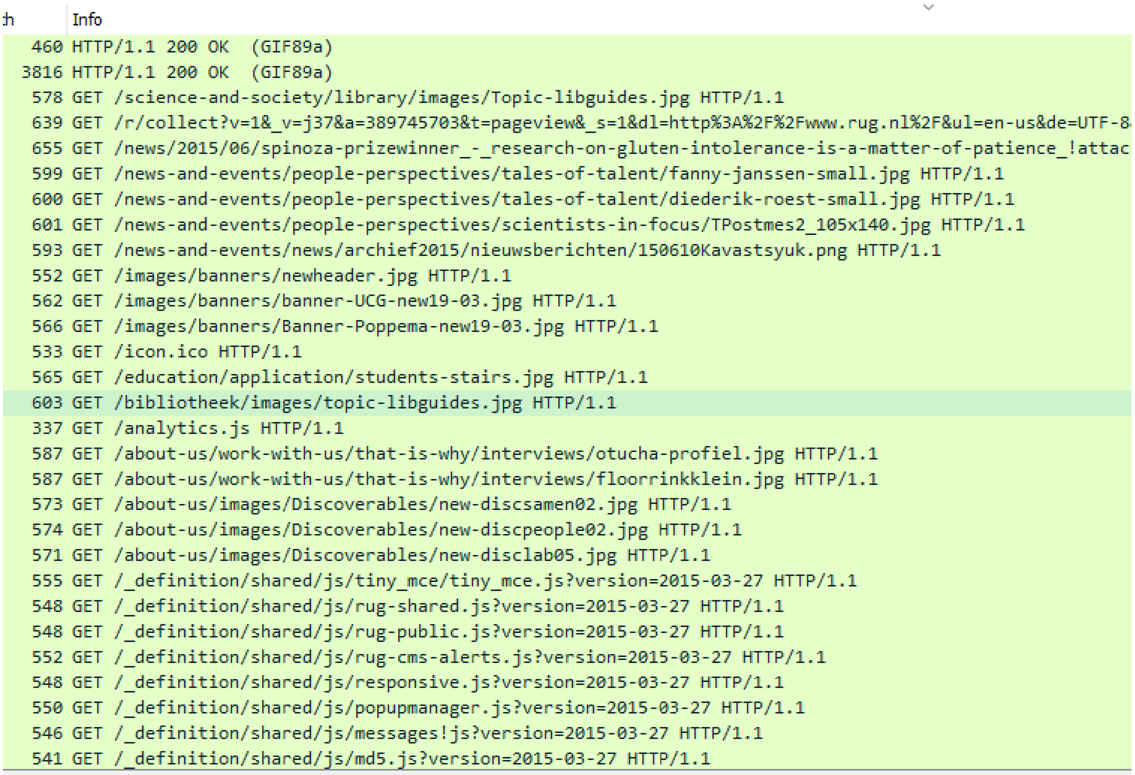
☑ public.css

☑ analytics.js

☑ popupmanager.js

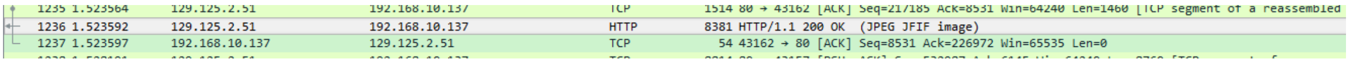
□ wordpress.css

☑ screen.css

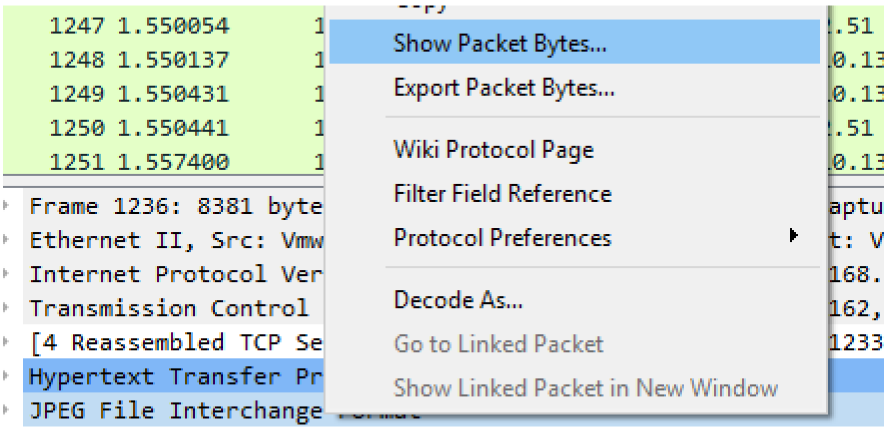


```
h      Info
  460 HTTP/1.1 200 OK  (GIF89a)
 3816 HTTP/1.1 200 OK  (GIF89a)
  578 GET /science-and-society/library/images/Topic-libguides.jpg HTTP/1.1
  639 GET /r/collect?v=1&_v=j37&a=389745703&t=pageview&_s=1&dl=http%3A%2F%2Fwww.rug.nl%2F&ul=en-us&de=UTF-8
  655 GET /news/2015/06/spinoza-prizewinner_-_research-on-gluten-intolerance-is-a-matter-of-patience_!attac
  599 GET /news-and-events/people-perspectives/tales-of-talent/fanny-janssen-small.jpg HTTP/1.1
  600 GET /news-and-events/people-perspectives/tales-of-talent/diederik-roest-small.jpg HTTP/1.1
  601 GET /news-and-events/people-perspectives/scientists-in-focus/TPostmes2_105x140.jpg HTTP/1.1
  593 GET /news-and-events/news/archief2015/nieuwsberichten/150610Kavastsyuk.png HTTP/1.1
  552 GET /images/banners/newheader.jpg HTTP/1.1
  562 GET /images/banners/banner-UCG-new19-03.jpg HTTP/1.1
  566 GET /images/banners/Banner-Poppema-new19-03.jpg HTTP/1.1
  533 GET /icon.ico HTTP/1.1
  565 GET /education/application/students-stairs.jpg HTTP/1.1
  603 GET /bibliotheek/images/topic-libguides.jpg HTTP/1.1
  337 GET /analytics.js HTTP/1.1
  587 GET /about-us/work-with-us/that-is-why/interviews/otucha-profiel.jpg HTTP/1.1
  587 GET /about-us/work-with-us/that-is-why/interviews/floorrinkklein.jpg HTTP/1.1
  573 GET /about-us/images/Discoverables/new-discsamen02.jpg HTTP/1.1
  574 GET /about-us/images/Discoverables/new-discpeople02.jpg HTTP/1.1
  571 GET /about-us/images/Discoverables/new-disclab05.jpg HTTP/1.1
  555 GET /_definition/shared/js/tiny_mce/tiny_mce.js?version=2015-03-27 HTTP/1.1
  548 GET /_definition/shared/js/rug-shared.js?version=2015-03-27 HTTP/1.1
  548 GET /_definition/shared/js/rug-public.js?version=2015-03-27 HTTP/1.1
  552 GET /_definition/shared/js/rug-cms-alerts.js?version=2015-03-27 HTTP/1.1
  548 GET /_definition/shared/js/responsive.js?version=2015-03-27 HTTP/1.1
  550 GET /_definition/shared/js/popupmanager.js?version=2015-03-27 HTTP/1.1
  546 GET /_definition/shared/js/messages!js?version=2015-03-27 HTTP/1.1
  541 GET /_definition/shared/js/md5.js?version=2015-03-27 HTTP/1.1
```

(Sorted by info)



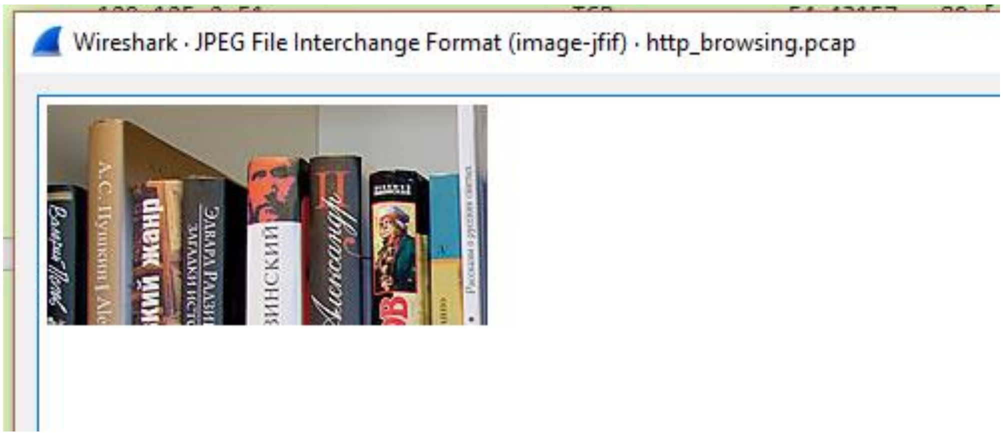
```
1235 1.523564   129.125.2.51     192.168.10.137   TCP    1514 80 → 43162 [ACK] Seq=217185 Ack=8531 Win=64240 Len=1460 [TCP segment of a reassembled
1236 1.523592   129.125.2.51     192.168.10.137   HTTP   8381 HTTP/1.1 200 OK  (JPEG JFIF image)
1237 1.523597   192.168.10.137   129.125.2.51     TCP      54 43162 → 80 [ACK] Seq=8531 Ack=226972 Win=65535 Len=0
```



```
1247 1.550054      1
1248 1.550137      1
1249 1.550431      1
1250 1.550441      1
1251 1.557400      1
```

```
Frame 1236: 8381 byte
Ethernet II, Src: Vmw
Internet Protocol Ver
Transmission Control
[4 Reassembled TCP Se
Hypertext Transfer Pr
JPEG File Interchange
```

(right-click JPEG file Interchange format and show)



Wireshark · JPEG File Interchange Format (image-jfif) · http_browsing.pcap

Q6

weight: 1.0

In Wireshark, you can use the function “Show packet bytes” on the **data** field. Use this function to view the last JPEG image. What does this image show?

Select one answer

□ A Scientist

□ Buildings

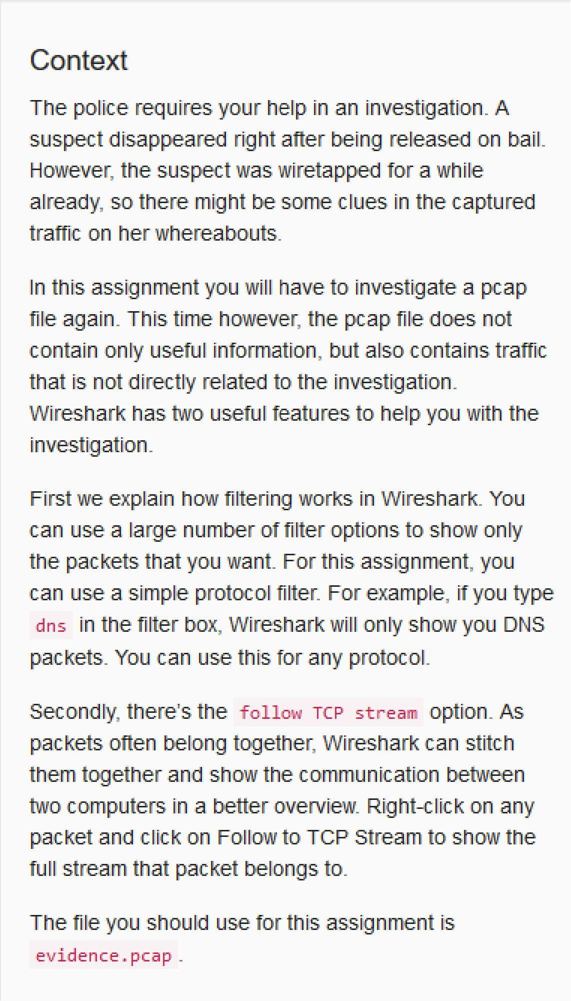
☑ Books

□ A grass field

□ Website icons

□ Water

Network Forensics



Context

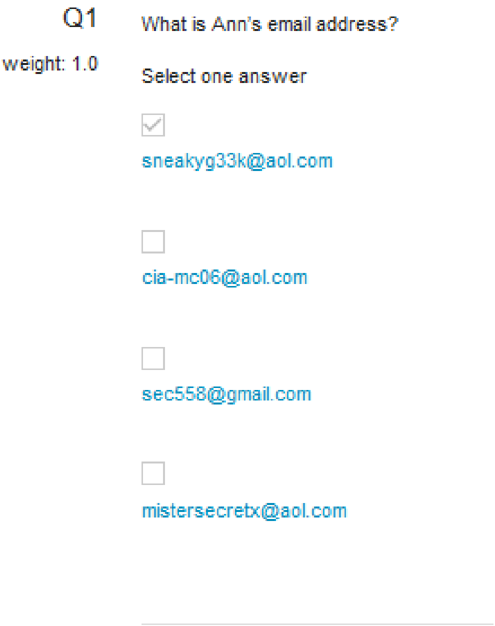
The police requires your help in an investigation. A suspect disappeared right after being released on bail. However, the suspect was wiretapped for a while already, so there might be some clues in the captured traffic on her whereabouts.

In this assignment you will have to investigate a pcap file again. This time however, the pcap file does not contain only useful information, but also contains traffic that is not directly related to the investigation. Wireshark has two useful features to help you with the investigation.

First we explain how filtering works in Wireshark. You can use a large number of filter options to show only the packets that you want. For this assignment, you can use a simple protocol filter. For example, if you type `dns` in the filter box, Wireshark will only show you DNS packets. You can use this for any protocol.

Secondly, there's the `follow TCP stream` option. As packets often belong together, Wireshark can stitch them together and show the communication between two computers in a better overview. Right-click on any packet and click on Follow to TCP Stream to show the full stream that packet belongs to.

The file you should use for this assignment is `evidence.pcap`.



Q1

weight: 1.0

What is Ann's email address?

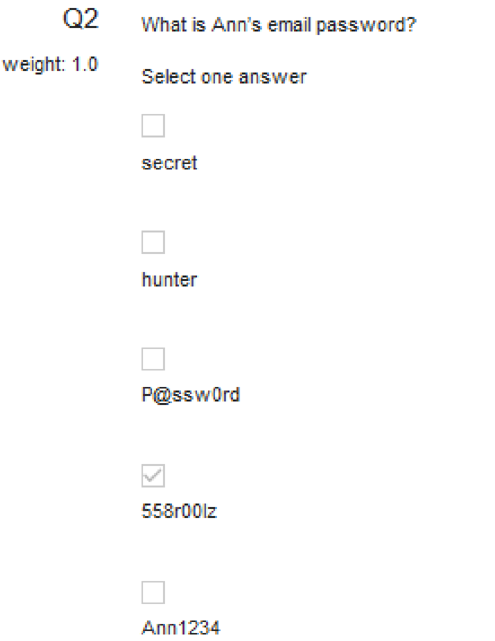
Select one answer

☑ sneakyg33k@aol.com

□ cia-mc06@aol.com

□ sec558@gmail.com

□ mistersecretx@aol.com



Q2

weight: 1.0

What is Ann's email password?

Select one answer

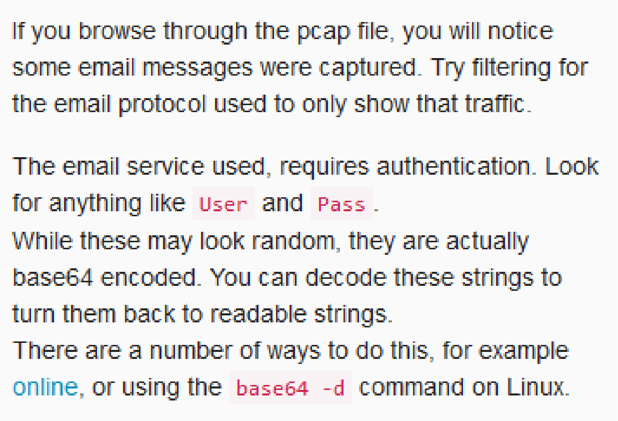
□ secret

□ hunter

□ P@ssw0rd

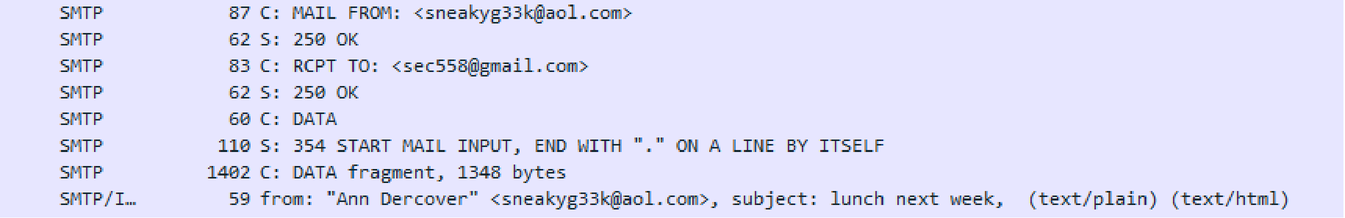
☑ 558r00lz

□ Ann1234

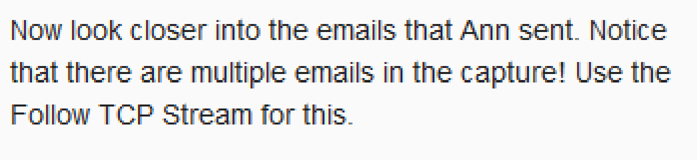


If you browse through the pcap file, you will notice some email messages were captured. Try filtering for the email protocol used to only show that traffic.

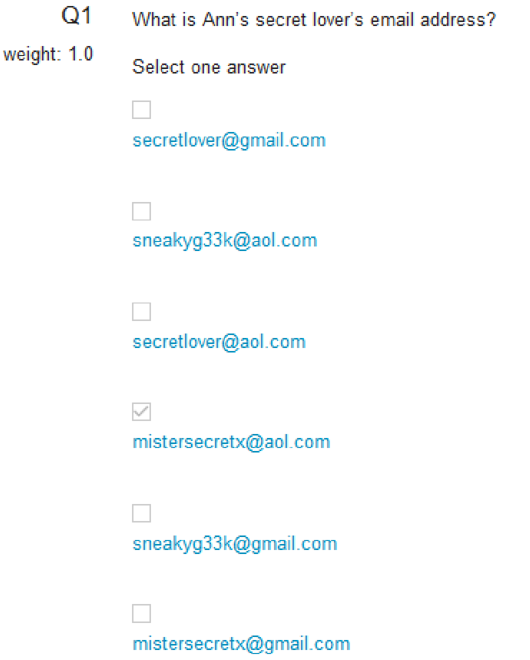
The email service used, requires authentication. Look for anything like `User` and `Pass`.
While these may look random, they are actually base64 encoded. You can decode these strings to turn them back to readable strings.
There are a number of ways to do this, for example online, or using the `base64 -d` command on Linux.



```
SMTP           87 C: MAIL FROM: <sneakyg33k@aol.com>
SMTP           62 S: 250 OK
SMTP           83 C: RCPT TO: <sec558@gmail.com>
SMTP           62 S: 250 OK
SMTP           60 C: DATA
SMTP          110 S: 354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF
SMTP         1402 C: DATA fragment, 1348 bytes
SMTP/I…        59 from: "Ann Dercover" <sneakyg33k@aol.com>, subject: lunch next week,  (text/plain) (text/html)
```



Now look closer into the emails that Ann sent. Notice that there are multiple emails in the capture! Use the Follow TCP Stream for this.



Q1
weight: 1.0

What is Ann's secret lover's email address?

Select one answer

□ secretlover@gmail.com

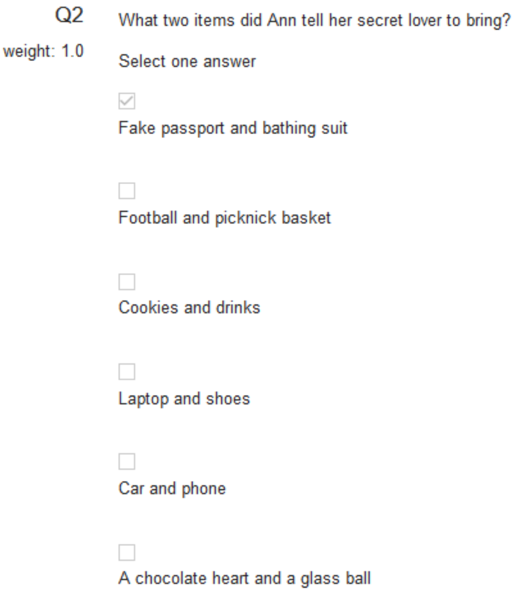
□ sneakyg33k@aol.com

□ secretlover@aol.com

☑ mistersecretx@aol.com

□ sneakyg33k@gmail.com

□ mistersecretx@gmail.com



Q2
weight: 1.0

What two items did Ann tell her secret lover to bring?

Select one answer

☑ Fake passport and bathing suit

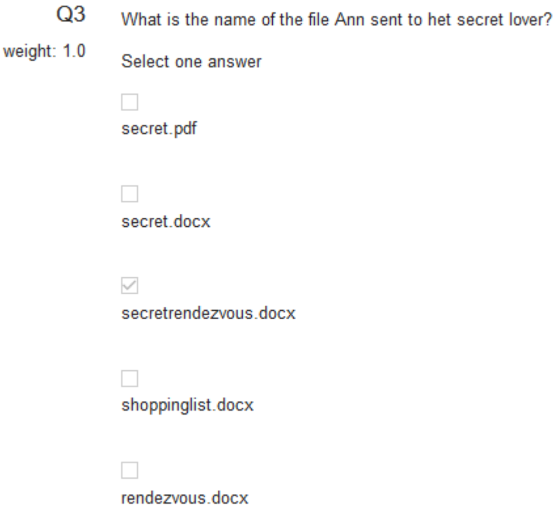
□ Football and picknick basket

□ Cookies and drinks

□ Laptop and shoes

□ Car and phone

□ A chocolate heart and a glass ball



Q3
weight: 1.0

What is the name of the file Ann sent to het secret lover?

Select one answer

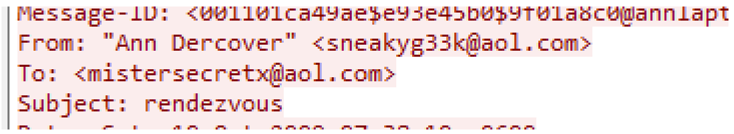
□ secret.pdf

□ secret.docx

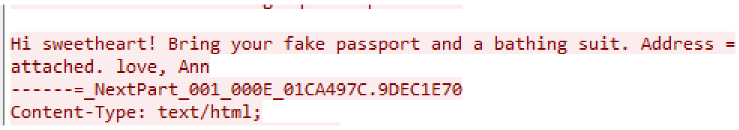
☑ secretrendezvous.docx

□ shoppinglist.docx

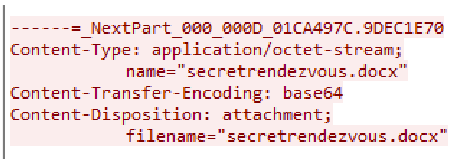
□ rendezvous.docx



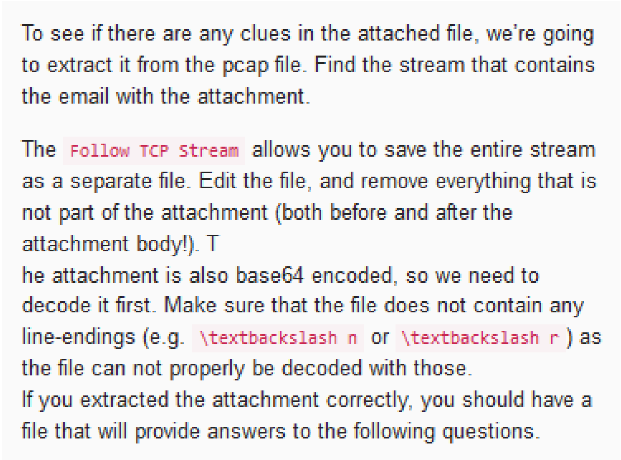
```
Message-ID: <001101ca49ae$e93e45b0$9f01a8c0@annlapt
From: "Ann Dercover" <sneakyg33k@aol.com>
To: <mistersecretx@aol.com>
Subject: rendezvous
```



```
Hi sweetheart! Bring your fake passport and a bathing suit. Address =
attached. love, Ann
------=_NextPart_001_000E_01CA497C.9DEC1E70
Content-Type: text/html;
```

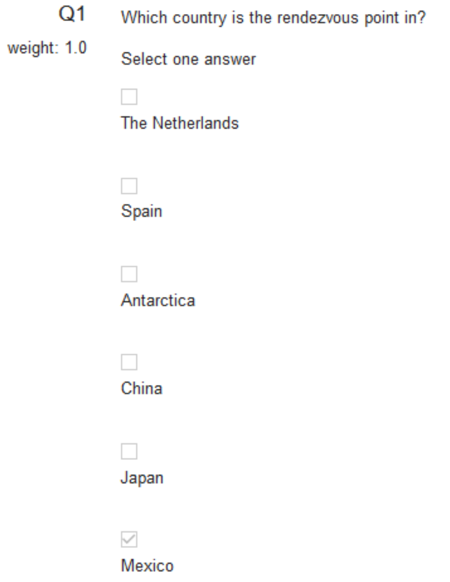


```
------=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: application/octet-stream;
        name="secretrendezvous.docx"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        filename="secretrendezvous.docx"
```



To see if there are any clues in the attached file, we're going to extract it from the pcap file. Find the stream that contains the email with the attachment.

The `Follow TCP Stream` allows you to save the entire stream as a separate file. Edit the file, and remove everything that is not part of the attachment (both before and after the attachment body!). T
he attachment is also base64 encoded, so we need to decode it first. Make sure that the file does not contain any line-endings (e.g. `\textbackslash n` or `\textbackslash r`) as the file can not properly be decoded with those.
If you extracted the attachment correctly, you should have a file that will provide answers to the following questions.



Q1

weight: 1.0

Which country is the rendezvous point in?

Select one answer

□ The Netherlands

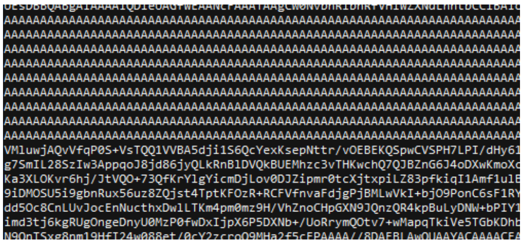
□ Spain

□ Antarctica

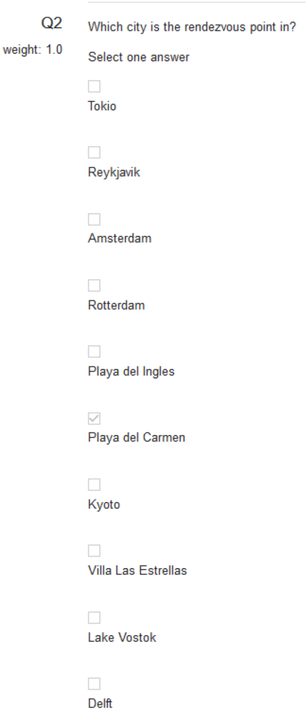
□ China

□ Japan

☑ Mexico



```
UEsDBBQABgAIAAAAIQDIeUAGYWEAANCPAAATAAgCW0NvbnRlbnRfVHlwZXNdLnhtbCCiBAIo
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
VMluwjAQvVfqP0S+VsTQQ1VVBA5dji1S6QcYexKsepNttr/vOEBEKQSpwCVSPH7LPI/dHy61
g7SmIL28SzIw3AppqoJ8jd86jyQLkRnBlDVQkBUEMhzc3vTHKwchQ7QJBZnG6J4oDXwKmoXc
Ka3XLOKvr6hj/JtVQO+73QfKrYlgYicmDjLov0DJZipmr0tcXjtxpiLZ83pfkiqI1Amf1ulE
9iDMOSU5i9gbnRux56uz8ZQjst4TptKFOzR+RCFVfnvaFdjgPjBMLwVkI+bjO9PonC6sF1RY
dd5Oc8CnLUvJocEnNucthxDwlLTKm4pm0mz9H/VhZnoCHpGXN9JQnzQR4kpBuLyDNW+bPIY1
imd3tj6kgRUgOngeDnyU0MzP0fwDxIjpX6P5DXNb+/UoRrymQOtv7+wMapqTkiVe5TGbKDhb
N9OnISxg8nm19HfI24w088et/0cY2zcroO9MHa2f5cFPAAAA//8DAFBLAwQUAAYACAAAACEA
```



Q2

weight: 1.0

Which city is the rendezvous point in?

Select one answer

□ Tokio

□ Reykjavik

□ Amsterdam

□ Rotterdam

□ Playa del Ingles

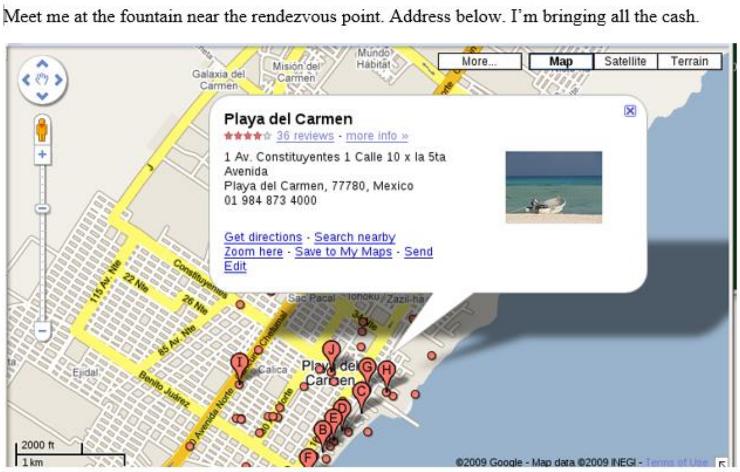
☑ Playa del Carmen

□ Kyoto

□ Villa Las Estrellas

□ Lake Vostok

□ Delft



Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.

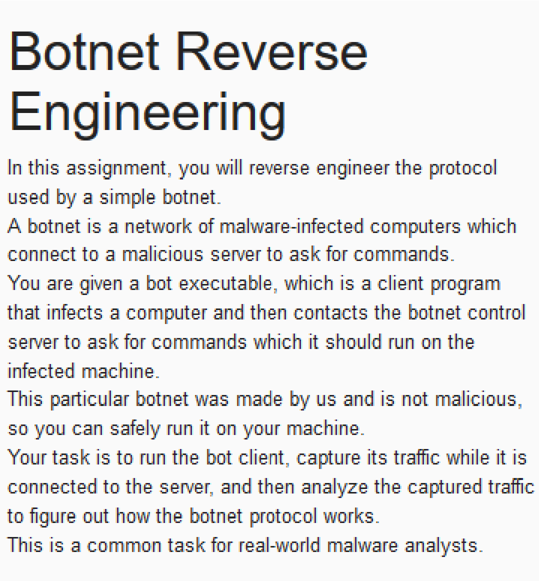
Playa del Carmen

★★★★☆ 36 reviews · more info »

1 Av. Constituyentes 1 Calle 10 x la 5ta
Avenida
Playa del Carmen, 77780, Mexico
01 984 873 4000

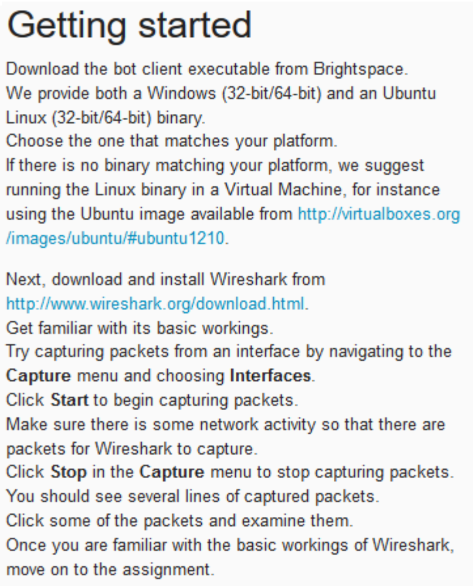
Get directions · Search nearby
Zoom here · Save to My Maps · Send
Edit

Botnet reverse Engineering



Botnet Reverse Engineering

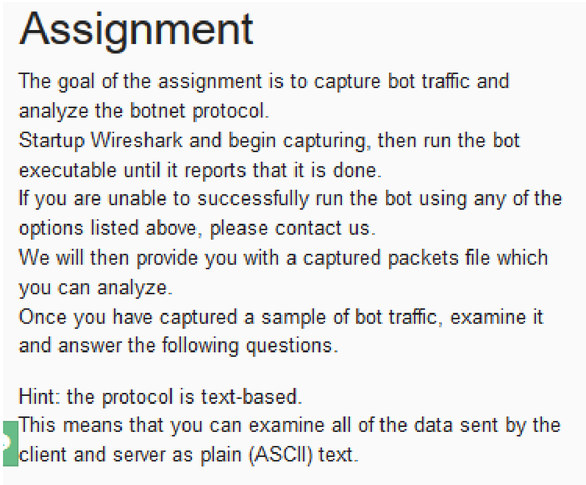
In this assignment, you will reverse engineer the protocol used by a simple botnet.
A botnet is a network of malware-infected computers which connect to a malicious server to ask for commands.
You are given a bot executable, which is a client program that infects a computer and then contacts the botnet control server to ask for commands which it should run on the infected machine.
This particular botnet was made by us and is not malicious, so you can safely run it on your machine.
Your task is to run the bot client, capture its traffic while it is connected to the server, and then analyze the captured traffic to figure out how the botnet protocol works.
This is a common task for real-world malware analysts.



Getting started

Download the bot client executable from Brightspace.
We provide both a Windows (32-bit/64-bit) and an Ubuntu Linux (32-bit/64-bit) binary.
Choose the one that matches your platform.
If there is no binary matching your platform, we suggest running the Linux binary in a Virtual Machine, for instance using the Ubuntu image available from http://virtualboxes.org/images/ubuntu/#ubuntu1210.

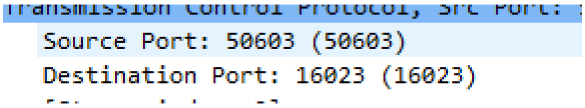
Next, download and install Wireshark from http://www.wireshark.org/download.html.
Get familiar with its basic workings.
Try capturing packets from an interface by navigating to the **Capture** menu and choosing **Interfaces**.
Click **Start** to begin capturing packets.
Make sure there is some network activity so that there are packets for Wireshark to capture.
Click **Stop** in the **Capture** menu to stop capturing packets.
You should see several lines of captured packets.
Click some of the packets and examine them.
Once you are familiar with the basic workings of Wireshark, move on to the assignment.



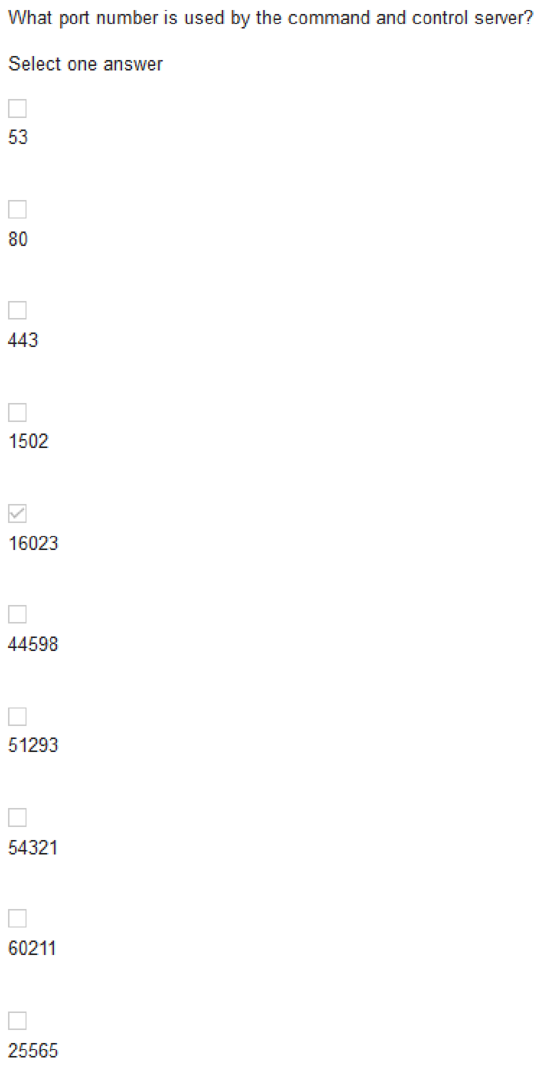
Assignment

The goal of the assignment is to capture bot traffic and analyze the botnet protocol.
Startup Wireshark and begin capturing, then run the bot executable until it reports that it is done.
If you are unable to successfully run the bot using any of the options listed above, please contact us.
We will then provide you with a captured packets file which you can analyze.
Once you have captured a sample of bot traffic, examine it and answer the following questions.

Hint: the protocol is text-based.
This means that you can examine all of the data sent by the client and server as plain (ASCII) text.



```
Transmission Control Protocol, Src Port: 
    Source Port: 50603 (50603)
    Destination Port: 16023 (16023)
```



What port number is used by the command and control server?

Select one answer

□ 53

□ 80

□ 443

□ 1502

☑ 16023

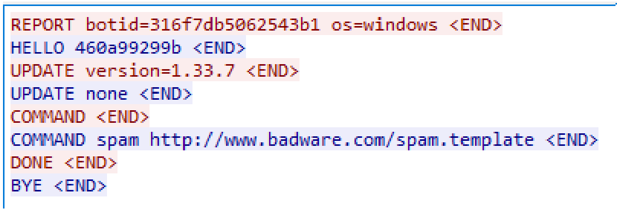
□ 44598

□ 51293

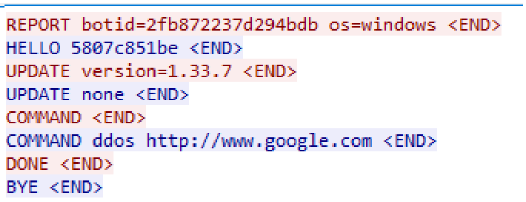
□ 54321

□ 60211

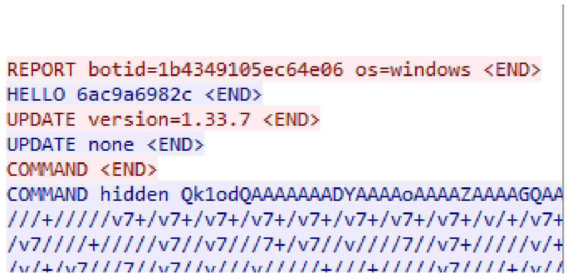
□ 25565



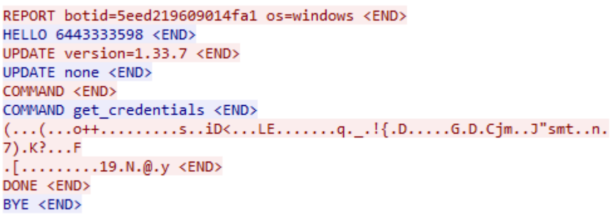
```
REPORT botid=316f7db5062543b1 os=windows <END>
HELLO 460a99299b <END>
UPDATE version=1.33.7 <END>
UPDATE none <END>
COMMAND <END>
COMMAND spam http://www.badware.com/spam.template <END>
DONE <END>
BYE <END>
```



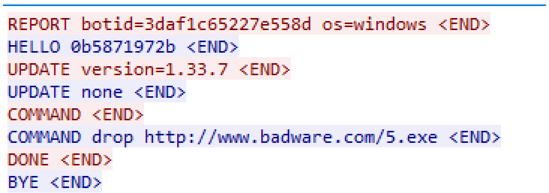
```
REPORT botid=2fb872237d294bdb os=windows <END>
HELLO 5807c851be <END>
UPDATE version=1.33.7 <END>
UPDATE none <END>
COMMAND <END>
COMMAND ddos http://www.google.com <END>
DONE <END>
BYE <END>
```



```
REPORT botid=1b4349105ec64e06 os=windows <END>
HELLO 6ac9a6982c <END>
UPDATE version=1.33.7 <END>
UPDATE none <END>
COMMAND <END>
COMMAND hidden Qk1odQAAAAAAADYAAAAoAAAAZAAAAGQAA
///+/////v7+/v7+/v7+/v7+/v7+/v7+/v7+/v/+/v7+
/v7////+/////v7//v7///7+/v7//v////7//v7+/////v/+
/v/+/v7///7//v7//v///v/////+///+/////v7////+/v//
```



```
REPORT botid=5eed219609014fa1 os=windows <END>
HELLO 6443333598 <END>
UPDATE version=1.33.7 <END>
UPDATE none <END>
COMMAND <END>
COMMAND get_credentials <END>
(...(...o++.........s..iD<...LE.......q._.!{.D.....G.D.Cjm..J"smt..n.
7).K?...F
.[.........19.N.@.y <END>
DONE <END>
BYE <END>
```



```
REPORT botid=3daf1c65227e558d os=windows <END>
HELLO 0b5871972b <END>
UPDATE version=1.33.7 <END>
UPDATE none <END>
COMMAND <END>
COMMAND drop http://www.badware.com/5.exe <END>
DONE <END>
BYE <END>
```

The botnet supports 5 different commands.
What are they?
You may have to run the bot several times to see all the commands.

Select all that apply

☑ ddos

☑ spam

☑ hidden

☑ drop

☐ infect

☐ weaponize

☐ hack

☐ break

☐ sudo

☐ extract_data

☑ get_credentials

What is the version number of the given bot client?

Select one answer

☐ 1

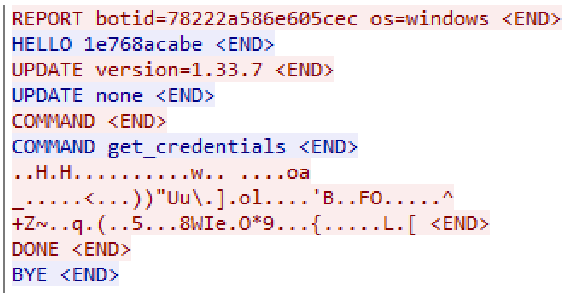
☑ 1.33.7

☐ 3.4

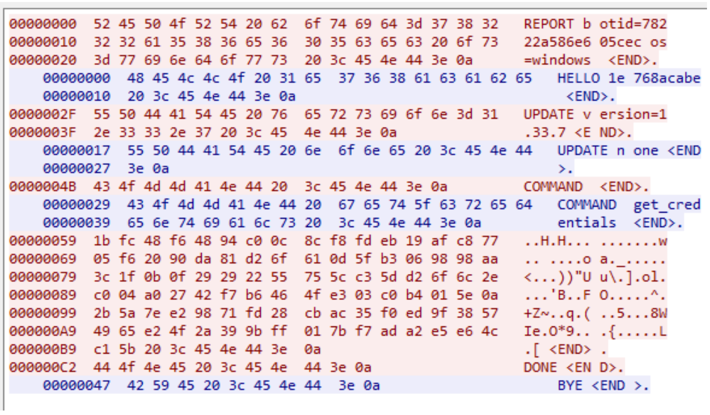
☐ h4.xx.0r

☐ Version 0x1234

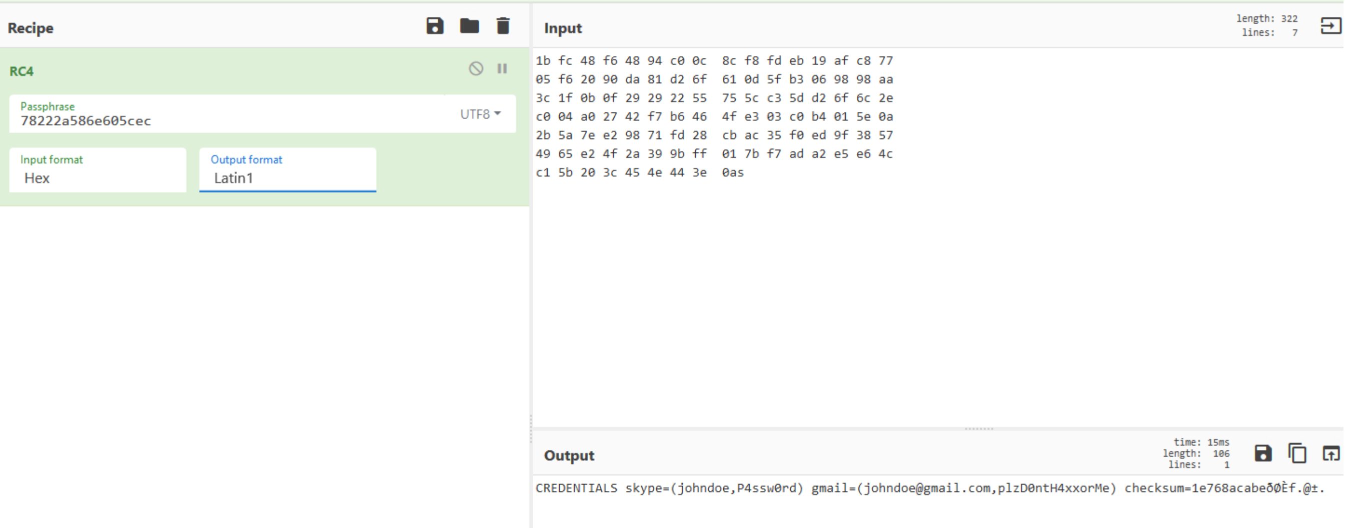
☐ 2



```
REPORT botid=78222a586e605cec os=windows <END>
HELLO 1e768acabe <END>
UPDATE version=1.33.7 <END>
UPDATE none <END>
COMMAND <END>
COMMAND get_credentials <END>
..H.H...........w.. ....oa
_.....<...))"Uu\.].ol....'B..FO.....^
+Z~..q.(..5...8WIe.O*9...{.....L.[ <END>
DONE <END>
BYE <END>
```



```
00000000  52 45 50 4f 52 54 20 62  6f 74 69 64 3d 37 38 32   REPORT b otid=782
00000010  32 32 61 35 38 36 65 36  30 35 63 65 63 20 6f 73   22a586e6 05cec os
00000020  3d 77 69 6e 64 6f 77 73  20 3c 45 4e 44 3e 0a      =windows  <END>.
    00000000  48 45 4c 4c 4f 20 31 65  37 36 38 61 63 61 62 65   HELLO 1e 768acabe
    00000010  20 3c 45 4e 44 3e 0a                               <END>.
0000002F  55 50 44 41 54 45 20 76  65 72 73 69 6f 6e 3d 31   UPDATE v ersion=1
0000003F  2e 33 33 2e 37 20 3c 45  4e 44 3e 0a               .33.7 <E ND>.
    00000017  55 50 44 41 54 45 20 6e  6f 6e 65 20 3c 45 4e 44   UPDATE n one <END
    00000027  3e 0a                                              >.
0000004B  43 4f 4d 4d 41 4e 44 20  3c 45 4e 44 3e 0a         COMMAND  <END>.
    00000029  43 4f 4d 4d 41 4e 44 20  67 65 74 5f 63 72 65 64   COMMAND  get_cred
    00000039  65 6e 74 69 61 6c 73 20  3c 45 4e 44 3e 0a         entials  <END>.
00000059  1b fc 48 f6 48 94 c0 0c  8c f8 fd eb 19 af c8 77   ..H.H... .......w
00000069  05 f6 20 90 da 81 d2 6f  61 0d 5f b3 06 98 98 aa   .. ....o a._.....
00000079  3c 1f 0b 0f 29 29 22 55  75 5c c3 5d d2 6f 6c 2e   <...))"U u\.].ol.
00000089  c0 04 a0 27 42 f7 b6 46  4f e3 03 c0 b4 01 5e 0a   ...'B..F O.....^.
00000099  2b 5a 7e e2 98 71 fd 28  cb ac 35 f0 ed 9f 38 57   +Z~..q.( ..5...8W
000000A9  49 65 e2 4f 2a 39 9b ff  01 7b f7 ad a2 e5 e6 4c   Ie.O*9.. .{.....L
000000B9  c1 5b 20 3c 45 4e 44 3e  0a                        .[ <END> .
000000C2  44 4f 4e 45 20 3c 45 4e  44 3e 0a                  DONE <EN D>.
    00000047  42 59 45 20 3c 45 4e 44  3e 0a                        BYE <END >.
```



RC4

Passphrase: 78222a586e605cec UTF8

Input format: Hex

Output format: Latin1

Input — length: 322 lines: 7

```
1b fc 48 f6 48 94 c0 0c  8c f8 fd eb 19 af c8 77
05 f6 20 90 da 81 d2 6f  61 0d 5f b3 06 98 98 aa
3c 1f 0b 0f 29 29 22 55  75 5c c3 5d d2 6f 6c 2e
c0 04 a0 27 42 f7 b6 46  4f e3 03 c0 b4 01 5e 0a
2b 5a 7e e2 98 71 fd 28  cb ac 35 f0 ed 9f 38 57
49 65 e2 4f 2a 39 9b ff  01 7b f7 ad a2 e5 e6 4c
c1 5b 20 3c 45 4e 44 3e  0as
```

Output — time: 15ms length: 106 lines: 1

```
CREDENTIALS skype=(johndoe,P4ssw0rd) gmail=(johndoe@gmail.com,plzD0ntH4xxorMe) checksum=1e768acabeðØÈf.@±.
```

The protocol includes a single encrypted message type, which is sent to the server after a certain kind of command is received.
You may have to run the bot multiple times to see the encrypted message.
Try to find out how this message is encrypted, and then decrypt it.
What information is sent by the server? Select the best answer,

Hint: the encryption used is RC4
Second hint: Decrypt the HEX, not the text of message shown by Wireshark.

Select one answer

☐ Skype credentials

☐ Gmail credentials

☐ Server credentials

☑ Skype and Gmail credentials

☐ Skype, Gmail and Server credentials