Sistema de Comunicação Anônima

Eduardo Britto da Costa, Rodrigo Valente Bernardes, Andrey Carvalho e Morgana Silva Prado

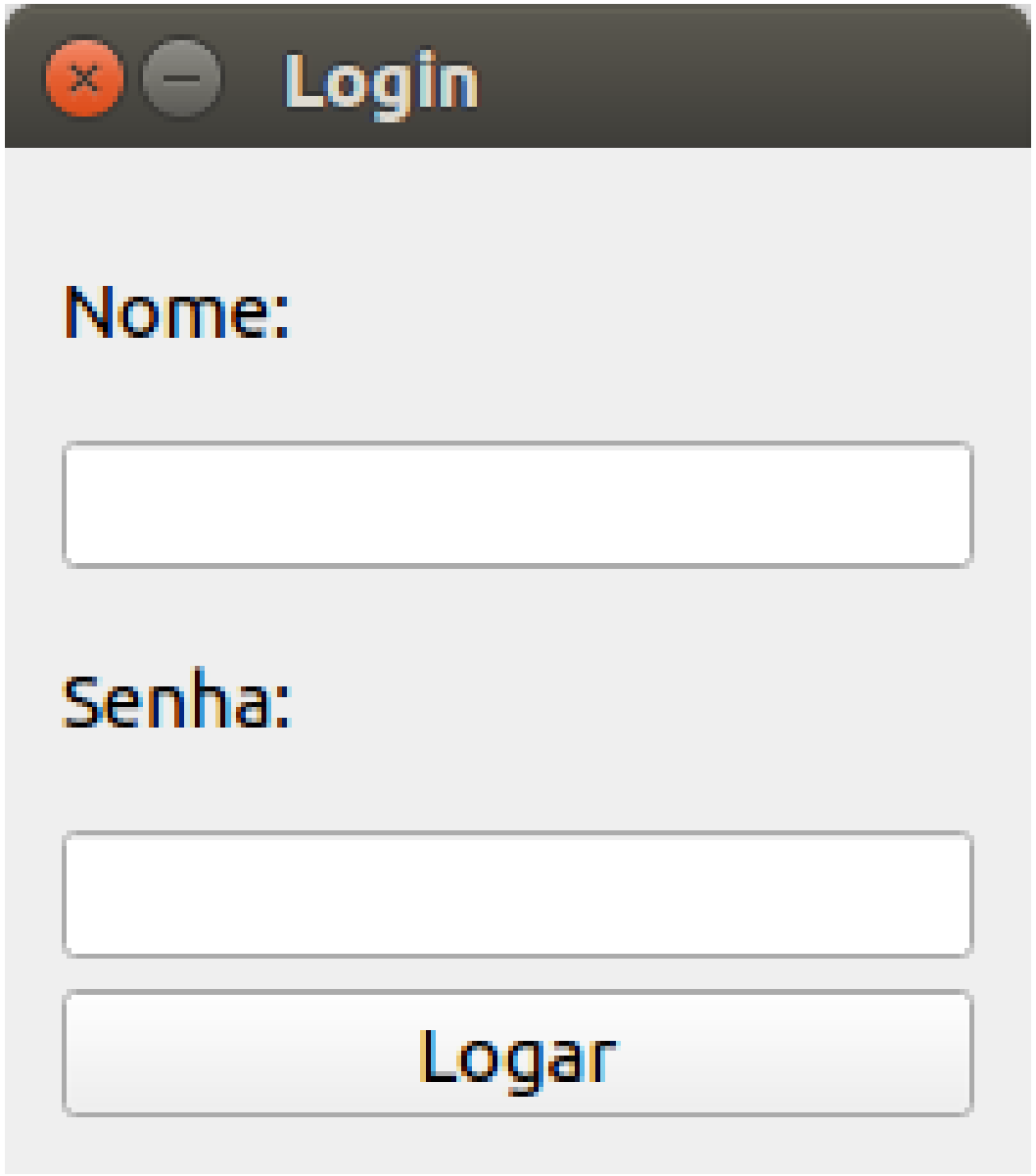
Problema?

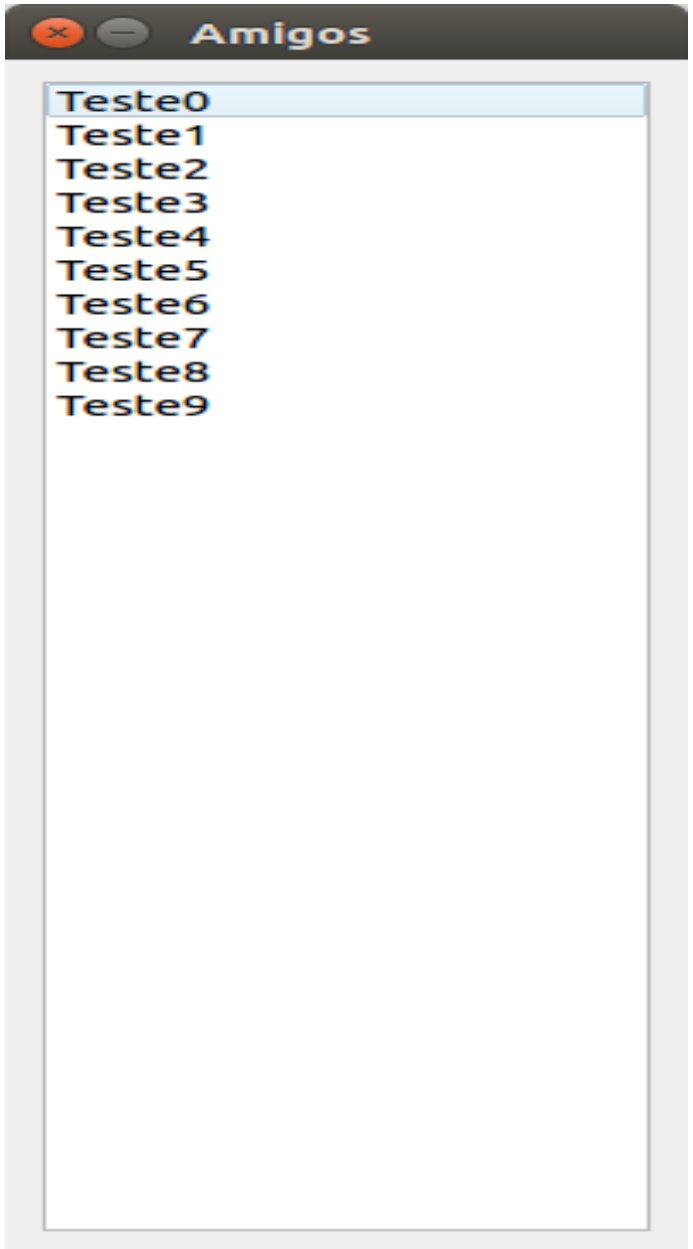
- A interceptação de mensagens em sistemas de comunicação online.

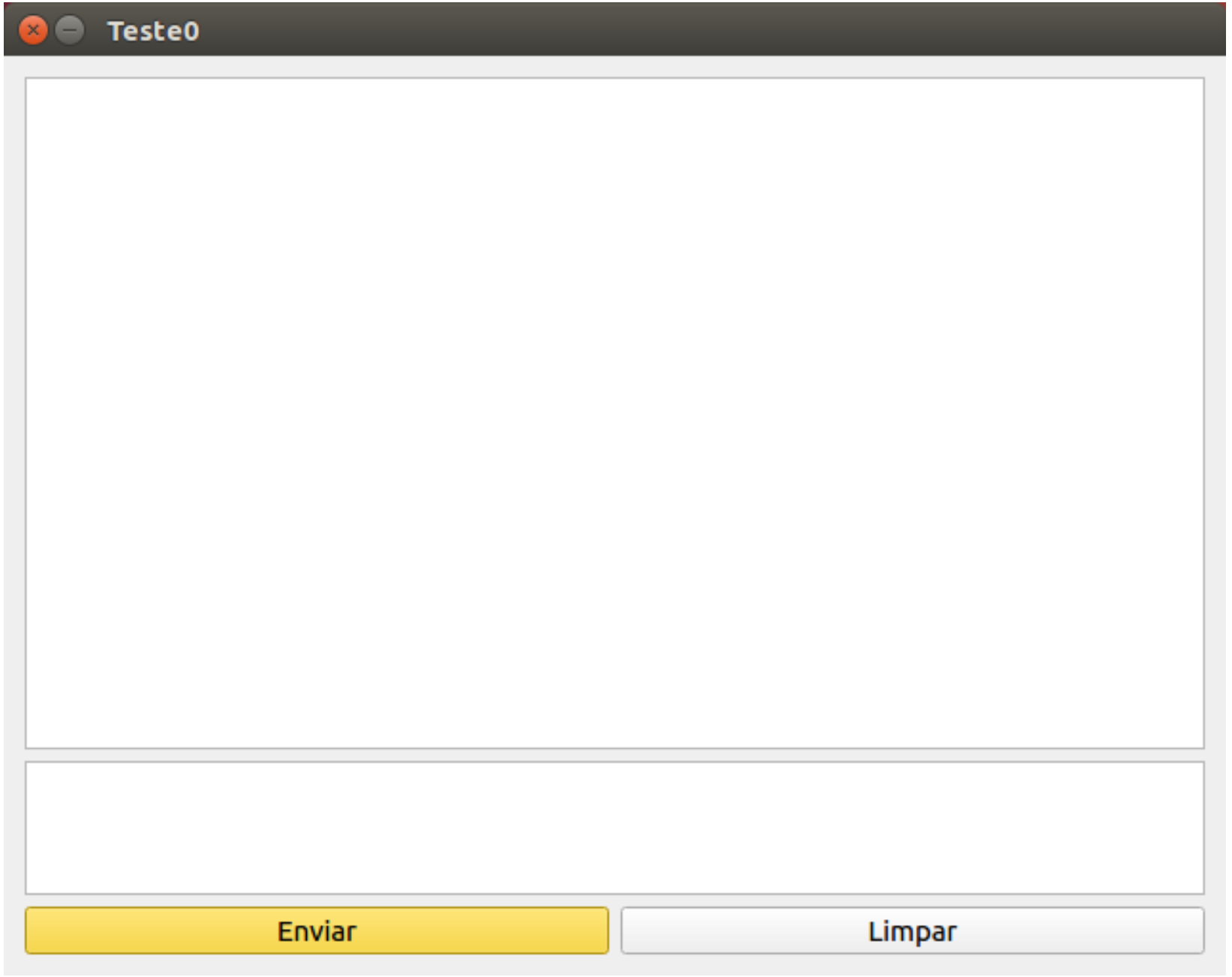
Proposta

- Solução: Proposta de desenvolvimento de um sistema de comunicação instantânea criptografado.
- Ideia:
  - Todas as mensagens trocadas serão criptografados pela criptografia simétrica (AES).
  - A realização de um login com usuário e senha, caso o usuário não tenha cadastro no sistema, momento do login é criado um novo usuário e um par chave de criptografia assimétrica (RSA), onde a chave privada é armazenada em disco e a chave pública no banco de dados .
  - Os usuários cadastrados terão uma lista de amigos que poderão trocar mensagem de forma segura.
  - Mensagens trocadas serão apagadas do banco de dados no final da comunicação.
- Teste: Sniffer (Wireshark).

Demonstração do Sistema.


Login
Nome:
Senha:
Logar


Amigos
Teste0
Teste1
Teste2
Teste3
Teste4
Teste5
Teste6
Teste7
Teste8
Teste9


Teste0
Enviar
Limpar

Testes Wireshark

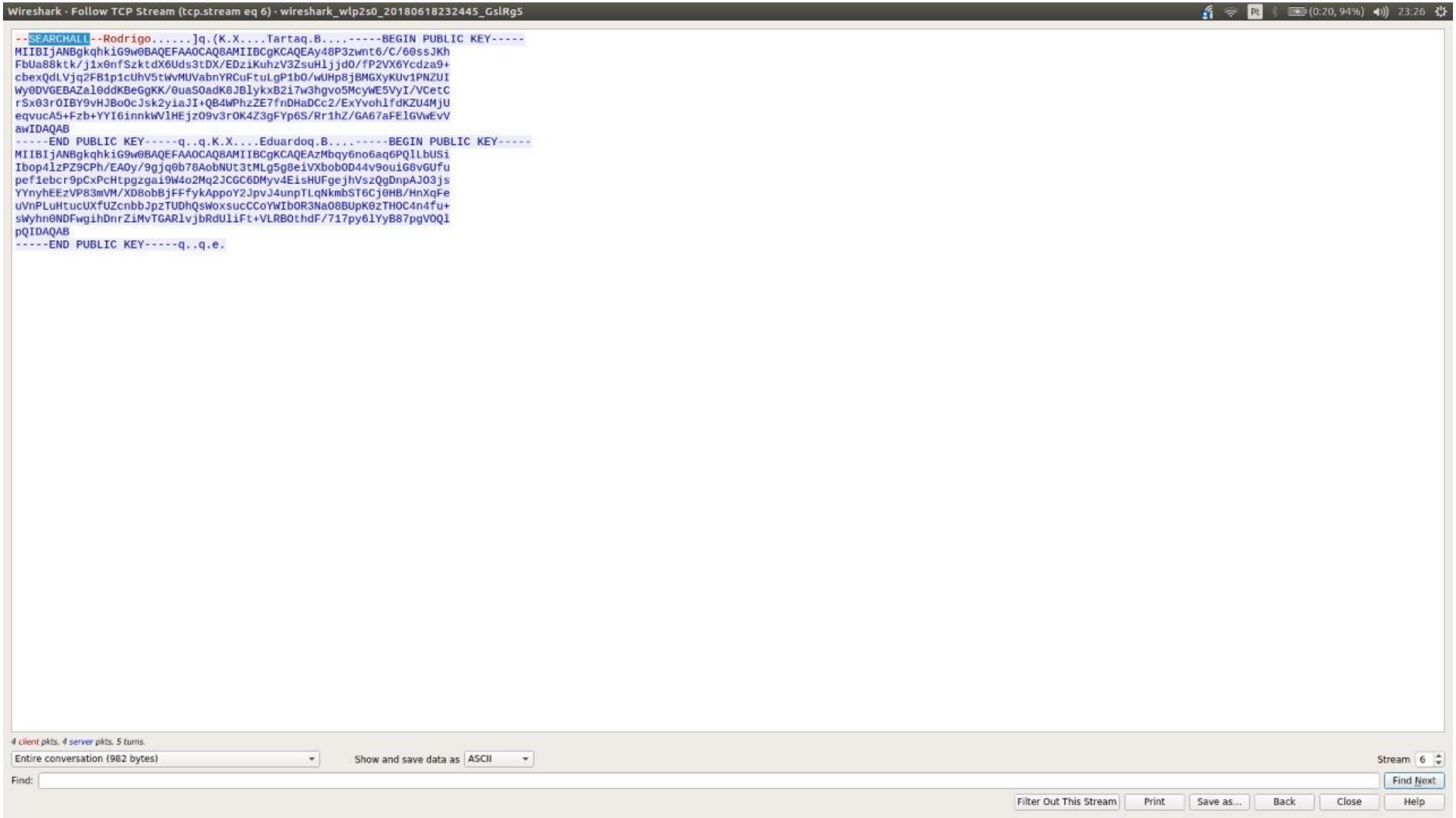
```
--LOGINREQ-------BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0JBTjxEmEf77yZu/q3mo
T1ZKji4pSCUyh4oHkLefZyOOtU1jHCzyDmIlrVVygq7eBfg0l1t/jfE/isiqaJ9R
9RdXglMRBFfvSzBwT8PlYzbVQlBLIhANC2jU7X4CPIZs50ZBrmqfRVzF8kGocv2U
Tkp0W/z2sMp3FFkAOmzXkjNS2bOdBXR5e9AgYeco5VkCzfTNdVIzYREuGha0tccL
cL3pUoAPqP6OlPZKSfnxQzgOOyYUSCD1wRqVkirp0ian5cX1JU2S+x1wUMfSfD6A
91xQEUzQ0L5wjz5VPaSpnRicy/3+5h+Yf0i5uxVAD8xzbCgkrazU3yDmjSDFrXFp
/wIDAQAB
-----END PUBLIC KEY-----..}q.{X    ...publickeyq.B....-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuZJJJf9neOa5JMF4ZnAp
XFtkWaXQZlXYsZu9bKkK3N19ldYYh+kDLFIfBOEdL5mkLxUPJnfI/AvLsEMmFsP8
P+Pg/8FwqC7kK2JWzSohmQeCSp9Ip0p8m9rR7KM71b1vaZEyD/+N85ylkndRDS/E
brmVU6syqElhqUxqsYIjmPq1PTJ7PArrvVuBUUK1/dxdXIKdWSZ5/k9kJfM8YXb4
rxD5kL6NfcyzsCic3+WlpIgvBjey7BzHHt2OLgNx6g0yWTBohcNkSzYXolm+7GX7
j5TJ2GA+iCIGxyk0t5Cu9aJtOIHtlwYrJc5ewEBUY9qXKFyhUn1uJFsMWqBFWSn8
gQIDAQAB
-----END PUBLIC KEY-----q.X....userq.B....G...%.ox..1.F..~..>.d..y....`.........O...tg..i...K..7k`2.3.?g..v.3.....>...\{%..|.....<%.wE{....J.v...R.....{        ..2X6.j.$.d..^...=_.J...-5J...Kut..b.sa...
.........S....v.Y..t..    ..bC.]j..2B....e..y.....Ww.CC.....i.... ....y..f.=..7=.        .D.0.......n{....
7...q.X....passwordq.B.......d......h......<........{.'"V..2...........E.+...4..F.....3.9....7.{.R$........z....a]...y..9....        ..........VlN...4
a......Q.%....{.*s..XZ N.d-;._\..(0.@..!....N."..R..)..._-q**_..s_-..r....-.;..0.)...S.....h.M....2..4..A......(.n...k..W..  8...a....P..7}.q.u.True-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuZJJJf9neOa5JMF4ZnAp
XFtkWaXQZlXYsZu9bKkK3N19ldYYh+kDLFIfBOEdL5mkLxUPJnfI/AvLsEMmFsP8
P+Pg/8FwqC7kK2JWzSohmQeCSp9Ip0p8m9rR7KM71b1vaZEyD/+N85ylkndRDS/E
brmVU6syqElhqUxqsYIjmPq1PTJ7PArrvVuBUUK1/dxdXIKdWSZ5/k9kJfM8YXb4
rxD5kL6NfcyzsCic3+WlpIgvBjey7BzHHt2OLgNx6g0yWTBohcNkSzYXolm+7GX7
j5TJ2GA+iCIGxyk0t5Cu9aJtOIHtlwYrJc5ewEBUY9qXKFyhUn1uJFsMWqBFWSn8
gQIDAQAB
-----END PUBLIC KEY-----
```


4 client pkts, 5 server pkts, 5 turns.

Entire conversation (1949 bytes) | Show and save data as ASCII | Stream 4

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help


Wireshark · Follow TCP Stream (tcp.stream eq 6) · wireshark_wlp2s0_20180618232445_GslRg5
(0:20, 94%)
23:26
--SEARCHALL--Rodrigo.....]q.(K.X....Tartaq.B....-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAy48P3zwnt6/C/60ssJKh
FbUa88ktk/j1x0nfSzktdX6Uds3tDX/EDziKuhzV3ZsuHljjdO/fP2VX6Ycdza9+
cbexQdLVjq2FB1p1cUhV5tWvMUVabnYRCuFtuLgP1bO/wUHp8jBMGXyKUv1PNZUI
Wy0DVGEBAZal0ddKBeGgKK/0uaSOadK8JBlykxB2i7w3hgvo5McyWE5VyI/VCetC
rSx03rOIBY9vHJBoOcJsk2yiaJI+QB4WPhzZE7fnDHaDCc2/ExYvohlfdKZU4MjU
eqvucA5+Fzb+YYI6innkWVlHEjzO9v3rOK4Z3gFYp6S/Rr1hZ/GA67aFElGVwEvV
awIDAQAB
-----END PUBLIC KEY-----q..q.K.X....Eduardoq.B....-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzMbqy6no6aq6PQllbUSi
Ibop4lzPZ9CPh/EAOy/9gjq0b78AobNUt3tMLg5g8eiVXbobOD44v9ouiG8vGUfu
pef1ebcr9pCxPcHtpgzgai9W4o2Mq2JCGC6DMyv4EisHUFgejhVszQgDnpAJO3js
YYnyhEEzVP83mVM/XD8obBjFFfykAppoY2JpvJ4unpTLqNkmbST6Cj0HB/HnXqFe
uVnPLuHtucUXfUZcnbbJpzTUDhQsWoxsucCCoYWIbOR3NaO8BUpK0zTHOC4n4fu+
sWyhn0NDFwgihDnrZiMvTGARlvjbRdUliFt+VLRBOthdF/717py6lYyB87pgVOQl
pQIDAQAB
-----END PUBLIC KEY-----q..q.e.
4 client pkts, 4 server pkts, 5 turns.
Entire conversation (982 bytes)
Show and save data as
ASCII
Stream
6
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

```
--RMSGREQ--..}q.(X....senderq.X....Eduardoq.X....receiverq.X....Rodrigoq.u.,&e.P;.x,.....)T..*.4.....t...]...KSp...'..lc{&..R..a3...p..W....Z....q...N....kO...s.v..c..BSP....TZ.>..#.
2..0@"....pB.T.*.b......s..zuv...._..>.w.....E.o
..d~....7....o..G.@.)..=..j..|..RB.*..'V.L.~.R. .......:ei..(E.=#........./...=....8.;.,..A...Vj.B....]q.(K.B>.....(C.....q.C..I#Cn.a...e....\q.C...A.........+.f.q.B.....hn..3..}'Q
.Sh....8....1..S6.;....    .....)..7.EU..`.Y.#.a....6...x.....|.w.%..Lv.4d......0..!Q1.*rw.:.#o$..6...Q.c.0
..W.....^.TDR....#.z[._.]s.f.6....U/.............z.bc#d...VlL.@..J..f......?k......|.....s|..=...d..Q.@.s.*4.0.
..E.pB.G.......?..#i'......q.tq..q.cdatetime
date
q.C.....q..q.Rq.h.C.....q..q.Rq.K.X....0q    K.tq
a.--ALLREAD--
```


5 client pkts, 5 server pkts, 6 turns.

Entire conversation (739 bytes) | Show and save data as ASCII | Stream 482

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help

--SMSGREQ--..}q.(X....senderq.X....Rodrigoq.X....receiverq.X....Eduardoq.u.--OKTOSEND--,&e.P;.x,.....)T..*.4.....t...]...KSp...'..lc{&..R..a3...p..W....Z....q...N....kO...s.v..c..BSP....TZ.>..#.
2..0@"....pB.T.*.b.....s..zuv...._..>.w.....E.o
..d~....7....o..G.@.)..=..j..|..RB.*..'V.L.~.R. ....:ei..(E.=#........./...=....8.;.,..A...Vj.B....]q.(B?.....(C..<<!<q.C.............+.vq.C.....i..2....=
.q.B.....x...(2.....j.M.gu"..ZG2.T.....@..y.A.....d.m...]..-$c..9^....U...\...O..^zQ...5..Zt\.....o...R...........1.....T....S.....4B$.~.P.b.....S+9....=.   ..4.&.h..........
......QO.AK.|.V.....H.....XN..r.....2.x....r.~[g~i.2.........3..E.d.^C(.}...|i.k .{.   .Sq.tq..q.X....Rodrigoq.X....Eduardoq.cdatetime
date
q.C.....q..q.Rq.e.--OK--

5 client pkts, 6 server pkts, 7 turns.

Entire conversation (742 bytes) | Show and save data as ASCII | Stream 263

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help