Networks and security assignment 2

exercise 1a

ubuntu@ubun2004:~$ dig @a.root-servers.net snt.utwente.nl (a till m used)
;; AUTHORITY SECTION:
nl. 172800 IN NS ns3.dns.nl.
nl. 172800 IN NS ns1.dns.nl.
nl. 172800 IN NS ns2.dns.nl.

;; ADDITIONAL SECTION:
ns3.dns.nl. 172800 IN A 194.0.25.24
ns3.dns.nl. 172800 IN AAAA 2001:678:20::24
ns1.dns.nl. 172800 IN A 194.0.28.53
ns1.dns.nl. 172800 IN AAAA 2001:678:2c:0:194:0:28:53
ns2.dns.nl. 172800 IN A 194.146.106.42
ns2.dns.nl. 172800 IN AAAA 2001:67c:1010:10::53

ubuntu@ubun2004:~$ dig @ns1.dns.nl snt.utwente.nl
ubuntu@ubun2004:~$ dig @ns2.dns.nl snt.utwente.nl
ubuntu@ubun2004:~$ dig @ns3.dns.nl snt.utwente.nl

;; AUTHORITY SECTION:
utwente.nl. 3600 IN NS ns2.utwente.nl.
utwente.nl. 3600 IN NS ns1.utwente.nl.
utwente.nl. 3600 IN NS ns3.utwente.nl.

;; ADDITIONAL SECTION:
ns3.utwente.nl. 3600 IN A 131.155.0.37
ns2.utwente.nl. 3600 IN A 130.89.1.3
ns1.utwente.nl. 3600 IN A 130.89.1.2
ns2.utwente.nl. 3600 IN AAAA 2001:67c:2564:a102::3:2
ns1.utwente.nl. 3600 IN AAAA 2001:67c:2564:a102::3:1

ubuntu@ubun2004:~$ dig @ns1.utwente.nl. snt.utwente.nl
ubuntu@ubun2004:~$ dig @ns2.utwente.nl. snt.utwente.nl
ubuntu@ubun2004:~$ dig @ns3.utwente.nl. snt.utwente.nl

;; ANSWER SECTION:
snt.utwente.nl. 3600 IN A 130.89.149.254

Exercise 1b
ubuntu@ubun2004:~$ dig +trace @a.root-servers.net ygritte.cs.ru.nl

; <<>> DiG 9.16.1-Ubuntu <<>> +trace @a.root-servers.net ygritte.cs.ru.nl
; (2 servers found)
;; global options: +cmd

```
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      RRSIG   NS 8 0 518400 20220228050000
20220215040000 9799 .
Z09bmklPvZuQJUQ/xTmPSxDGWedNCcH1ZyC3v8+OqOyf0V7oQTu5w4bI
cAHTGF4m0BVH2zFw/VVKV5MSYT22HIdl3iuB4U7aMyPmcBH1kMz4RZHC
X3GWShtHUKPkDF5xA65ZvHjcy8yxbchHR4b+Q3hJCJf/s+ND1TZKQb50
4fYLt7k37TBGuQFv8gKQyvWw0j7rQVXezAS81E7jbCP3cGm5QjnYxckM
LlxfIEGn/KUbThdDvvBm1scSEvwiHSX3mBVAwDnBhYQ4pwqPpI4mct4x
xeXPHzXhLqJywZ2NTqyJdJfbg6Mt8b9VbcqaPMhjsPMyvc3Agauwrqf7 9QaFzA==
;; Received 1097 bytes from 198.41.0.4#53(a.root-servers.net) in 48 ms

nl.                     172800  IN      NS      ns1.dns.nl.
nl.                     172800  IN      NS      ns2.dns.nl.
nl.                     172800  IN      NS      ns3.dns.nl.
nl.                     86400   IN      DS      34112 8 2
3C5B5F9B3557455C50751A9BE9EBE9238C88E19F5F07F930976917B5 1B95CD22
nl.                     86400   IN      RRSIG   DS 8 1 86400 20220228050000
20220215040000 9799 .
amQBRBxKYcPl16XTnYi7miJckXHAUdRwnw4TXYhEPE7OP+2cYIX0lH22
5NzMO0i73xOhyNVYNpimbUm6v+7EZad7HnfJAhyP1FvubkvsJEt8ti9s
zMpAC3L0tDZwmkxbiaWUjPZawNQetJEw1sdmQ+P7uzLSbCXEt3TUBRBg
T1sYyPCVfPt4lf4xyNOMUTAxHGSytBaYIRge62S8Sv1lxRvZlgUnPgSR
RE5U5wx7o9LeMLYLyh11dWaGSnbcg5oLFdBQI98ERiwoxpzOH623XJ8h
Kb3Rehumpnie7O0zl4v51ojFQCM9CH1GlO8El4U0J0JFOikkLD9h2LAj 3ohfRw==
;; Received 570 bytes from 199.7.91.13#53(d.root-servers.net) in 12 ms

ru.nl.                  3600    IN      NS      ns3.ru.nl.
ru.nl.                  3600    IN      NS      ns1.surfnet.nl.
ru.nl.                  3600    IN      NS      ns4.ru.nl.
ru.nl.                  3600    IN      DS      4996 8 2
1180262B2D21E3CC330D2E2231317E2A8303A17FFCBE948F90CEBC7B 27212839
ru.nl.                  3600    IN      DS      49090 8 2
17ACE84567E27DE7DFCBB3CE1D1531441A7AF2C5238033B3AF42D5E3 CAE6DAA2
ru.nl.                  3600    IN      RRSIG   DS 8 2 3600 20220301052242
20220214233833 31851 nl.
hVXvM9kMT3oCphjrM6iC8zdw8DUvTO77yEcy5muhcb8H0KHK0AwVyhhV
```

hSAMjBr5IeRCGO7vcDm+YXUgazI8LogKgt3sWSQ9a/zbp+4OEEw3ZbtC
MRw60Osbc3iya9cxVnAhtMWPteWLCmCQdwYLvxSK6PE/8rNBUZLN5Qsr aWM=
;; Received 448 bytes from 194.0.28.53#53(ns1.dns.nl) in 16 ms

cs.ru.nl. 86400 IN NS ns3.science.ru.nl.
cs.ru.nl. 86400 IN NS ns1.science.ru.nl.
cs.ru.nl. 86400 IN NS ns2.science.ru.nl.
cs.ru.nl. 86400 IN DS 53911 8 2
6741C21EF79E47E1773A71214FAFE64E68613ED67FA956CB113E2BB0 1D6274F7
cs.ru.nl. 86400 IN RRSIG DS 8 3 86400 20220219081707
20220215080206 17805 ru.nl.
wS0t88z69oJXJjZp+77GTXRygxK+xDBCYP22cC2r9eSW4E+acZXEH2oW
OGmSicJfgE70ikJHu9D9vJDKWiGj/P3onoi3LbJEl/qZBj05myLP8uUT
IrVmjG6bOgjvGJvBYFXo1mMUAgz0ulMH8jIErJXmOH86O6NMswr26a6S PAE=
cs.ru.nl. 86400 IN RRSIG DS 8 3 86400 20220219081707
20220215080206 54153 ru.nl.
N9Rr6PuGD/W0RlkUd6zKBLr7A+y2wLXZZcB0NdLz8raP7a28Hce1m180
SeyGQrZJ+tmBgzctqBjbX3NFuIpNVDO467ijTdfindQicaU7oxsipuR4
CMxKABXc4VQckIu3IVWcF9H/biaaU9Mv1QpzkDng0KgdQinDQ64TOldi 2x0=
;; Received 533 bytes from 192.87.106.101#53(ns1.surfnet.nl) in 16 ms

ygritte.cs.ru.nl.86400 IN A 131.174.31.164
ygritte.cs.ru.nl.86400 IN RRSIG A 8 4 86400 20220310044743 20220210042408 21249
cs.ru.nl. DynBFqGTD/qoOElLIcamLSOLQzSz9W1H5Lb3sXapxaqFxjSEiOWAfmiC
hlXryW72+3cNKBBt8oOFMNV3r3eyo9u7omlsqbbJruyzeM1GJKvkhj1b
+4jFdxURc9tPs/UFBNwAHaxdsXo9GPhLtVTfcUoXGTW6+90fE8318xEI cKY=
cs.ru.nl. 86400 IN NS ns3.science.ru.nl.
cs.ru.nl. 86400 IN NS ns1.science.ru.nl.
cs.ru.nl. 86400 IN NS ns2.science.ru.nl.
cs.ru.nl. 86400 IN RRSIG NS 8 3 86400 20220310074408
20220210074037 21249 cs.ru.nl.
fQYTCQF3R7Yvdn+pmtyWanXIQkSdjG06grQn5SEiACti1LwlU2l2NskR
K5EF/9asaei5itDV5HVxl9BiZIwFehULxT7xuZajpok6AETTXY53857w
+Z8BLgGp6vr4O3ycA2VtHOAsRUPlvrUDofc5T4MNWvgRq3pHuaCtIUb/ xkA=
;; Received 1054 bytes from 131.174.30.34#53(ns3.science.ru.nl) in 20 ms

So first we look at the name servers, which we can see as there is iterated over all of them. After this we look at the found hostnames and iterate over these similar to how we did this manually (ns1 till ns3.dns.nl.)
After this we look at the results within these results twice, so we run the command for @ns3.ru.nl, @ns1.surfnet.nl and @ns4.ru.nl.
This returns the science.ru.nl domains in ns1 till ns3, querying with this in dip gives us the ip 131.174.31.164.

Exercise 2a
The final dot (.) is gotten from the root directory.
The .org is received from the TLD directory.

The random.example is presumed to be the domain name, from the Domain directory. (First example then random is processed)
www is the hostname, which is added last.
The structure detailed above is a bottom down hierarchy, where the highest point is at the top .

Exercise 2b
The most likely one is an example, because we know that .org probably is in TLD and . is in root.
Because we know this we also know that the following one is most likely to be dns, even more so than random.
This is because random could be in the hostname zone as well .

Least likely to be found is the . because it is always found in the root directory.

Exercise 2c
The TTL does not say anything about how often a record is looked up.
It does tell you something about how often an address is changed.
This is because the TTL tells when the cached data expired, if expired new data is requested and hence the address is changed.

Exercise 2d
You can see if the dns of the website is inside of the DNS cache.

Exercise 2e
The ip4 address is 134.122.131.10
printer.random.example.org. is the full FQDN of the printer.

Exercise 2f
It is most likely to use beta, because 10 is a higher priority then 10.
Hostname: beta, IP: 131.122.131.10

Exercise 2g
This makes it more dynamic. If using A entries, when we update we have to replace all the ip values. With using CNAME however, only alpha has to be updated, the CNAME entries adjust automatically.

Exercise 3a
Commands:
Client -> Server PASSWD(userPWD)
Server -> Client -> Auth(Session)
Server -> Client -> RefuseAuth()
Client -> Server QueryBalance(Session)
Server -> Client {Balance}
Client -> Server WithdrawAmount(Session, Amount)
Server -> Client Withdrawfailed()
Server -> Client WithdrawConf(Amount, NewBalance)
Server -> Client Terminate(Session)

Explanation

Client -> Server PASSWD(userPWD)
A message is sent from the client to the server with the PIN of the user so the server can authenticate the user.

Server -> Client -> Auth(Session)
The server authenticates the user.

Server -> Client -> RefuseAuth()
The server sends a message that the client typed the wrong PIN and can type a new one.

Client -> Server QueryBalance(Session)
A message from the client that asks to see its balance.

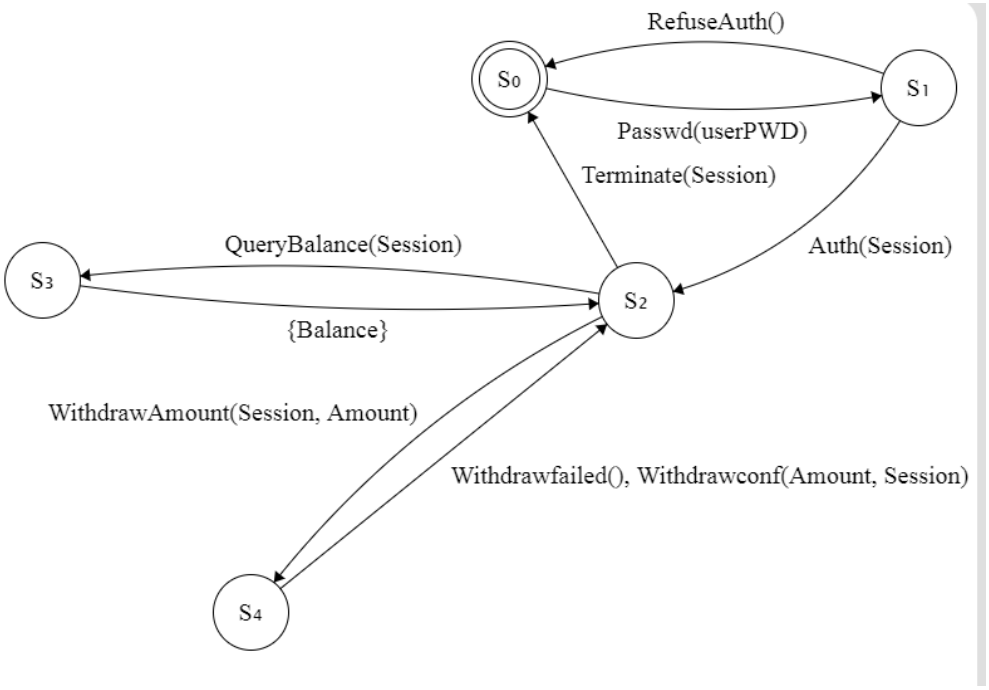
Server -> Client {Balance}
The server sends the client the balance on his/her bank account.

Client -> Server WithdrawAmount(Session, Amount)
The client sends a message with how much money he/she wants to withdraw from the ATM.

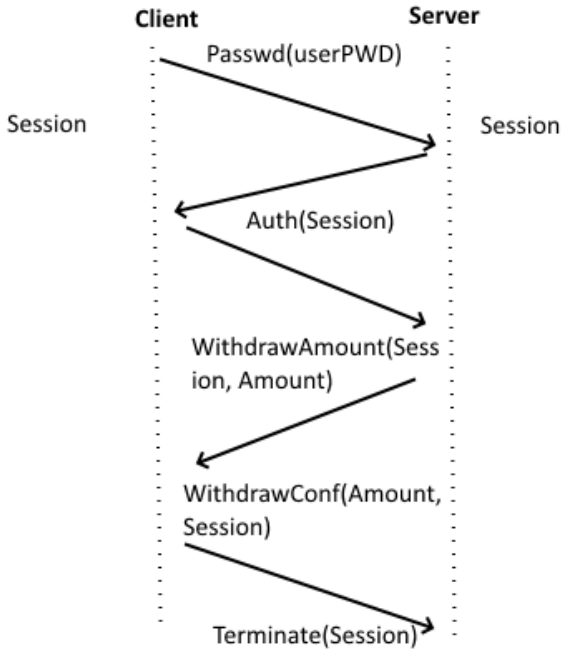
Server -> Client Withdrawfailed()
The server shows that the money cant be withdrawn, because there isn't enough money in the bank account.

Server -> Client WithdrawConf(Amount, Session)
The server sends a confirmation of the withdrawal and gives the client the amount of money he/she wanted.

Server -> Client Terminate(Session)
The server terminates the session.

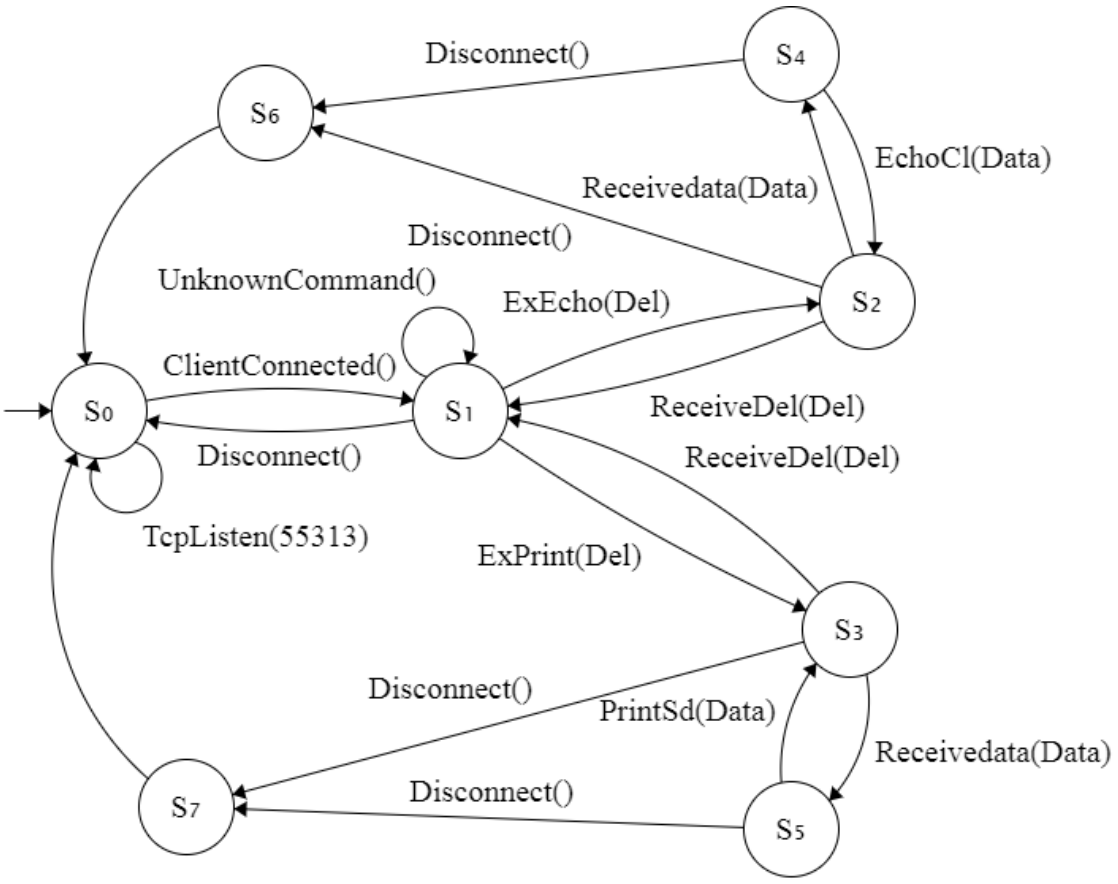

RefuseAuth()
S0
S1
Passwd(userPWD)
Terminate(Session)
QueryBalance(Session)
Auth(Session)
S3
S2
{Balance}
WithdrawAmount(Session, Amount)
Withdrawfailed(), Withdrawconf(Amount, Session)
S4

Exercise 3b


Client
Server
Passwd(userPWD)
Session
Session
Auth(Session)
WithdrawAmount(Session, Amount)
WithdrawConf(Amount, Session)
Terminate(Session)

Exercise 4a

Note that S6 and S7 were only added to make it more clear what is done, ideally we would want a line back to S0 directly, however this would **** up our graph extensively.



Exercise 4b
See python file.