Chapter 5

For Whom Ma Bell Tolls

by Joe Grand as "The Don"

The sun had already sunk beyond the harbor as Don Crotcho woke up. He neither noticed nor cared. It had been a little more than a year since his flight from Boston after a successful theft of the United States' next-generation stealth landmine prototype, and he had been enjoying his self-prescribed seclusion in this land of fire and ice…

Between the wonders of volcanic activity, the lush, moss-covered fields, beautiful countryside, and seductive nightlife, what was there not to like about Iceland? It was a nice change from the urban concrete playground and he was glad to get away.

Don Crotcho, affectionately called *The Don* by his associates, had become a local in his neighborhood of Norðurmýri in the city of Reykjavík. By word of mouth, his skills as a *phone phreak* were respected and feared by the underground world of computer misfits and organized (and not-so-organized) criminal enterprises, reaching far and wide.

The Call

A few days ago, The Don got a phone call from some guy named Knuth. He was a friend of a friend. Rather, more like somebody who knew somebody who knew The Don. He didn't give The Don a lot of background information, which was probably for the better.

As Knuth so bluntly put it, the telephone systems were a key part of some operation he was involved in. He needed The Don to gain access to a specific cellular phone switch in the Republic of Mauritius (a small tropical island on the southeast coast of Africa), trace the phone calls made to and from a particular phone, and then disconnect the line. If he did it, he'd get paid a good chunk of change. If not, well, that wasn't really an option after Knuth described how The Don's anatomy would be creatively rearranged.

Now, The Don was used to threats on his life and limb by the bloated egos of underworld criminals, and Knuth was no exception. In this line of business, it came as no surprise. Since The Don had heard it all before, he brushed it off and got right to the point: payment.

The Don demanded a modest fee of $100,000 cash. Low by criminal standards, but The Don enjoyed his work so much that sometimes he had to remind himself not to just do it for free.

That phone call was like a spark that lit a fire under The Don's sleeping baby soul. He was reenergized, invigorated. And he celebrated by taking a walk to the one place he frequented.

Maxim's

The Don lounged in a plush red velvet seat at Maxim's as he flicked dollar bills towards the stage. From the outside, settled on a small side street in downtown Reykjavík, Maxim's didn't seem to be much—fitting snugly between two brick row houses, the single wooden door into the establishment gave no clue as to its purpose.

Inside the smoke-filled club, the black walls reflected the multicolored lights that shined down onto the stage. The bar in the center was crowded with familiar faces, men and women obviously enjoying their night—drinking, laughing, and taking in the sights. Worn-out fabric couches lined the open spaces and a handful of individual seats were facing the stage. Rhythmic music pumped out of speakers hanging by chains from the ceiling.

Maxim's was a refuge for The Don. Finishing off the rest of his chilled Brennivín, he headed downstairs. The iron spiral staircase led to a few small "rooms," each separated by a swatch of black velvet hung on old shower rods. As in any establishment like this, these rooms were reserved for the richer clientele—or for the select few who had earned *respect*. He walked past the cashier and around the dark corner to the room at the end of the hallway.

Brushing the velvet cloth aside, he made himself comfortable in the secluded room, usually kept free by Maxim's owners for The Don's frequent visits. The Don used this room as a makeshift office, because he wasn't always able to get back to his pad when the need for a computer was taunting him.

The room was illuminated with a single black-light tube nailed to the ceiling. There was a flimsy plastic table, the kind you see for $2.99 at the local swapmeet, placed in the center of the room, and a vinyl couch as a seat. The walls were painted black, but years of neglect left them peeling, showing the drywall beneath. It wasn't luxury, but it got the job done.

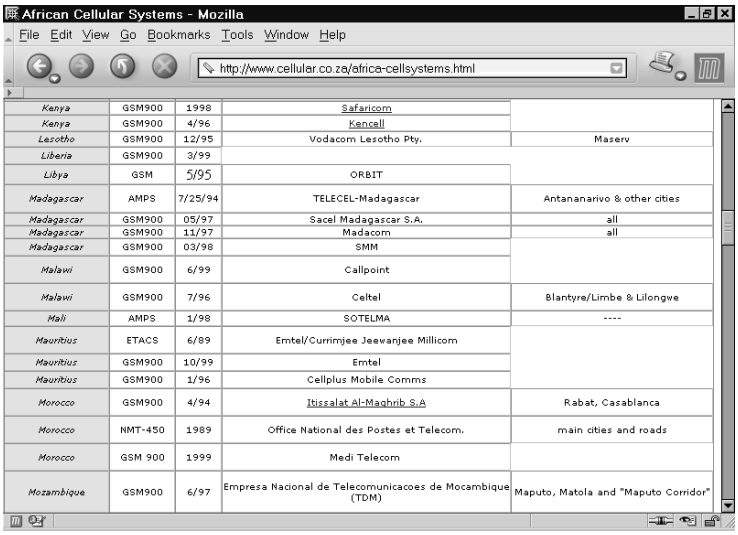
The Don flipped his laptop open and set it down on the table. He stared into space for what seemed like an eternity as Windows finished loading.

From his basement location inside Maxim's, The Don could identify two wireless access points. Neither had WEP enabled (though that would have been just a temporary roadblock requiring him to monitor enough network traffic to then use wepcrack or airsnort to determine the key). One access point used the typical default SSID of `default` and the other used `linksys`. He assumed that they were personal wireless networks set up by people living in

nearby flats. They were wide open, issued IP addresses at request, and gave The Don full Internet access.

He dedicated the rest of the night to doing some initial research on the switch that Knuth wanted him to access. The Don did some preliminary Google searches to learn about Mauritius and to find the Web sites of the cellular telephone providers. He came across a page that gave him a listing of all available cellular technologies and operators in Africa. Mauritius was covered by two: Cellplus Mobile Comms and Emtel.

All Available Cellular Technologies and Operators in Africa

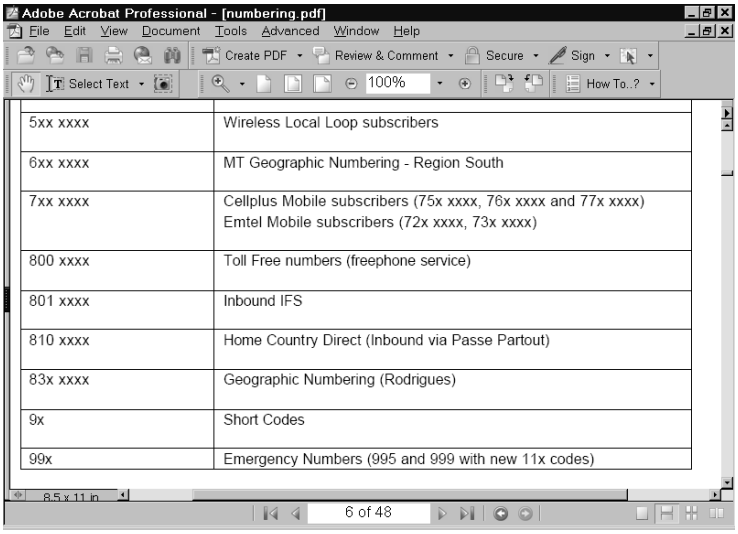


Kenya	GSM900	1998	Safaricom	
Kenya	GSM900	4/96	Kencell	
Lesotho	GSM900	12/95	Vodacom Lesotho Pty.	Maseru
Liberia	GSM900	3/99		
Libya	GSM	5/95	ORBIT	
Madagascar	AMPS	7/25/94	TELECEL-Madagascar	Antananarivo & other cities
Madagascar	GSM900	05/97	Sacel Madagascar S.A.	all
Madagascar	GSM900	11/97	Madacom	all
Madagascar	GSM900	03/98	SMM	
Malawi	GSM900	6/99	Callpoint	
Malawi	GSM900	7/96	Celtel	Blantyre/Limbe & Lilongwe
Mali	AMPS	1/98	SOTELMA	----
Mauritius	ETACS	6/89	Emtel/Currimjee Jeewanjee Millicom	
Mauritius	GSM900	10/99	Emtel	
Mauritius	GSM900	1/96	Cellplus Mobile Comms	
Morocco	GSM900	4/94	Itissalat Al-Maghrib S.A	Rabat, Casablanca
Morocco	NMT-450	1989	Office National des Postes et Telecom.	main cities and roads
Morocco	GSM 900	1999	Medi Telecom	
Mozambique	GSM900	6/97	Empresa Nacional de Telecomunicacoes de Mocambique (TDM)	Maputo, Matola and "Maputo Corridor"

Knuth had requested that The Don trace all calls going into and coming from the mobile phone at 230-723-8424.

The Don checked more of the Google search results and found a document that described the current telephone numbering scheme for Mauritius. According to the document, all numbers with a "72" prefix belong to Emtel mobile subscribers. Knowing that, the Emtel cellular phone switch would be the target for Knuth's request.

Telephone Numbering Scheme for Mauritius



5xx xxxx	Wireless Local Loop subscribers
6xx xxxx	MT Geographic Numbering - Region South
7xx xxxx	Cellplus Mobile subscribers (75x xxxx, 76x xxxx and 77x xxxx) Emtel Mobile subscribers (72x xxxx, 73x xxxx)
800 xxxx	Toll Free numbers (freephone service)
801 xxxx	Inbound IFS
810 xxxx	Home Country Direct (Inbound via Passe Partout)
83x xxxx	Geographic Numbering (Rodrigues)
9x	Short Codes
99x	Emergency Numbers (995 and 999 with new 11x codes)

Another simple search led The Don to the Emtel main Web site at www.emtel-ltd.com. Looking at the Customer Care page, he saw that the 465 prefix is used for both the main and fax numbers.

A whois of emtel-ltd.com provided some additional clues.

```
% GANDI Registrar whois database for .COM, .NET, .ORG.

domain: EMTEL-LTD.COM
owner-address: Web Ltd
owner-address: Chancery House
owner-address: 99
owner-address: PORT LOUIS
owner-address: Mauritius
admin-c: EL534-GANDI
tech-c: WC169-GANDI
bill-c: SC721-GANDI
reg_created: 1997-05-20 00:00:00
expires: 2004-05-21 00:00:00
created: 2003-04-18 10:55:49
changed: 2004-02-04 13:19:24
```

```
person: EMTEL LTD
nic-hdl: EL534-GANDI
phone: +230.4657800
fax: +230.4657812
lastupdated: 2004-02-04 13:24:22
```

The 465 prefix also is used for the phone and fax numbers in this listing. So, chances are, the Emtel offices were issued a block of telephone numbers within the 465 prefix. The likelihood of success is high that The Don would encounter computer systems with modems connected to some of the lines within the block. The Don shut down his laptop and headed back up the spiral staircase into the excitement of the club.

Shall We Play a Game?

Wardialing, made famous by the movie *WarGames* in 1983, is like knocking on the door of 10,000 neighbors to see who answers. You make a note of those that do and come back later to check out the house.

The act of wardialing is as easy as it gets—a host computer dials a given range of telephone numbers using a modem. Every telephone number that answers with a modem and successfully connects to the host is stored in a log. At the conclusion of the scan, the log is manually reviewed and the phone numbers are individually dialed in an attempt to identify the systems.

You'd be surprised at what sorts of systems are accessible through the modem. Even today, most "security administrators" still ignore the threat of wardialing.

"Who's going to find this and why would they want to?" they think, "We need to focus on the security hot spots of our network, like the wireless and Internet connections."

However, that poor, forgotten modem connected to the computer in the telephone closet will answer to anyone or anything that calls its assigned phone number. Unsecured modems are usually the easiest way into a target network.

Modems are equal opportunity—they don't discriminate. PBXs, UNIX, VAX/VMS systems, remote access servers, terminal servers, routers, bulletin board systems, credit bureaus, elevator control, hotel maintenance, alarm and

HVAC control, paging systems, and, of course, telephone switches. There's something for everyone if you just have the patience.

The Don's next step was to decide on a way to call the numbers in Africa for free from Iceland. Free phone calls are not a difficult thing to obtain. The Don could use a stolen credit card, calling card, or mobile phone, reroute his call through a corporate PBX, or take advantage of a misconfigured outdial, a feature of some remote access network equipment which allows you to call in to the device on one modem and dial out on another.

He chose to go with using a stolen mobile phone. Since wardialing a complete prefix takes usually three or four days of nonstop dialing, The Don needed to make sure to obtain a phone that wouldn't immediately be noticed as missing. One that was left in an office on a Friday afternoon would do just fine—the owner wouldn't return until Monday to notice that the phone had disappeared. Even then, the owner might fumble around for a few more days while thinking it had legitimately been lost.

Not only was a stolen phone easy to get hold of, The Don could wardial from any location within Iceland where Og Vodafone provided service. Better yet, it was untraceable. He'd just destroy the phone when he was done.

The next evening, The Don made a few calls and walked down to the Tjörn, the park and pond in city centre. Feeding the ducks, he waited.

As expected, one of The Don's acquaintances, a fence from the neighborhood, stopped by. They shook hands and exchanged pleasantries as they strolled the path along the water. The Don handed the fence a small envelope filled with currency and received a small plastic shopping bag in return. The bag contained a Nokia 6600 tri-band smartphone and stolen SIM card. Just what he had asked for.

Back in his flat, he grabbed the required drivers from the Nokia support Web site and connected the Nokia 6600 to the serial port of his computer. Now, the computer would simply treat the phone as a landline modem.

ToneLoc is The Don's wardialer of choice. Although it's a few years old, it works fine with current Windows versions. He set up a spare machine to dedicate to the task. He isn't worried about being in a fixed location. It will be obvious that thousands of numbers are being dialed from the same phone within the same cell location, but The Don would be done wardialing before the corporate wheels of fraud detection start turning, and the phone would be long gone by then.

The numbering system in Mauritius uses a fixed 7-digit format and a country code of 230, so configuring ToneLoc to run was easy:

```
toneloc emtel.dat /m:230-465-xxxx.
```

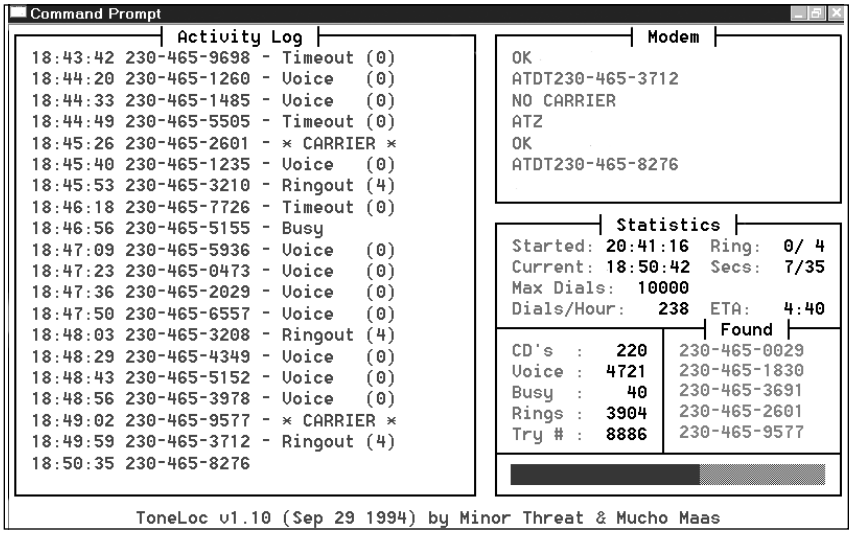
With the wardialing happily on its way, The Don turned off the monitor screen, locked the door behind him, and headed out toward the street.

The Booty

It was early evening and ToneLoc had been averaging nearly 240 calls an hour for the past two days. The Don was getting antsy to check out the results.

Four hours to go. He sighed, and waited.

ToneLoc Call List



Finally, the wardialing finished. The Don, curious as to how many modems he actually had discovered, ran the simple tlreport tool included with ToneLoc.

```
C:\TONELOC>tlreport emtel.dat

TLReport;  Reports status of a ToneLoc data file
           by Minor Threat

Report for emtel.DAT: (v1.00)

                      Absolute   Relative
                      Percent    Percent
Dialed       = 10000  (100.00%)
Busy         =    56  ( 0.56%)   ( 0.56%)
Voice        =  4969  (49.69%)   (49.69%)
Noted        =     3  ( 0.03%)   ( 0.03%)
Aborted      =     0  ( 0.00%)   ( 0.00%)
Ringout      =  4117  (41.17%)   (41.17%)
Timeout      =   635  ( 6.35%)   ( 6.35%)
Tones        =     0  ( 0.00%)   ( 0.00%)
Carriers     =   220  ( 2.20%)   ( 2.20%)

Scan is 100% complete.
50:57 spent on scan so far.
```

Two hundred and twenty modems. The Don smiled as he copied the log files to his laptop and securely wiped the wardialing contents from his desktop machine.

To check the results of the scan, The Don needed a change of scenery. He decided that it was a fine night to be at Maxim's.

Later, illuminated by the glow of his 15" laptop screen, The Don checked each of the numbers that the wardialer had marked as potential hits, one by one, hoping for the one golden egg, the light at the end of the tunnel.

Many of the systems to which The Don connected just sat there. A dead modem connection, a digital black hole, so to speak. No matter what keys were pressed, they didn't respond. But The Don wasn't discouraged; for every handful of unresponsive machines, there is usually a diamond in the rough. Or at least a computer that can be probed for more information.

Finally, The Don got his first hit.

```
CONNECT 1200/NONE

01:45:38/04  0018  01  PEREYBERE
================================================
CHAN       NO     NO2     NOX    TEMP      CO     SO2
UNITS     PPM     PPM     PPM   DEG K     PPM     PPM
================================================
01:45    0.045  0.025  0.069     261     0.2   0.020
```

As soon as the connection was made, the system spit out a table containing concentration readings of various pollutants in parts-per-million—Nitric Oxide, Nitrogen Dioxide, Carbon Monoxide, and Sulfur Dioxide. It looked like some sort of environmental monitoring system.

A quick Web search showed that Pereybere, printed on the first line of the table, is a small beach town on the northwest part of Mauritius. Poking around with various keys, The Don found that typing `L` provided a configuration menu.

```
L

# PWR FAIL TO PRT (1-A) - 4
5 MIN STATUS 0,1 - 1
# A/D SMPS (1-99) - 06

PRELIMINARY AVG; 1=1MIN, 2=2MIN, 3=3MIN = 1
INTERIM AVG; 1=5MIN, 2=6MIN, 3=10MIN = 1
FINAL; 1=60MIN, 2=30MIN, 3=15MIN = 1
AVERAGE (1) OR INSTANTANEOUS (2) = 1
CARTRIDGE INTERVAL; 1=FINAL, 2=INTERIM, 3=PRELIM, = 1
NUMBER OF WS/WD PAIRS 0-3 = 0
WD SENSOR TYPE; 1=540 2=360 = 1
# CHANNEL TO RECORD 1-8 = 6

IS CHANNEL 1 RAINFALL (Y/N) - N
CART ROLLOVER (Y/N) - Y
RECORD DATA STATUS - Y
```

```
RECORD INPUT STATUS - N
MULTIPLE UNIT - N
PORTABLE OPERATION - N
PARALLEL PORT - Y
PRT SMALL CHARS Y/N - N

                    CAL CONFIGURATION
PARAMETER  TYPE  8  -   1   16  -  9  EXPECTED  CAL FS
       NO    I   ..Z.....   ........     0.000   0.500
       NO    I   .S......   ........     0.000   0.500
      NO2    I   ..Z.....   ........     0.000   0.500
      NO2    I   .S......   ........     0.366   0.500
      NOX    I   ..Z.....   ........     0.000   0.500
      NOX    I   .S......   ........     0.367   0.500
       CO    I   ......Z.   ........     0.0     50.0
       CO    I   .....S..  . .......     36.9    50.0
      SO2    I   ....Z...  . .......     0.000   0.500
      SO2    I   ...S....  . .......     0.356   0.500

04-11-69.M28,JD131, P740,AQM,NS,RAIN=10IN,AC-2,SP=4,SQ=4,PSW-0
,OME,TP,BKT,8CH,16CO,24S,PP-6,OMA,4M,FDA,HBA
```

With a snicker, The Don moved down the list. A few more dead modem connections before he hit another interesting one.

```
CONNECT 9600

@ Userid:
```

He instantly recognized this as a Shiva LanRover, a remote access server, probably part of the University on the island. Logging in as `root` with no password, The Don was granted supervisor access to the device. The funny thing is that the unpassworded root account has been a known problem with Shiva LanRovers for over a decade.

"Chalk it up to choosing user convenience over security," quipped The Don.

```
@ Userid: root

Shiva LanRover/8E, Version 2.1.2
LanRoverE_3F6500# ?

clear <keyword>       Reset part of the system
configure             Enter a configuration session
connect <port set>    Connect to a shared serial port
debug                 Enter a debug session
disable               Disable privileges
help                  List of available commands
initialize <keyword>  Reinitialize part of the system
passwd                Change supervisor password
ppp                   Start a PPP session
quit                  Quit from shell
reboot                Schedule reboot
show <keyword>        Information commands, type "show ?" for list
slip                  Start a SLIP session
LanRoverE_3F6500# show ?

arp                   ARP cache
bridge <keyword>      Bridging information
buffers               Buffer usage
configuration         Stored configuration
interfaces            Interface information
ip <keyword>          Internet Protocol information
lines                 Serial line information
log                   Log buffer
modem <keyword>       Internal modem information
netbeui <keyword>     NetBeui information
novell <keyword>      NetWare information
processes             Active system processes
security              Internal userlist
users                 Current users of system
version               General system information
LanRoverE_3F6500#
```

Since the LanRover can be used to gain access to any phone lines connected to it (or to any networked machines connected to it via the telnet command), The Don could use this system as a relay point to mask his steps for future attacks. That could be fun for stuff later on, but his goal right now was to find the telephone switch. He had promised, and he'd deliver.

A few minutes later, another good connection.

```
CONNECT 2400/NONE

Version 0101, Release 29(09/14), Rom 3, 128K.

Password : 110XXXXXXXX
```

Some sort of password was already entered in the field, so on a hunch The Don simply pressed Enter. Not surprisingly, he was presented with a menu.

```
                    Credit Report Menu

                    Credit Station
                    Bureau Status
                    Other Services
                    Function Key setup
                    Initiate Service Call

              Use arrows to select Choice and press return.
              Or enter first letter of selection.
              Hit ESC to return to previous menu.
```

Pressing C, The Don was prompted with a submenu.

```
::::::::::::::::::CREDIT STATION:::::::::USER A::::BATCH 1 :::::::
 A)dd, E)dit, F)ind applicant, G)enerate letter, H)old, D)elete, L)ist,
 T)ransmit, O)nline, C)ancel transmit, B)atch selection, P)rint letters.
                        Use Arrows. ESC-exit
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
```

Curious of what the system could be, The Don pressed G to delve deeper and was greeted with yet another menu.

```
                                CREDIT STATION          USER A    BATCH 1

                                LETTER GENERATION

A- DENIAL           J- INADEQUATE COLL  S- WE DO NOT GRANT  1- COND APPRVL
B- CREDIT APP INC   K- TOO SHORT RESID  T- OTHER (SPECIFY)  2- ADD COLLATRL
C- INSUFF CR REF    L- TEMP RESIDENCE   U- PAY HIST LETTER  3- CO-SIGN REQ
D- TEMP/IRR EMPLY   M- UNABLE VER RESI  V- Info. From CBI   4- PAY HISTORY
E- UNABLE VER EMP   N- NO CREDIT FILE   W- Info Local Bur   5- CLAIMS & ACK
F- LENGTH OF EMPLY  O- INSUFF CR FILE   X- Info. From TU    6- PNOTE LETTER
G- INSUFF INCOME    P- DEL CR OBLIGAT   Y- Info. From TRW   7- cllctr ctgs
H- EXCESSIVE OBLIG  Q- GAR,ATT,FOREC,   Z- CLOSING          8- MEMO
I- UNABLE VER INCO  R- BANKRUPTCY       0-                  9- OUT. SOURCE
```

The system appeared to be an insurance, rental, or leasing agency. Escaping back to the main menu, The Don selected B for Bureau Status. A short listing appeared on his screen.

```
                          CREDIT STATION          USER A

                          BUREAU STATUS DEPT 1
  # Bureau       #Ind #Jnt Calls Tot_Access Last_Access    #err Status
  1 CBI          4790   0  1135 17:01:30    Wed  15:04     41 Ready
  2 TRW          1136   0   168 15:38:04    Thu  12:46      8 Ready
  3 TRANS UNION   290   0    97  3:13:56    Tue  02:53      2 Ready
  C TRANS UNION   234   0    27  1:18:33    Thu  01:01      4 Ready
  J ATLAS           3         4  0:00:59    Wed  01:39      0 Ready
```

So, this system also had direct access to a variety of credit bureaus. Just like the other systems that The Don had encountered thus far, no password was required. If The Don ever needed to pull credit information on an individual target, this would be the place to do it. Maybe he'll mention this to Knuth. Or maybe he'll just keep it to himself for now. He chuckled, made a note of it, and kept going.

The next system looked familiar. But from where?

```
CONNECT 19200

Local -010- Session 1 to GG established

*********************************************************************
*                                                                   *
*                         W A R N I N G                             *
*                                                                   *
*                       INTERNAL USE ONLY                           *
*                                                                   *
*               UNAUTHORIZED ACCESS IS PROHIBITED                   *
*                                                                   *
*********************************************************************

Username:
```

The Don grabbed a small notebook from his courier bag, laid it out on the table, and started flipping through the ragged pages. Then it dawned on him—while doing some research for the landmine heist with the crew back in Boston, he had happened upon a similar looking system that served him well. And although it looked like a typical DECServer prompt, it was not. It was most likely an Alcatel/DSC DEX 600 switch or the older 200 or 400 series. When The Don came across this type of system last year, he had turned away from his computer to sift through some papers. He turned back around to realize that he had been logged in automatically. The system timed out and just let him through. Was that a bug or feature? What were the chances that the same thing would occur here?

The Don sat motionless for a few seconds and waited to find out. The seconds turned into minutes. Then, suddenly, the screen came to life.

```
Error reading command input
Timeout period expired

>
```

And there he was.

The Switch

The Don cracked his knuckles, loosened up his wrists, and got down to business. To make sure he was on the same type of system he had seen before, he typed the universal command for help.

```
>HELP

   FORMAT :

   COMMAND(S) :

   MMI COMMAND(S)
   [ (UNIQUE             - "KEYWORD1 KEYWORD2 KEYWORD3")
     (GROUP              - "? ? ?")
     (ALL MMIS           - "ALLKEY")
     (TEXT FOR ALL MMIS - "ALLTXT") ] : ALLKEY
ABOUT  ADDING  CELLS
ABOUT  DELET   CELLS
ACK    ALARM
ACTIVA CELNET  LINK
BUILD  CP      ROAMER
CALL   TRACE
CHANGE CELL    FEATUR
CHANGE CP      MOBID
CHANGE MOB     CELL
CHANGE MTN     PHYLNK
CHANGE TEST    ACCESS
CHANGE USNAME
COPY   DAN
DELETE CELL    FEATUR
DELETE CP      BILLID
DELETE CP      CARIER
DELETE CP      MOBID
DELETE PASSWO
DISPLA ALARM   DEFCON
DISPLA CALL    RECAVL
```

```
DISPLA CP       MOBID
DISPLA CP       SUBSCR
DUMP   DISK
HELP
IDLE   MOBILE
INIT   CRASH
LOAD   DAN      MESSAG
MANUAL TRUNK    TEST
MODIFY SYNCH    LINE
PUT    MOB      CHAN
RECORD DAN      MESSAG
REPORT BAD      SECTOR
STATUS CALL
STATUS NETWOR
VERIFY MOB      NAILED
```

The list kept going. The commands scrolled down the screen like a waterfall. Over 1000 available commands. Most were self-explanatory, like `CHANGE CP MOBID` to change the phone number of the mobile phone or `STATUS NETWOR` to obtain the status of the system. Others were more obscure. For once, a help menu was surprisingly useful and gave The Don the ammunition he needed to complete his mission. It even listed diagrams on how to add or delete a cell from the network.

This was definitely the cellular switch he was looking for. And, judging by the command list, he had complete control. Beautiful.

From his previous score, he was already familiar with the `DISP CP SUBSCR` command, which was used to display specific information about a single mobile phone or range of phones. This was the best way to identify the phone number Knuth had given him.

```
>DISP CP SUBSCR
  Enter the single 7-digit MOBILE ID number or the range of
  7-digit MOBILE ID numbers to be accessed or DEFAULT
  [0000000 - 9999999, DEFAULT]
  :  7238424
```

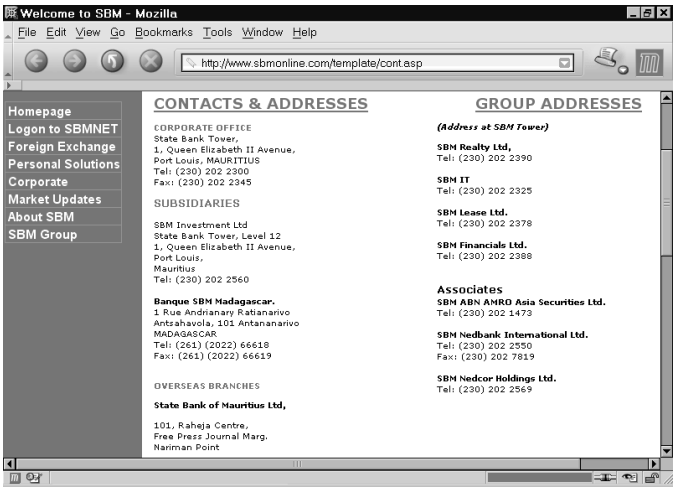
```
MOBILE ID = 7238424     COVERAGE PACKAGE = 0      SERIAL NUMBER = 82A5CDC7
ORIGINATION CLASS = 1   TERMINATION CLASS = 0     SERVICE DENIED =  N
PRESUBSCR CARRIER = Y   CARRIER NUMBER = 288      OVERLOAD CLASS = 0
FEATURE PACKAGE = 4     CHARGE METER = N          LAST KNOWN EMX = 16
PAGING AREA = 1         VOICE PRIVACY = N         CALL FORWARDING = N
FORWARD # =             BUSY TRANSFER = N         NO-ANSWER TRANSFER = Y
TRANSFER # = 2022560    CREDIT CARD MOBILE = N    SUBSCR INDEX = 54768
ROAM PACKAGE =   15     LAST KNOWN LATA =  1      CALL COMPLETION = NA
CCS RESTR SUBSCR = NA   CCS PAGE = NA             VMB MESSAGE PEND = NA
VMB SYSTEM NUMBER = 0   LAST REGISTR = NA         VRS FEATURE = N
VOICE MAILBOX # =       NOTIFY INDEX = 0          DYNAMIC ROAMING = Y
REMOTE SYS ROAM = N     OUT OF LATA = N           PER CALL NUMBER = N
PRES RESTRICT = NA      DMS MSG PENDING = NA      SUBSCRIBER PIN = NA
LOCKED MOBILE = NA      LOCKED BY DEFAULT = NA

04:14:36  BS3YCT  7.2.1.0        TERM 4
```

The interesting thing about this entry is that the No-Answer Transfer feature was enabled. All calls coming into this mobile phone were being transferred automatically to another number.

The Don quickly fired up Mozilla in another window and went straight to Google. Could this forwarding number be identified? It sure could. And it was the first hit on the list.

Identifying the Number



The phone number was a direct line into SBM Investment Ltd., a subsidiary of the State Bank of Mauritius. Whatever the Knuth was planning seemed to be much larger than The Don had imagined. It had piqued his interest and he made a mental note of the number. Then, he continued.

As Knuth requested, he wanted a list of calls coming into and going out of this mobile phone number. The CALL TRACE command provided exactly what he needed, in a friendly formatted display.

```
>CALL TRACE
MOBILE ID     : 7238424

--------      10:49:17      LINE = 0074    STN = 230
00:00:00      OUTGOING CALL
               DIGITS DIALED       226307888
00:01:28      CALL RELEASED

--------      18:55:10      LINE = 0053    STN = 230
00:00:00      INCOMING CALL       RINGING 0:04
               CALLING NUMBER      2634733033
               NAME
               UNKNOWN
00:05:19      CALL RELEASED

--------      01:12:45      LINE = 0069    STN = 230
00:00:00      INCOMING CALL       RINGING 0:02
               CALLING NUMBER      226307888
               NAME
               BIB
00:03:16      CALL RELEASED

--------      03:32:56      LINE = 0032    STN = 230
00:00:00      OUTGOING CALL
               DIGITS DIALED       2089767
00:00:47      CALL RELEASED

04:18:39  BS3YCT  7.2.1.0        TERM 4
```

The Don carefully transcribed the data from the screen to a small piece of paper. He folded it neatly and put it in his pocket. Hopefully Knuth would be happy with the results.

The final step was to remove the mobile number from the cellular phone database. As The Don noticed in the help file, a command existed specifically to do this.

```
>DELETE CP MOBID
MOBILE ID     : 7238424


<< DELETE SUCCESSFUL >>
04:21:03  BS3YCT  7.2.1.0        TERM 4
```

And it was done. Weary and with bloodshot eyes, The Don stumbled out of Maxim's and made his way back to his flat. The sun was starting to come up, but what did it matter? His mission was complete.

When he returned home, The Don removed the SIM card from the back of the Nokia 6600 and stuck it through his crosscut shredder. The shredder never liked handling plastic cards and it wheezed and moaned as it blended the SIM card into unreadable tidbits of torn plastic.

Then he counted sheep.

The Drop

The next morning, The Don went out to Bláalónið (the "Blue Lagoon"), a pool of mineral-rich water created by the run-off from a geothermal power station. It was the ultimate in outdoor hot tubs—steam and warmth amidst the jagged and cold lava fields. He sat at the edge of the water and waited, just as he was directed. He was to be approached by an elderly couple looking for directions to Krísuvík. He would give them the piece of paper, they would give him cash, and he would point them on their way.

It happened like clockwork—to celebrate, The Don went straight to Maxim's for a matinee show.

The Marketplace

Weeks passed and The Don was craving some more action. The call couldn't have come at a better time.

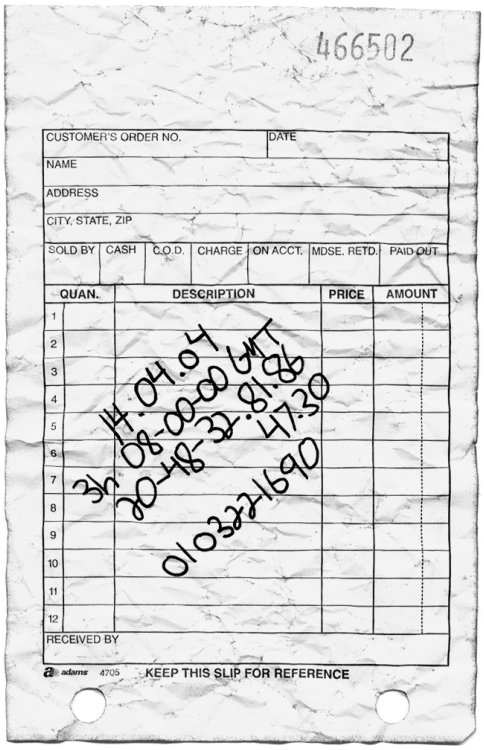
It was a Saturday morning and the weekly Kolaportið Flea Market was bustling. The smell of *harðsfiskur* (wind-dried fish) and *hákarl* (rotted shark), filled the air as people hawked crafts, delicacies, and second-hand goods from 4-foot by 4-foot wooden booths.

The Don was told to come here—another request from Knuth.

"Buy a bag of Kleinur from the vendor in the brown wool sweater," he was told, along with the order that he was to disable some phone numbers in Egypt for a specific length of time. He wandered around the large indoor warehouse, stopping at a few booths as he went. Finally, he found the vendor he was looking for—a baker. The Don's stomach grumbled.

The bag was filled with freshly made Icelandic donuts coated in powdered sugar. Inside the bag was a crumpled receipt. A sequence of numbers was written on it.

Special Receipt



Upon closer examination, it became clear what most of the sequence was: a date, a time, and three sets of numbers.

They say curiosity killed the cat, but that didn't stop The Don from starting to wonder about this Knuth guy and what he was up to. He hadn't thought much about it until Knuth contacted him for this new job. The fact that Knuth was depending so much on The Don to handle his telephone matters piqued The Don's interest. He had Knuth's phone number logged on his mobile phone, but chances are good that Knuth had called him from a payphone or spoofed his Caller ID by using an XML Integrated Voice Response application. These days, Caller ID can't be trusted and shouldn't be taken too seriously.

Maybe the phone numbers that The Don obtained from his earlier mobile phone trace for Knuth could provide some clues. One of the outgoing numbers on the phone was to the Banque Internationale du Burkina in Burkina Faso. A call from the Banque also came into the phone at one in the morning. The Don couldn't find any details online about the other two phone numbers on the phone trace, but one was obviously an outgoing call local to Mauritius and one was incoming from Zimbabwe.

As for the list of numbers he had just received, that remained to be seen. But once The Don gained access to the landline switch, he'd be sure to set up a voice intercept on one of the lines.

"Was there a connection between all of this?" The Don pondered. He would just have to wait and see. The Don took a bite of the handmade donut, put the paper back in the bag, and headed to his flat.

Landline

The public telephone network has evolved over the decades from manually switched wires carrying analog-encoded voice to an electrically switched, computer-controlled grid of wires, fiber optics, and radio carrying digitally encoded voice and other data.

Owning a landline telephone switch is nothing new. It's just that not many people have the skills to do it anymore. And that's why The Don can charge top dollar for his services, often with repeat customers. Phone phreaking (that is, hacks and exploration of telephone systems) never really

died, it has just been overshadowed by high-speed Internet connections and wireless networks. But if you look closely, it's still here.

Probably the most well-known exploits of phreaking were done by Kevin Poulsen in the mid-1980s. Kevin had access to many of California's Pacific Bell switches and routinely tapped lines and rerouted calls. And, there were the radio station contest grand prizes he won from KIIS-FM in Los Angeles, where famous DJ Rick Dees gave away Porsches to the 102nd caller during his morning show. Kevin used a clever trick that would guarantee his win every time.

Poulsen hacked into the Pacific Bell switch that controlled the subscriber lines for the radio station. Once the switch was compromised, Poulsen added the call forwarding feature to 520-KIIS, which was the first line, or pilot number, of a "hunt group," a group of numbers with a leading pilot number. When the pilot is dialed, the call hunts in sequence through the hunt group to find the first vacant, non-busy line and is connected. Kevin then forwarded the pilot to a number at his hideout; therefore, all calls into the pilot number would be forwarded to Kevin. Next, Kevin call forwarded his number to the second line in the hunt group, effectively creating a path between the pilot number, Poulsen's hideout, and second line of the hunt group. Poulsen had several other phone lines at his location in order to call into the radio station once the contest was announced.

Once Rick Dees started the Porsche giveaway, he announced each incoming caller number over the air as thousands dialed in. As the caller number neared 102, Poulsen deactivated the call forwarding from his line to the second line in the hunt group, and took his phone off the hook. This caused any legitimate caller who dialed 520-KIIS to be greeted with a busy signal, as they were being forwarded to Poulsen's off-the-hook phone.

Kevin and his associates starting calling the second line in the hunt group to guarantee that they would be the only callers into the radio station. After he won, Kevin simply removed call forwarding from the radio station's pilot number and things were back to normal. All it took was access to the phone switch and a desire for a brand-new, shiny red Porsche.

What it comes down to is that people implicitly trust the phone system. Once you gain access to the switch, the rest is like taking candy from a baby. It doesn't take much to convince someone to use the phone if they think their e-mail or network is being monitored. Most people would rather give

their credit card number to a stranger over the phone than they would through a "secure" Web site. It really doesn't matter either way; there are risks inherent in both.

Wiretapping has been around since the invention of the telephone. If the Feds can listen in on calls, so can other people, especially determined hackers. And especially The Don. Newer technologies, like Voice Over IP, can make snooping (and denial-of-service) that much easier. The switching systems also keep track of line usage, calling patterns, and customer billing in accounting logs. Most people don't care about that data, but it's there for the taking.

For all the organized crime members who hop from payphone to payphone to handle their business, there are hundreds more who talk on the phone as if they're in the "Cone of Silence." If they only knew.

Keys to the Kingdom

Through some Google searches, The Don learned that Telecom Egypt primarily used 5ESS switches, which made him smile.

By looking at the country and city codes, it was obvious that all the numbers on the crumpled receipt were located in Shebin El Kom, a sleepy Egyptian country town known for its wonderful shisha. The numbers all had the same exchange code, which meant they were in the same area.

One number was in a different format than the others. It looked like a Service Profile Identifier (SPID) for an ISDN BRI line. On a 5ESS switch, the actual subscriber number usually fits neatly between the "01" and "0" padding. ISDN often is used in place of less reliable analog modems, and The Don had seen these used with ATM machines—he'd often stick his head behind the ones in convenience stores and gas stations to see if any telephone information was written on the little tags attached to the phone wire (usually, there was).

Finding the landline phone switch for Shebin El Kom was no different than finding the cellular switch in Mauritius, though an entire 5ESS switch is much more complex than the switch he had encountered earlier. 5ESS is broken up into separate channels, each performing a specific job, and each with its own terminal connection.

The Don needed access to the Recent Change, the channel that is used to add, change, or remove services in the switch database. All the activity is logged directly to the SCCS, the Switching Control Center System, but no need to worry. There is usually so much legitimate activity on a switch that a few extra things added by The Don won't be noticed.

The Don went through the motions—researching the switch, obtaining another mobile phone, wardialing, and reviewing the list of carriers—until he found the prompt he needed.

A 5ESS switch, running on DMERT, a customized version of UNIX, was easy enough to identify.

```
CONNECT 9600


5ESS login
16 WCDS1 5E6(1) ttsn-cdN TTYW
Account name:
```

There are no default passwords for a 5ESS. The account name, also called a Clerk ID, is usually the name of an employee or his or her assigned employee number. The password usually is set to a commonly used word like RCV, RCMAC, SCC, SCCS, 5ESS, SYSTEM, MANAGER, or CLLI, though not necessarily. The Don didn't want to raise suspicion by guessing various login combinations, in case invalid login attempts were being logged.

Now, if The Don were in Shebin El Kom, he could have gone dumpster diving at the local telephone central office to obtain legitimate login and password credentials. As Artie Piscano, a mobster from the movie *Casino*, found out the hard way, writing things down that should be kept secret can lead to trouble. In Artie's case, detailed records of illegitimate transactions led to his death. It is obvious that most people have never taken this lesson to heart since all around the world there are passwords written on sticky notes attached to the sides of monitors, credit card receipts littered outside of gas stations, and printouts of financial records tossed ignorantly into the trash. It's a hacker's dream. Even knowing about the threat of trashing, companies rarely make any effort to destroy this type of information.

However, The Don was far from Egypt. So, social engineering was the next best thing. Through a few innocent phone calls to Telecom Egypt, The Don obtained the main number for RCMAC, the Recent Change Memory

Administration Center, which is the physical office in Shebin El Kom where the RC requests were handled. He took a deep breath and dialed.

"As-salaam a'alaykum," said an unfamiliar voice on the other end of the line.

"Hello? This is Dave Sullivan with Lucent 5ESS technical support services. Do you speak English?" said The Don.

"Yes, a little," the lineman responded with broken English. Luckily, though Arabic is the official language of Egypt, most educated people also speak English.

"Listen, I'm here at the AT&T Technical Support Center in Cairo and we're having trouble applying a critical service patch to the 5E software. My boss is breathing down my neck to get this fixed. Can you do me a favor?"

By now, the person on the other end would have hung up if he thought he was being tricked. But, not this time.

"Yes, Dave. How can I help?" The Don had this guy in his pocket.

"We are going to need you to log into the system and tell us what you're typing. We'll be verifying it on this end to make sure that our patch was installed correctly without affecting the line history block information."

It was that easy. The friendly lineman spelled out his Clerk ID and password. The Don held back a giggle as he wrote down the information.

"Well, it seems to be working. Hey, thanks a bunch for the help. I owe you one!"

"You are welcome," said the lineman, "Have a good day."

The Don hung up and took another deep breath. Sometimes all it took was to act as if you belong and to find a helpful person on the other end of the line. Social engineering always made him nervous. His palms were sweaty and his heart was racing, but he had what he needed. The keys to the kingdom.

Inside the Golden Pyramid

A few hours later, after he relaxed at Maxim's with a few shots of Brennivín, he continued on his quest.

```
5ESS login
16 WCDS1 5E8(1) ttsn-cdN TTYW
Account name: OBT135
```

```
Password: #####

<
```

And there he was. The 5ESS craft shell prompt. The switch was his.

"First things first," The Don thought to himself.

Using the Batch Mode Input feature, he entered three separate change orders to disable the three phone numbers specified on the paper—328186, 324730, and 322169—at Knuth's desired time. The switch swallowed up the commands and burped out an acknowledgement. On April 14, 2004, beginning at 08:00 GMT, the lines would be down for three hours.

Since he was already in the system, The Don decided to do some investigating of his own. Just for fun, he decided to set up a voice intercept using a No Test Trunk on one of the phone numbers given to him by Knuth. Maybe he would be able to figure out what Knuth was up to. When used legitimately, No Test Trunks are for emergencies, busy verification, or the testing of subscriber lines. They are also the easiest way to set up an unauthorized wiretap.

From the main prompt, The Don ran the interactive menu system and was greeted pleasantly.

```
< RCV:MENU:APPRC

                        5ESS SWITCH  WCDS1
                  RECENT CHANGE AND VERIFY CLASSES

H RCV HELP                9 DIGIT ANALYSIS          20 SM PACK & SUBPACK
A ADMINISTRATION         10 ROUTING & CHARGING      21 OSPS FEATURE DEF
B BATCH INPUT PARMS      11 CUTOVER STATUS          22 ISDN -- EQUIPMENT
1 LINES                  12 BRCS FEATURE DEFINITION 23 ISDN
2 LINES -- OE            13 TRAFFIC MEASUREMENTS    24 APPLICATIONS PROC
3 LINES -- MLHG          14 LINE & TRUNK TEST       25 LARGE DATA MOVE
4 LINES -- MISC.         15 COMMON NTWK INTERFACE   26 OSPS TOLL/ISP
5 TRUNKS                 17 CM MODULE               27 OSPS TOLL & ASSIST
7 TRUNKS - MISC.         18 SM & REMOTE TERMINALS   28 GLOBAL RC - LINES
8 OFFICE MISC. & ALARMS  19 SM UNIT

Menu Commands:
```

After finding the Routing Class assigned to the Busy Line Verification trunk group, The Don picked an unused telephone number served by the switch. He scribbled it down on the back of the receipt: 324799. Next, The Don added a test position and special route feature to his unused number. The final step was to add a Remote Call Forward feature from 324799 to 328186, the number he was interested in monitoring.

Choosing the BRCS FEATURE DEFINITION menu, The Don scrolled through to the Feature Assignment (Line Assignment) menu. He added /CFR to the first entry of the feature list, changed the value in column A (Activation) to Y, and typed U into column P (Presentation).

```
                    5ESS SWITCH WCDS1
                   RECENT CHANGE 1.11
          BRCS FEATURE ASSIGNMENT (LINE ASSIGNMENT)
*1. TN 324799 *2. OE ________ 3. LCC _____ 4. PIC 288
*5. PTY _____ *6. MLHG ______ 7. MEMB ____ 8. BFGN _____
               FEATURE LIST (FEATLIST) ROW 11.
    FEATURE A P FEATURE  A P FEATURE  A P FEATURE  A P
1. /CFR     Y U ________ _ _ ________ _ _ ________ _ _
2. ________ _ _ ________ _ _ ________ _ _ ________ _ _
3. ________ _ _ ________ _ _ ________ _ _ ________ _ _
4. ________ _ _ ________ _ _ ________ _ _ ________ _ _

Enter Insert, Change, Validate, Screen #, or Print: _
```

The Don pressed Enter twice and then U for Update. The Call Forwarding Line Parameters menu appeared automatically.

```
                    5ESS SWITCH WCDS1
                    RECENT CHANGE 1.22
                CALL FORWARDING (LINE PARAMETERS)
   *1. TN             324799
   *6. FEATURE        CFR
    9. FWDTODN        ______
   10. BILLAFTX       0                    16. SIMINTER        99
   11. TIMEOUT        0                    17. SIMINTRA        99
   12. BSTNINTVL      0                    18. CFMAX           32
   13. CPTNINTVL      0                    19. BSRING          N
```

The Don entered the number to forward to, 328186, in the FWDTODN field and pressed U again to update the contents of the screen into the database. The modifications were complete. Now, when The Don called his unassigned number, he would be bridged onto the target phone line if there were a call in progress.

Sort of like three-way calling. But much cooler. He logged out of the switch by pressing Q and then CTRL-P. Piece of cake.

Wiretap

A day later, after giving the RC time to process the change request, The Don dialed 324799, the formerly unassigned number. He heard the familiar "ta-tic" as the No Test Trunk seized the target line.

Two voices, obviously entranced in a conversation, fell silent.

"Kif tesma thalik?" a voice asked, obviously startled by the clicking of the wiretap.

"Na'am," someone replied, "Tafahdel."

"Tarid sa'id Knuth al-filus elan."

The Don didn't understand any of the conversation, but he caught Knuth's name mentioned clearly in one of the sentences. If only he spoke Arabic.

Over the next few weeks, The Don periodically checked in on his wiretap. Not surprisingly, the conversations were usually in Arabic. Occasionally, though, he caught on to some bits of English, which only served to increase his curiosity. Then, one day, he heard a familiar voice.

"Yes, I'd like to close all of the accounts."

"Right away, Mr. Knuth. May we ask what your reason is for leaving our bank?" asked a voice, speaking a perfect English dialect.

"I just don't feel that my money is safe here anymore."

The Don disconnected. He was definitely on to something big.

Aftermath

It was five in the morning. Don Crotcho, wearing a Scally cap and black tweed coat, flipped up his collar and stepped off the front stoop of his flat. He walked through the narrow, empty streets of Reykjavík.

The sun was long from rising and the air was crisp and still. He could see his breath as he made his way to the path along the Reykjavík Harbor. Past Hallgrímskirkja and the Government House, he kept walking.

"Another job well done," The Don thought to himself.

If only he knew the far reaches of the crimes he helped commit.