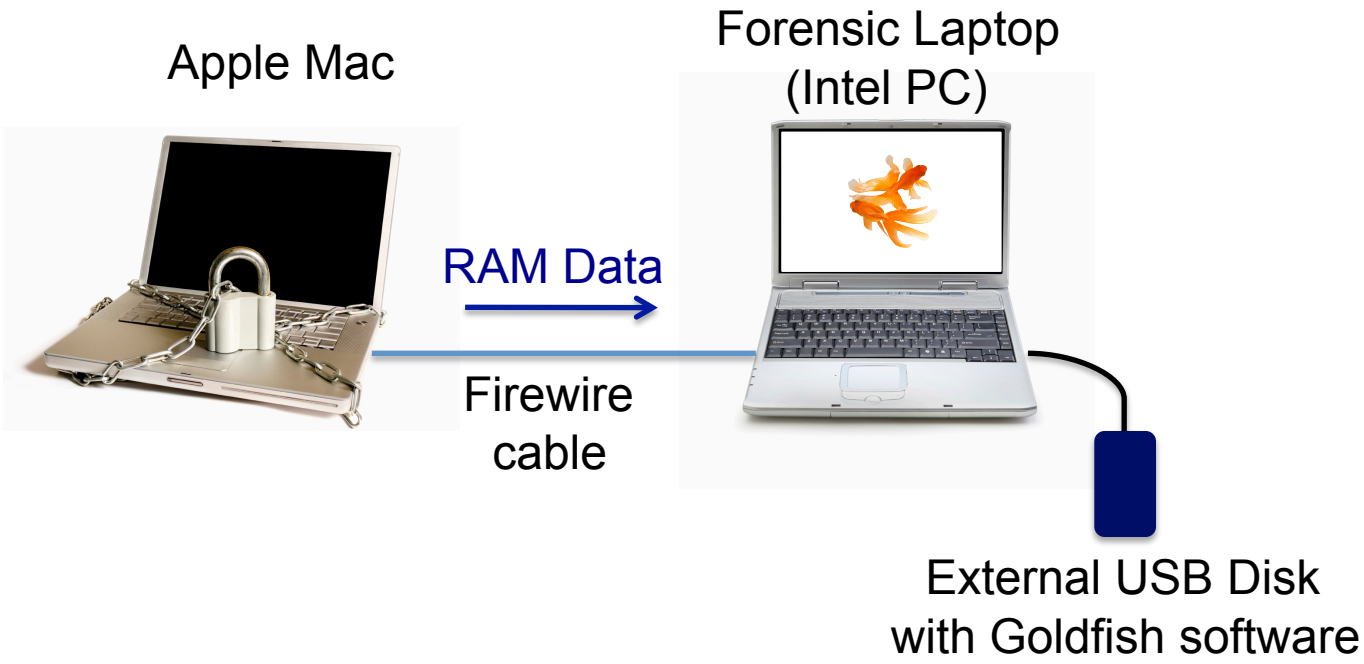
Goldfish

Mac OS X live forensics tool

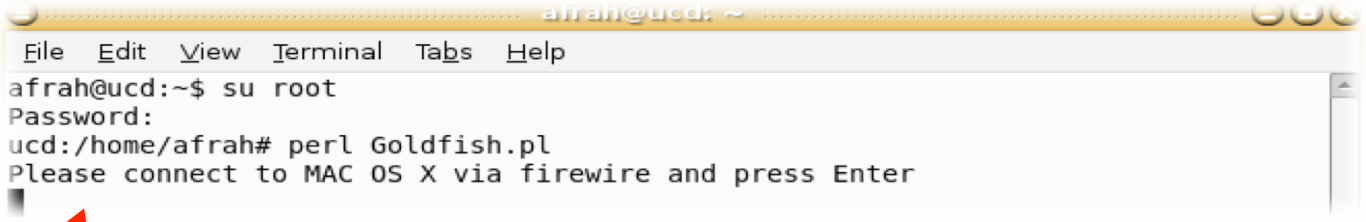
What is Goldfish?

- Goldfish is a MAC OS X live forensic tool.
- It dumps the system RAM of the target computer using a firewire cable.
- It extracts login password and any open AIM conversation fragments.
- Costs basically nothing except 15 minutes to get the results.
- Started as MSc project of Ms. Afrah Almansoori at UCD Centre for Cybercirme Investigaiton.

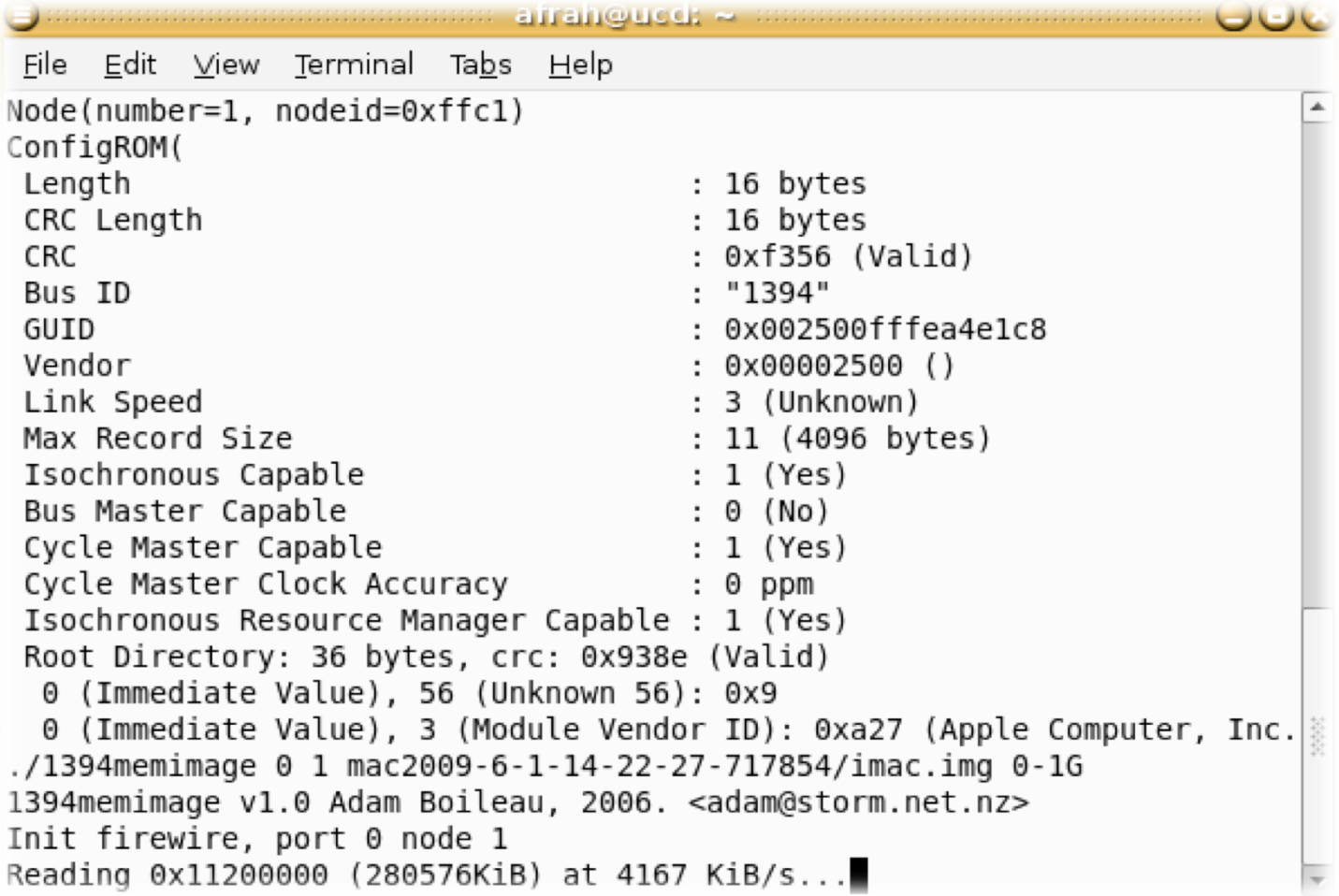
How it works?


Apple Mac
Forensic Laptop
(Intel PC)
RAM Data
Firewire
cable
External USB Disk
with Goldfish software

Snapshots

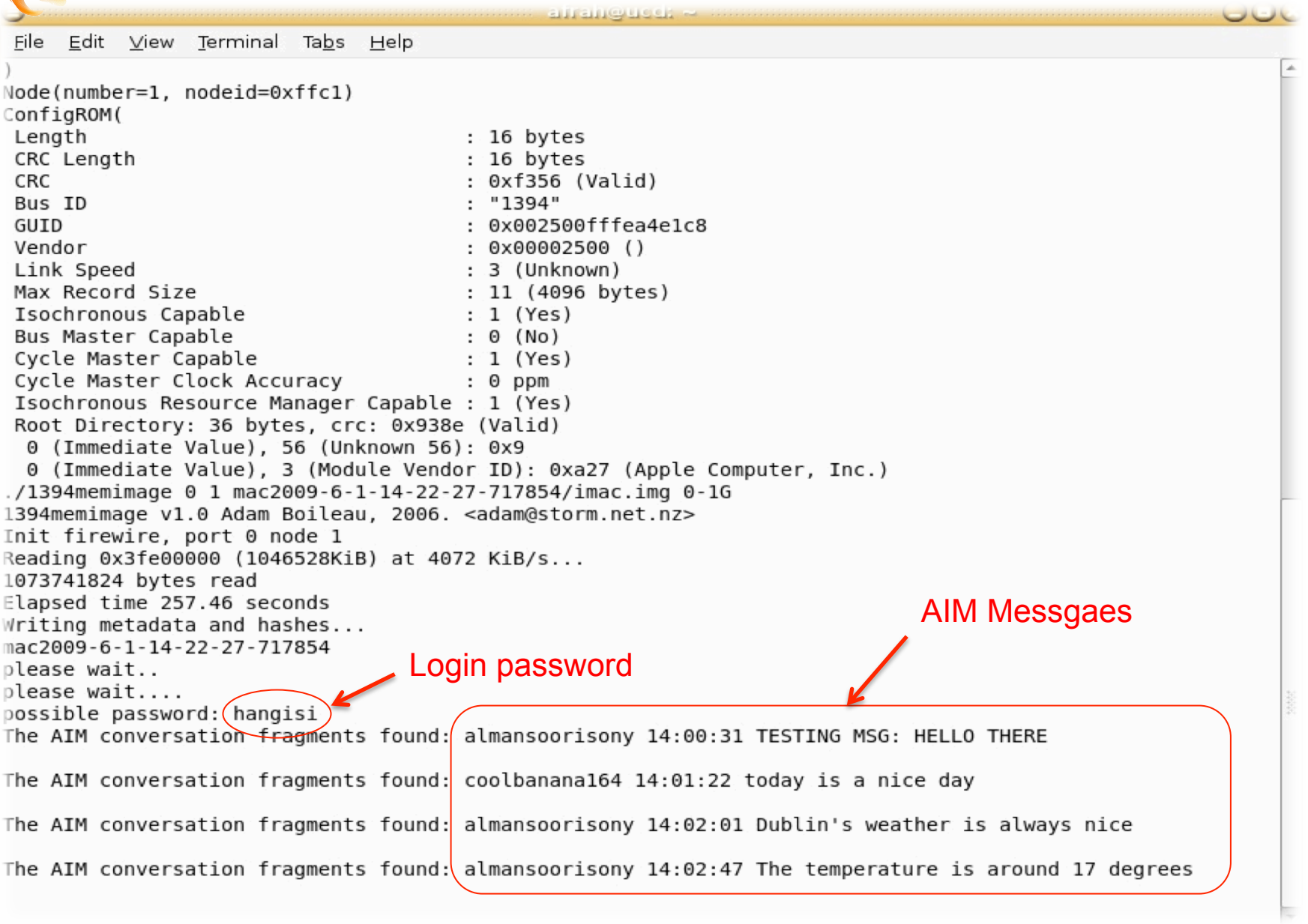


Starting Goldfish script



Imaging RAM…

Results


File Edit View Terminal Tabs Help
)
Node(number=1, nodeid=0xffc1)
ConfigROM(
Length : 16 bytes
CRC Length : 16 bytes
CRC : 0xf356 (Valid)
Bus ID : "1394"
GUID : 0x002500fffea4e1c8
Vendor : 0x00002500 ()
Link Speed : 3 (Unknown)
Max Record Size : 11 (4096 bytes)
Isochronous Capable : 1 (Yes)
Bus Master Capable : 0 (No)
Cycle Master Capable : 1 (Yes)
Cycle Master Clock Accuracy : 0 ppm
Isochronous Resource Manager Capable : 1 (Yes)
Root Directory: 36 bytes, crc: 0x938e (Valid)
0 (Immediate Value), 56 (Unknown 56): 0x9
0 (Immediate Value), 3 (Module Vendor ID): 0xa27 (Apple Computer, Inc.)
./1394memimage 0 1 mac2009-6-1-14-22-27-717854/imac.img 0-1G
1394memimage v1.0 Adam Boileau, 2006. <adam@storm.net.nz>
Init firewire, port 0 node 1
Reading 0x3fe00000 (1046528KiB) at 4072 KiB/s...
1073741824 bytes read
Elapsed time 257.46 seconds
Writing metadata and hashes...
mac2009-6-1-14-22-27-717854
please wait..
please wait....
possible password: hangisi
The AIM conversation fragments found: almansoorisony 14:00:31 TESTING MSG: HELLO THERE
The AIM conversation fragments found: coolbanana164 14:01:22 today is a nice day
The AIM conversation fragments found: almansoorisony 14:02:01 Dublin's weather is always nice
The AIM conversation fragments found: almansoorisony 14:02:47 The temperature is around 17 degrees
Login password
AIM Messgaes