

Pocket mein Rocket

By: Anant Shrivastava
&

Ankur Bhargava



THE FOLLOWING **PREVIEW** HAS BEEN APPROVED FOR

ALL AUDIENCES

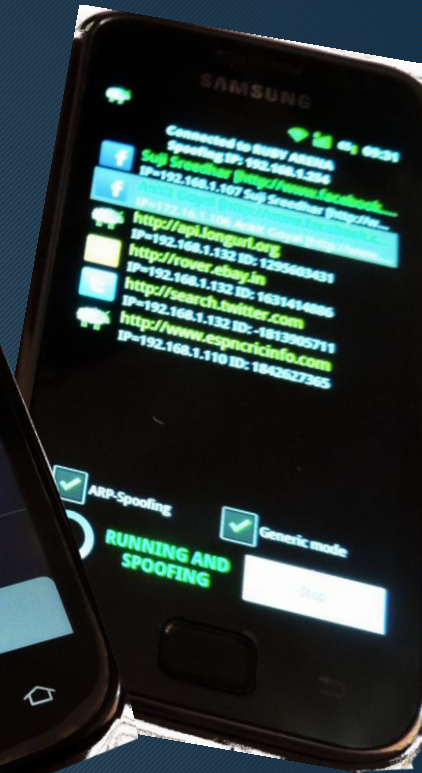
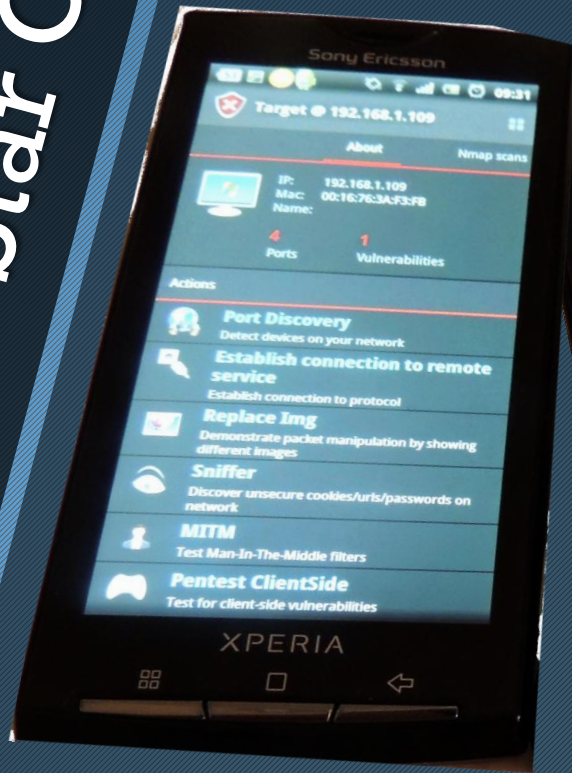
BY THE MOTION PICTURE ASSOCIATION OF AMERICA

THE FILM ADVERTISED HAS BEEN RATED



For information on film ratings,
go to www.filmratings.com

Star Cast



Supported by

- “ Network Discovery
- “ zAnti by Zimperium
- “ Droidsheep
- “ Shark / Reader
- “ And many more

Console Support

- “ Terminal Client
- “ Skipfish
- “ Blind Elephant

Dubbed in

“ Python

“ Perl

“ PHP

“ Bash

Network Discovery

The screenshot shows the Network Discovery app interface on an Android device. At the top, there is a status bar with icons for USB, Wi-Fi, cellular signal, battery, and the time 10:09. Below the status bar is the app title "Network Discovery" in a green header. The main content area features a "Cancel" button with a red 'X' icon and an "Options" button with a green gear icon. A list of discovered devices is displayed, each with a computer monitor icon, an IP address, a MAC address, and the manufacturer name. At the bottom, there is a summary section showing the current IP address (192.168.1.127/24 on eth0), a redacted SSID, and the connection mode (WiFi).

IP Address	MAC Address	Manufacturer
192.168.1.121	00:16:76:12:60:f6	Intel Corporation
192.168.1.120	00:22:68:5e:42:7c	Hon Hai Precision Ind. Co., Ltd.
192.168.1.132	78:e4:00:ac:1e:e0	Hon Hai Precision Ind. Co.,Ltd.
192.168.1.122	00:80:48:59:39:7e	COMPEX INCORPORATED
192.168.1.119	e0:69:95:eb:f4:6f	PEGATRON CORPORATION
192.168.1.117	a0:88:b4:a3:03:14	Intel Corporate

IP: 192.168.1.127/24 (eth0)
SSID: [REDACTED]
MODE: WiFi

Network Discovery

The screenshot shows an iOS interface for Network Discovery. At the top, there is a status bar with a USB icon, Wi-Fi signal, cellular signal, battery level, and the time 10:10. Below the status bar is a title bar labeled "Network Discovery" with a toggle switch on the right. The main content area displays a discovered device with a computer icon, the IP address 192.168.1.121, the MAC address 00:16:76:12:60:f6, and the manufacturer Intel Corporation. Below the device information are two buttons: "Open (2)" with a green checkmark icon and "Closed (1)" with a red X icon. Underneath these buttons, two ports are listed: "139/tcp (netbios-ssn)" and "445/tcp (microsoft-ds)". At the bottom of the screen are two navigation buttons: "Back" with a green left-pointing arrow and "Cancel" with a red X icon.

Network Discovery

192.168.1.121
00:16:76:12:60:f6
Intel Corporation










Open (2) Closed (1)

139/tcp (netbios-ssn)
445/tcp (microsoft-ds)

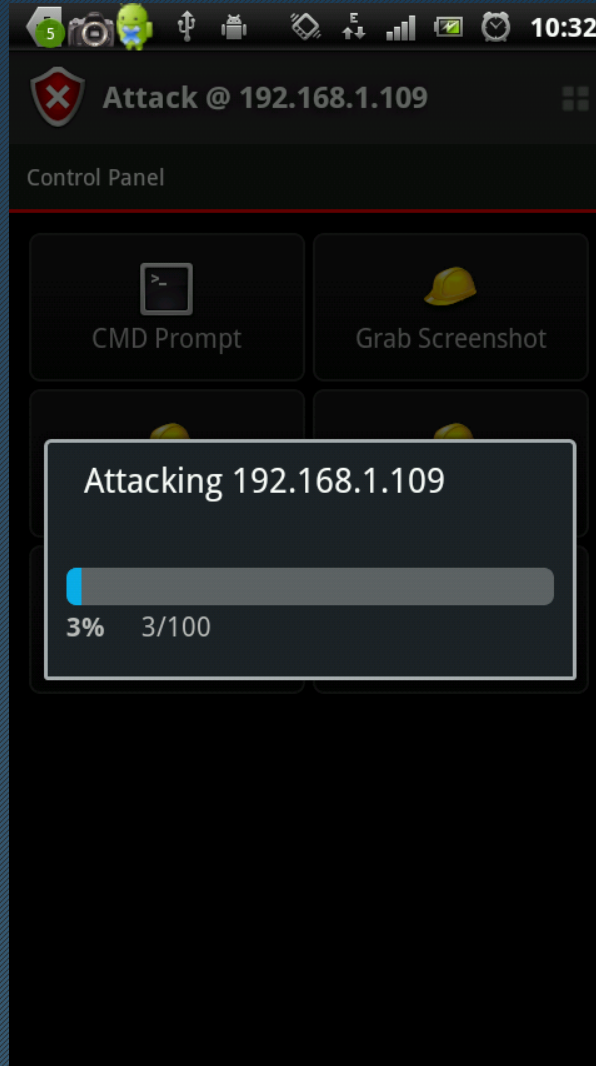
Back Cancel

zAnti

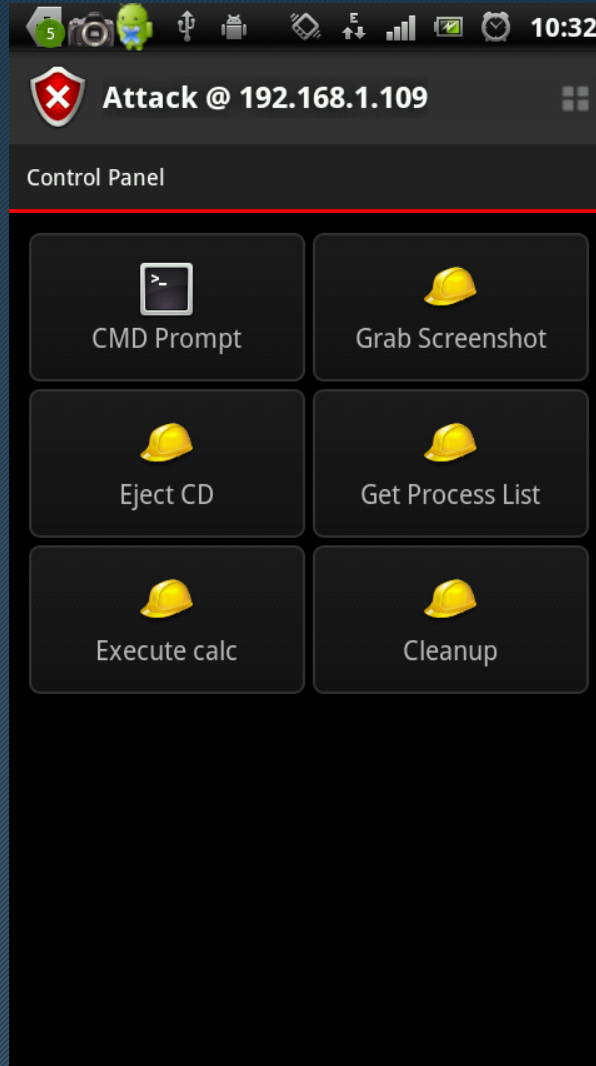
The screenshot shows the zANTI mobile application interface. At the top, there is a status bar with various icons and the time 10:31. Below that is the app header with the zANTI logo and a zScore of 86. The main content area displays a list of detected hosts under the 'Foreign' tab. Each host entry includes an icon, an IP address, a MAC address, and a 'ports' button with a red number indicating the number of open ports.

Foreign	ruby arena	ruby arena
	192.168.1.243 1C:AF:F7:6A:1E:27	ports 4
	192.168.1.102 00:27:0E:18:50:6B	ports 4
	192.168.1.233 14:D6:4D:50:05:26	ports 4
	192.168.1.235 14:D6:4D:50:05:26	ports 4
	192.168.1.235 14:D6:4D:50:05:01	ports 4
	192.168.1.231 14:D6:4D:50:06:81	ports 4
	192.168.1.109 00:16:76:3A:F3:FB	ports 4
	192.168.1.106 00:80:48:68:71:CC	ports 5
	192.168.1.112	ports

zAnti



zAnti



5

Attack @ 192.168.1.109

10:32

Control Panel

CMD Prompt

Grab Screenshot

Eject CD

Get Process List

Execute calc

Cleanup

DroidsSheep

Connected to Internet
Spoofing IP: 192.168.1.254

-  <http://www.google.de>
IP=192.168.1.109 http://www.google.de@...
-  <http://www.facebook.com/Sudh.Goyal/> [http://www.facebook.com/Sudh.Goyal/]
IP=192.168.1.107 Sudh.Goyal [http://www.facebook.com/Sudh.Goyal/]
-  <http://www.facebook.com/Ankit.Goyal/> [http://www.facebook.com/Ankit.Goyal/]
IP=172.16.1.106 Ankit Goyal [http://www.facebook.com/Ankit.Goyal/]
-  <http://api.longurl.org>
IP=192.168.1.132 ID: 1295603431
-  <http://rover.ebay.in>
IP=192.168.1.132 ID: 1631414886
-  <http://search.twitter.com>
IP=192.168.1.132 ID: -1813905711
-  <http://www.espn.com>
IP=192.168.1.110 ID: 1842627365
-  <http://www.google.com>
IP=192.168.1.116 ID: -1700429508
-  <http://www.google.co.in>
IP=192.168.1.116 ID: 1683548255
-  <http://api.webrep.avast.com>

ARP-Spoofing Generic mode

SPOOFING ONLY Start

Shark

Shark

DHARMA PRODUCTIONS AND RED CHILLIES ENTERTAINMENT PRESENT
A KARAN JOHAR FILM
STUDENT OF THE YEAR
DHARMA
ADMISSIONS OPEN!
WATCH THE TRAILER
TO ENROLL

Parameters: `-w -s 0`

Start

Stop

Open capture file (You can use Shark Reader)

Status: Running
Filename: /sdcard/shark_dump_1344054944.pcap
Size: 0 bytes
Got 584 Got 604

Terminal

```

$ export PATH=/data/local/bin:$PATH
$ ls
efs
config
sdcard
acct
mnt
vendor
d
etc
init
dbdata
cache
recovery.rc
default.prop
system
init.herring.rc
sbin
voodoo
recovery
sys
lpm.rc
ueventd.rc
usr
proc
init.rc
data
res
fota.rc
ueventd.herring.rc
lib
ueventd.goldfish.rc
init.goldfish.rc
tmp
dev
bin
$ █
```

Skipfish

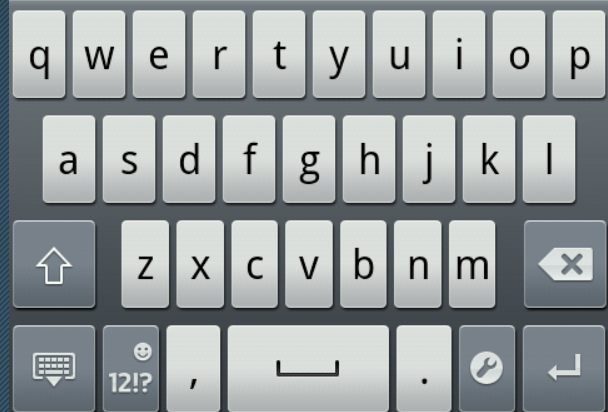
```
bash-4.0# skipfish --version
skipfish version 2.03b by <lcamtuf@google.com>
skipfish: invalid option -- '-'
Usage: skipfish [ options ... ] -o output_dir start_url
      [ start_url2 ... ]

Authentication and access options:

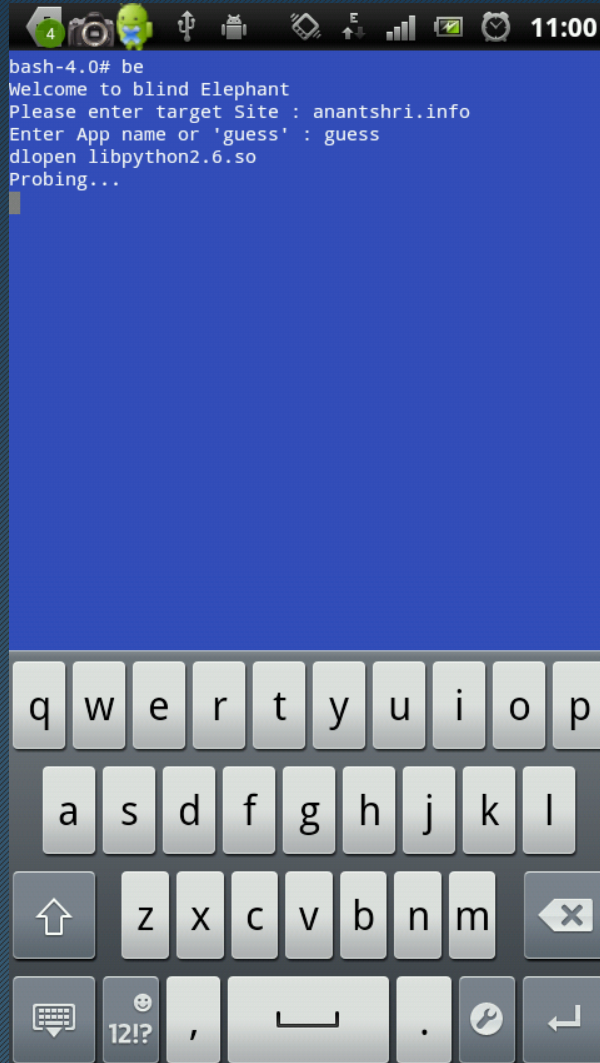
  -A user:pass  - use specified HTTP authentication
credentials
  -F host=IP    - pretend that 'host' resolves to 'IP'
  -C name=val   - append a custom cookie to all requests
  -H name=val   - append a custom HTTP header to all requests
  -b (i|f|p)   - use headers consistent with MSIE / Firefox / iPhone
  -N           - do not accept any new cookies

Crawl scope options:

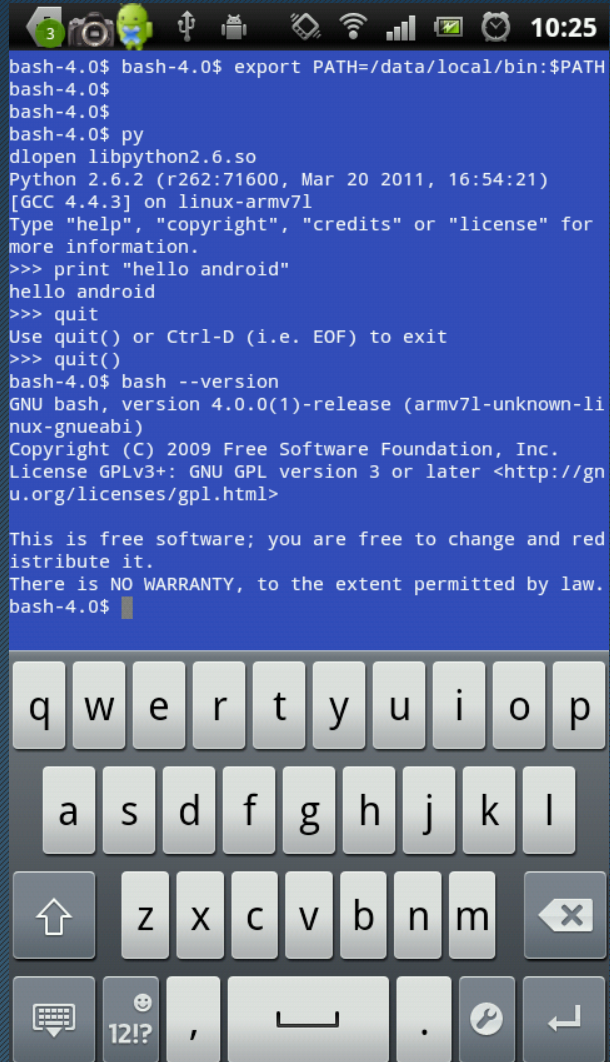
  -d max_depth - maximum crawl tree depth (16)
  -c max_child - maximum children to index per node (512)
  -x max_desc  - maximum descendants to index per b
```



Blind Elephant



Shells



The image shows a screenshot of an Android terminal application. At the top, there is a status bar with various icons and the time 10:25. The terminal window has a blue background and displays the following text:

```
bash-4.0$ bash-4.0$ export PATH=/data/local/bin:$PATH
bash-4.0$
bash-4.0$
bash-4.0$ py
dlopen libpython2.6.so
Python 2.6.2 (r262:71600, Mar 20 2011, 16:54:21)
[GCC 4.4.3] on linux-armv7l
Type "help", "copyright", "credits" or "license" for
more information.
>>> print "hello android"
hello android
>>> quit
Use quit() or Ctrl-D (i.e. EOF) to exit
>>> quit()
bash-4.0$ bash --version
GNU bash, version 4.0.0(1)-release (armv7l-unknown-li
nux-gnueabi)
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and red
istribute it.
There is NO WARRANTY, to the extent permitted by law.
bash-4.0$
```

Below the terminal window is a virtual keyboard with the following keys:

Row 1: q, w, e, r, t, y, u, i, o, p

Row 2: a, s, d, f, g, h, j, k, l

Row 3: ↑, z, x, c, v, b, n, m, ✕

Row 4: 🗃️, 12!?, , , _ , ., ⚙️, ↩️

Get your Own Rocket????

“ When are you getting your
own Rocket????”

Collection available as Droidcat
@ your nearest playstore
<http://bit.ly/w25pHq>

Directed and produced by

“ Anant : <http://anantshri.info>
“ Ankur : <http://hakers.info>