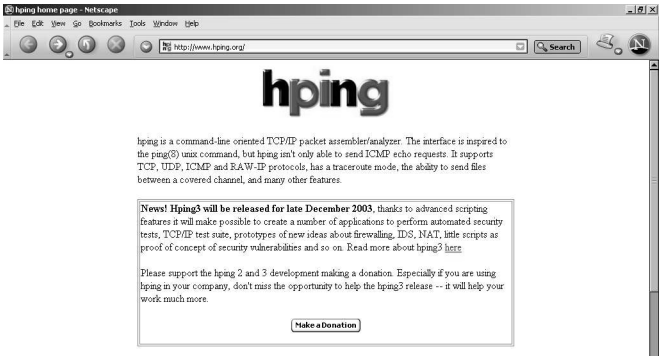
hping:
a packet injection tool

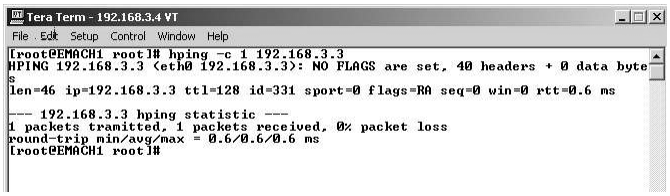
David Morgan

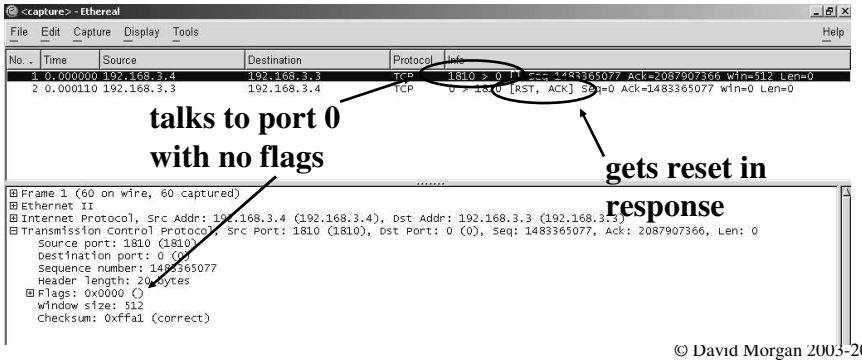
Installation



- download from the “hping 2.0.0 release candidate 3” link
- to get tarball hping2.0.0-rc3.tar.gz
- installation is smooth and uneventful
- call as “hping” or “hping2” but “man hping2” (*not* hping)

hping –c 1 192.168.3.3

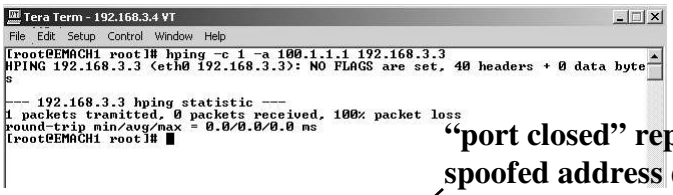




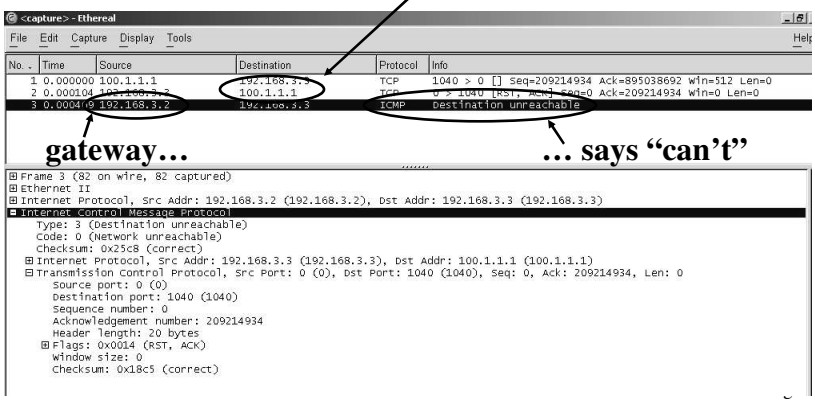
talks to port 0 with no flags

gets reset in response

hping –a 100.1.1.1 192.168.3.3



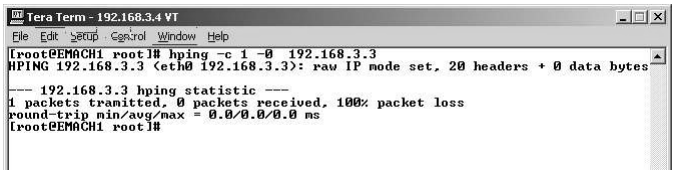
"port closed" reply goes to spoofed address (of course!)

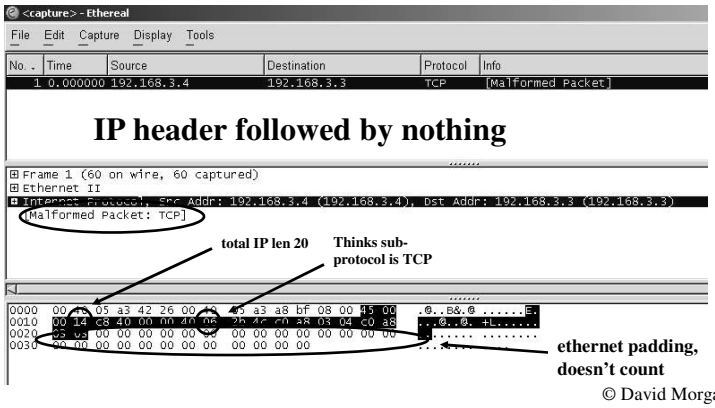


gateway…

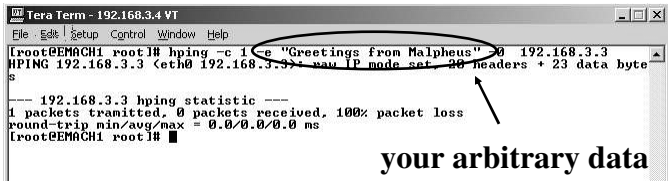
… says "can't"

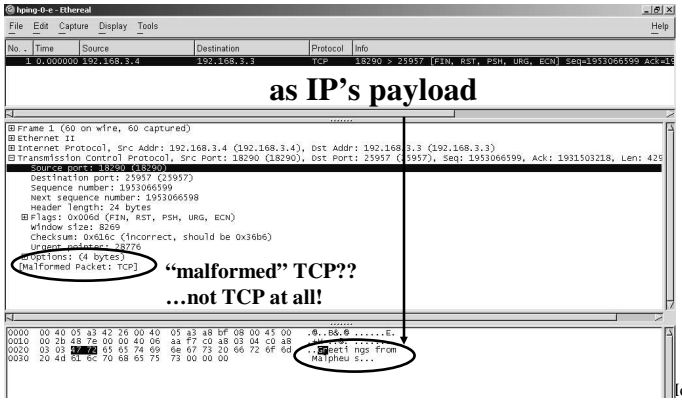
Raw IP mode: hping –0



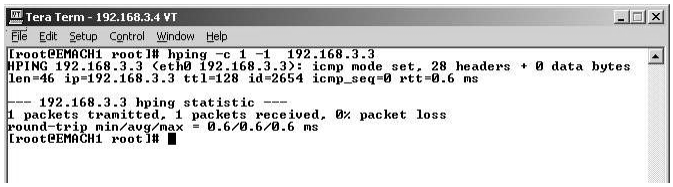


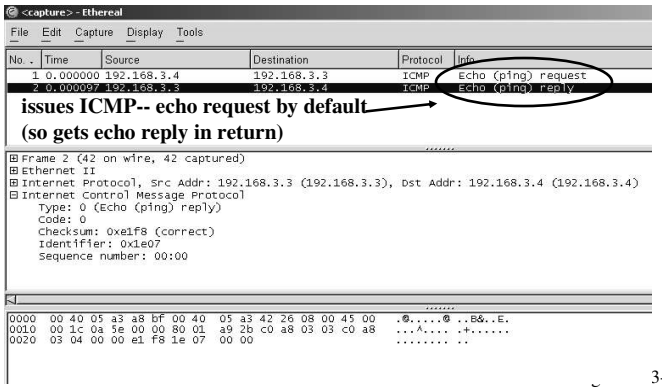
hping –0 –e *signature*





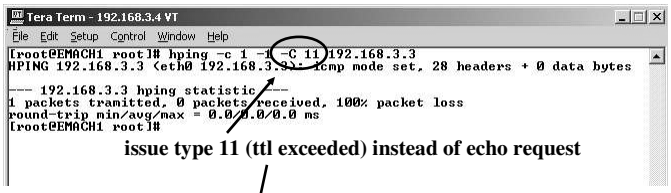
ICMP mode: hping –1

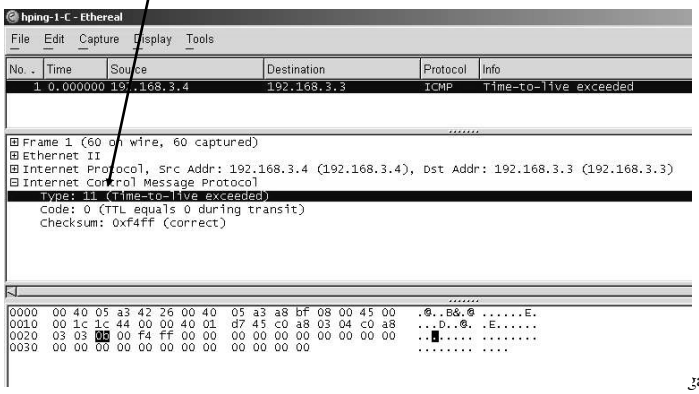




3-2008

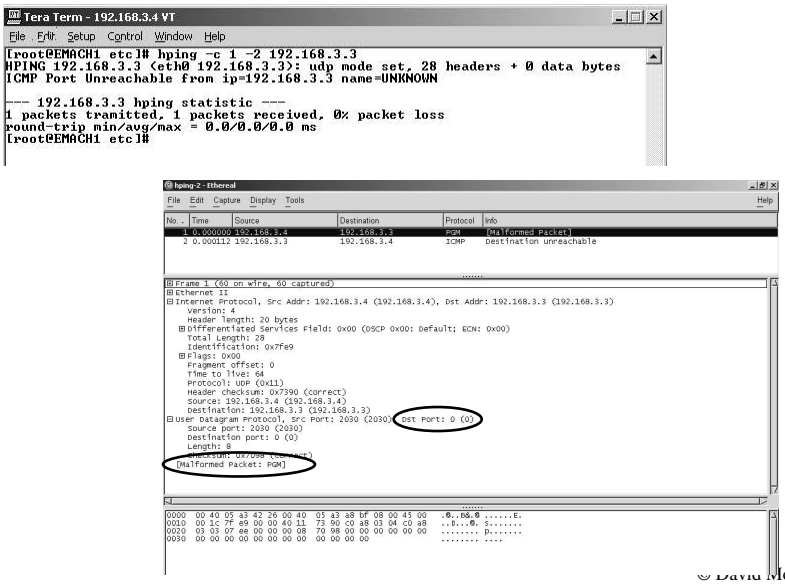
hping –1 –C *icmptype*





an 2003-2008

UDP mode: hping –2



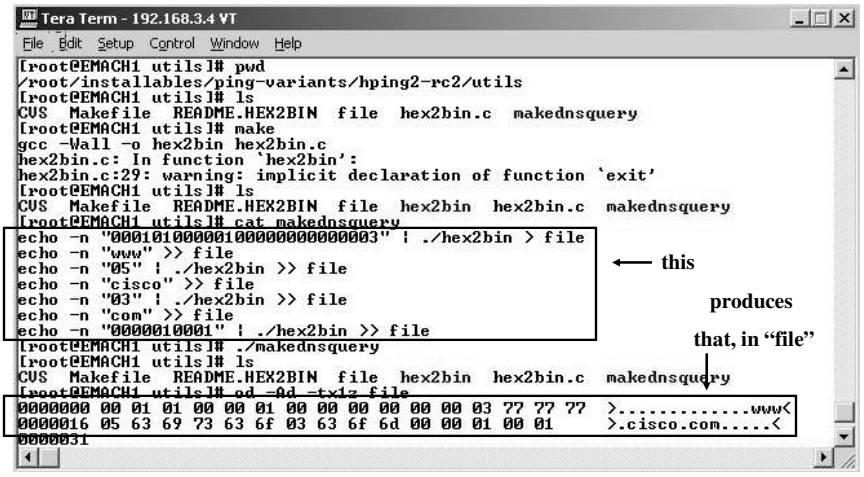
Want a packet that's not "malformed"? -- so form one

- must know the proper form (i.e., binary content) of the type of packet you want
- must compose it in a file
- hping –E will use your file content

hex2bin – binary file maker

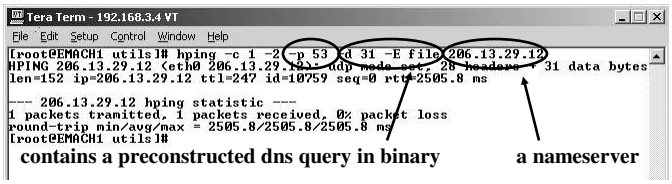
- comes with hping
- in hping2-rc3/utils directory
- converts ascii representation of hex ("ff002e") into binary

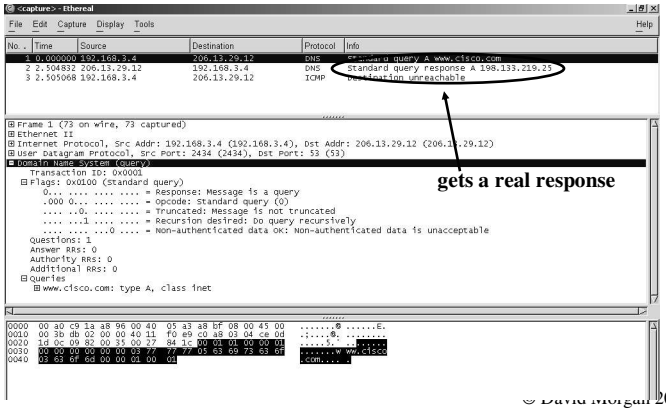
Fashion a legal, binary dns query



cf. equivalent C program, Network Troubleshooting Tools, p. 228

hping –2 –p 53





Extending it

- not interactive – needs scripting

  "Hping2 is the old version of the tool supporting the command line interfiace, while the new hping3 is the evolution that adds a Tcl scripting engine. ...If you plan to use hping in order to perform automated networks scans and security tests you can use hping3 scripts instead of hping2 + shell scripts, it is much more powerful!" - website

- scapy – another packet injection program
  http://www.secdev.org/projects/scapy/