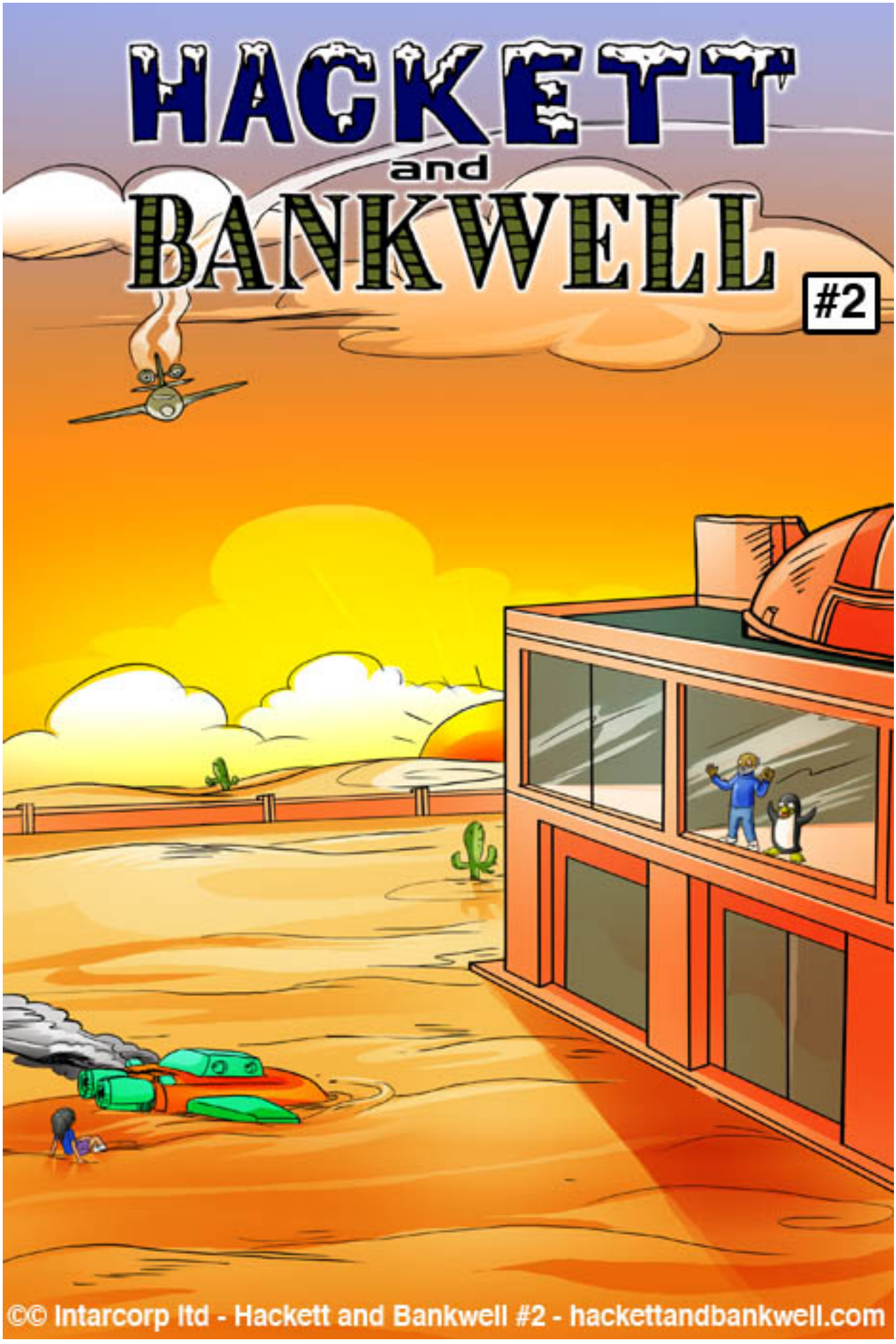
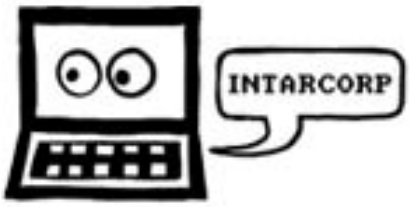

HACKETT
and
BANKWELL
#2
©© Intarcorp ltd - Hackett and Bankwell #2 - hackettandbankwell.com

Welcome to “Hackett and Bankwell” #2
Presented by Intarcorp Ltd.



This installment of “Hackett and Bankwell” introduces readers to the Command Line Interface. Like the last issue of “Hackett and Bankwell,” the goal is to leave readers with a conceptual understanding and a renewed sense of excitement in *NIX computing.

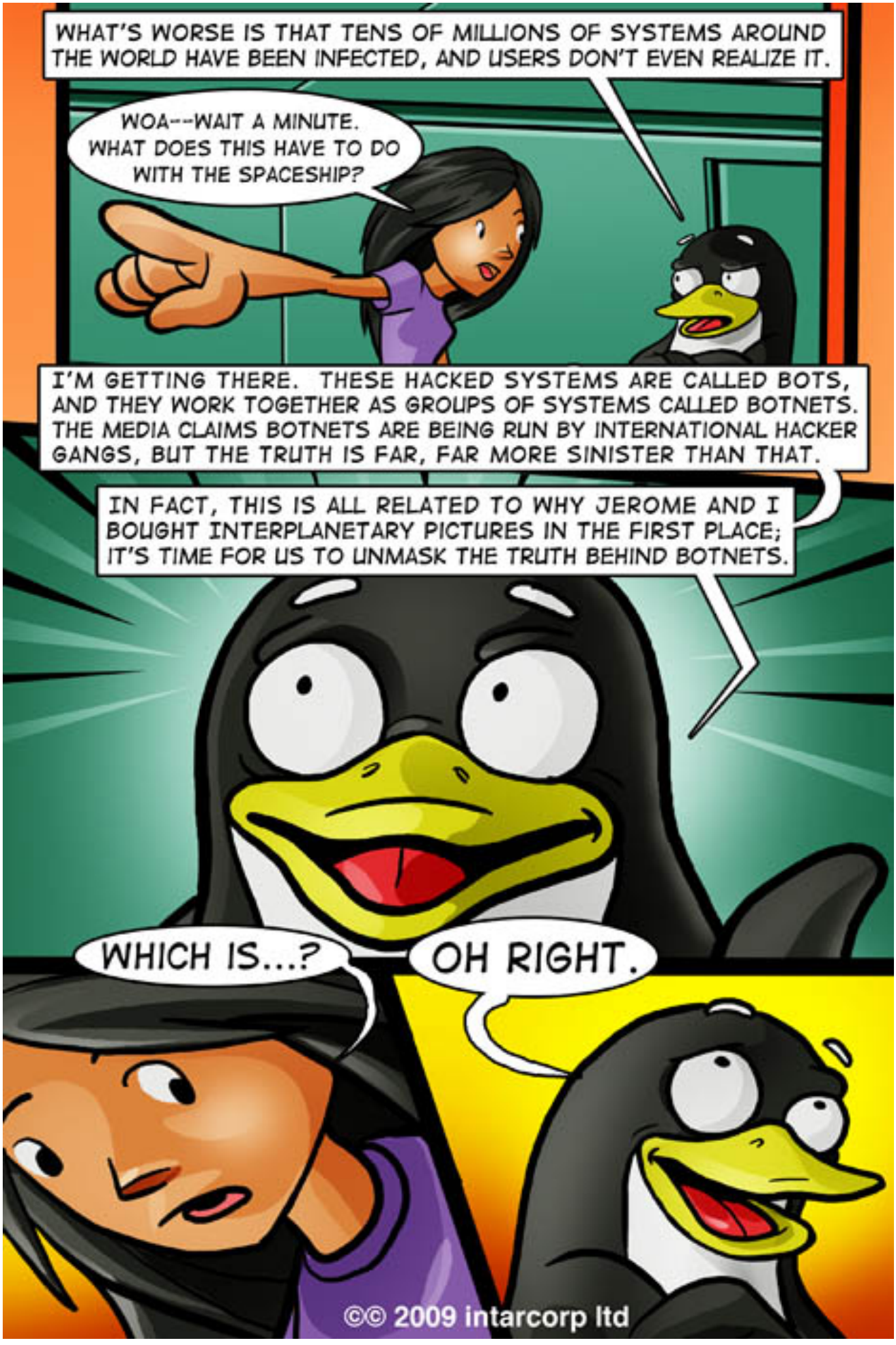
Credits:
Story: Jeremiah Gray
Illustration: Barry Cervantes
Color: Mike Borromeo

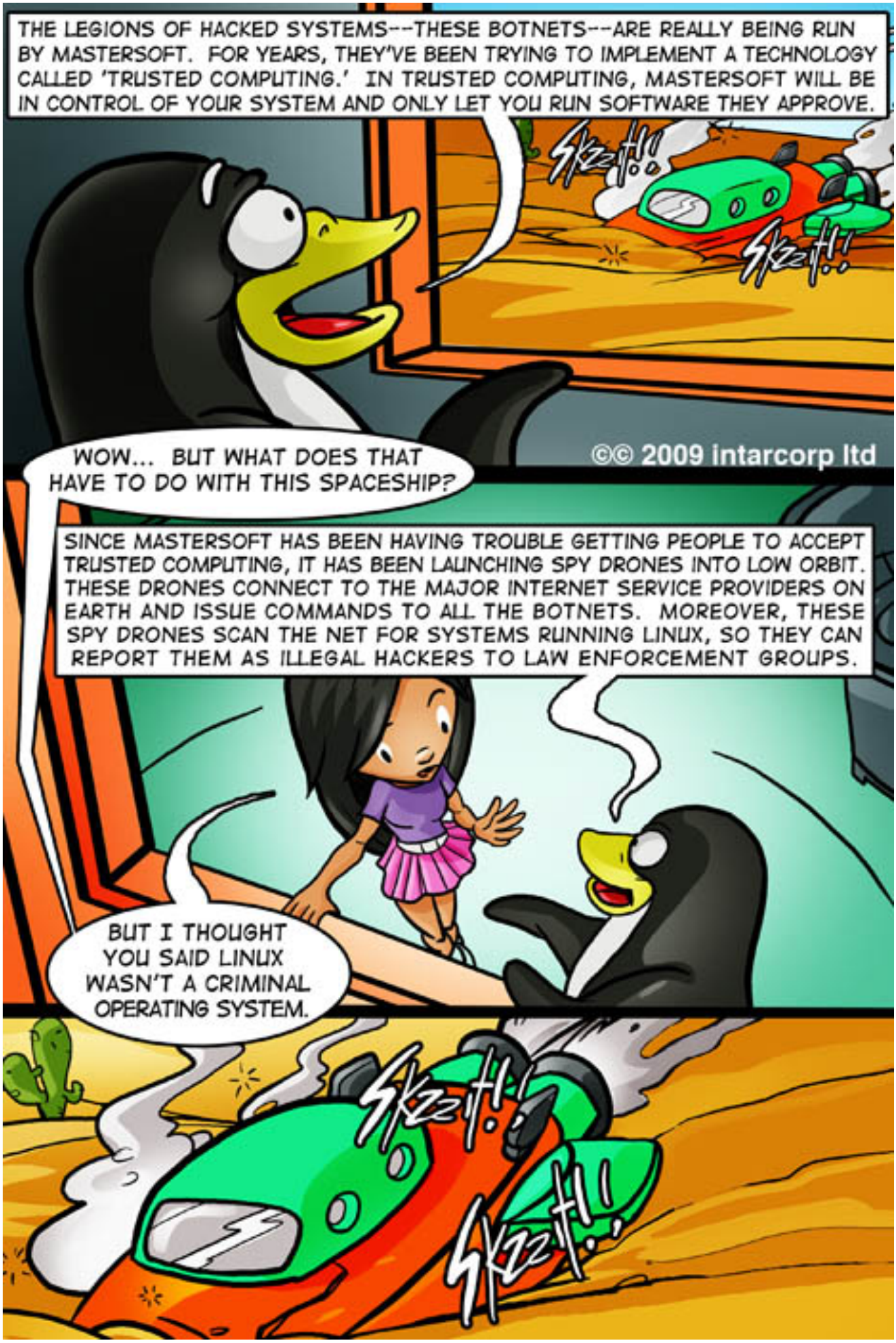
Hackett and Bankwell, characters, names, and all related indicia are trademarks of Intarcorp Ltd., licensed by Intarcorp Ltd.

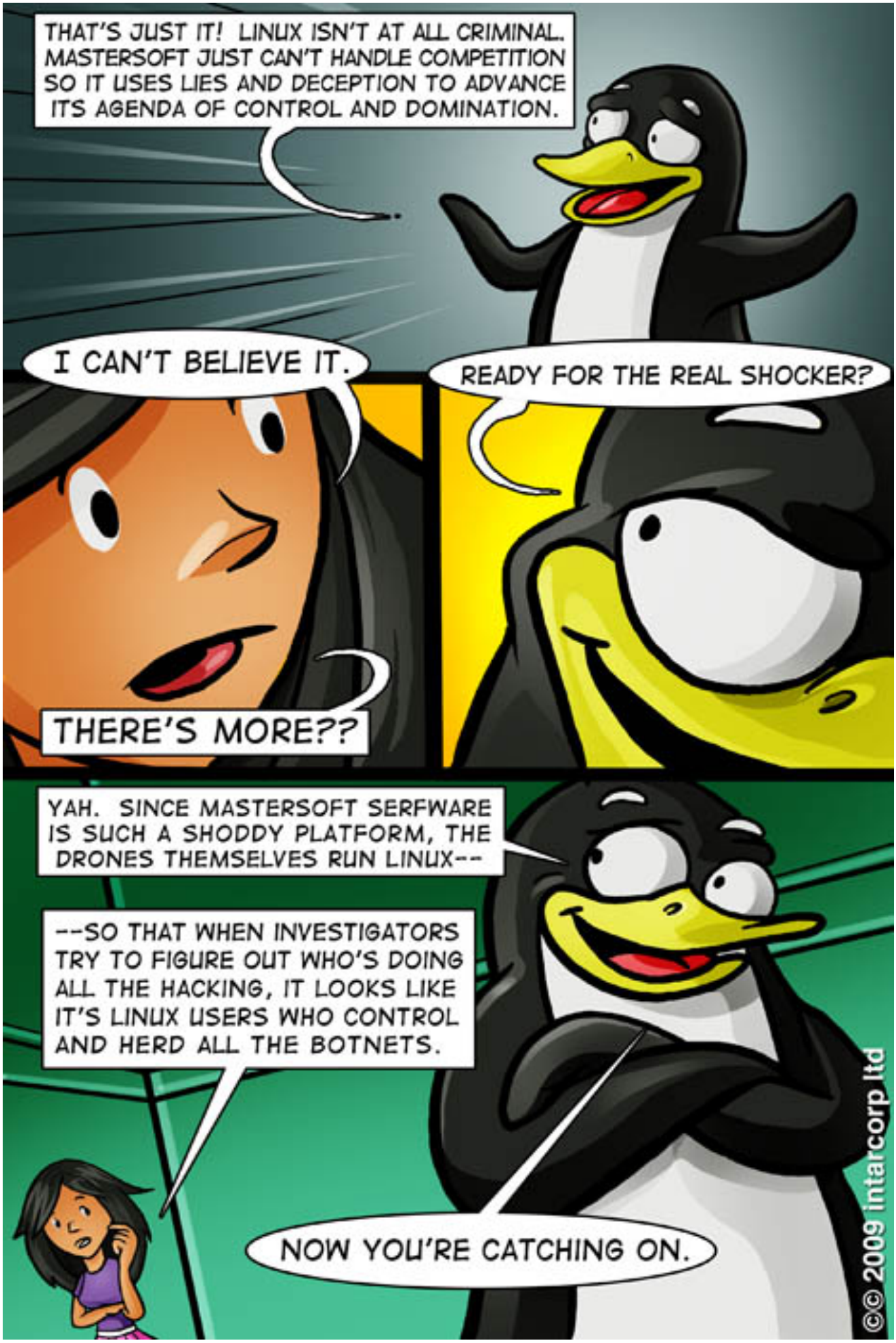
Now even comics use Linux®
Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.
Ubuntu is a trademark of Canonical Ltd.

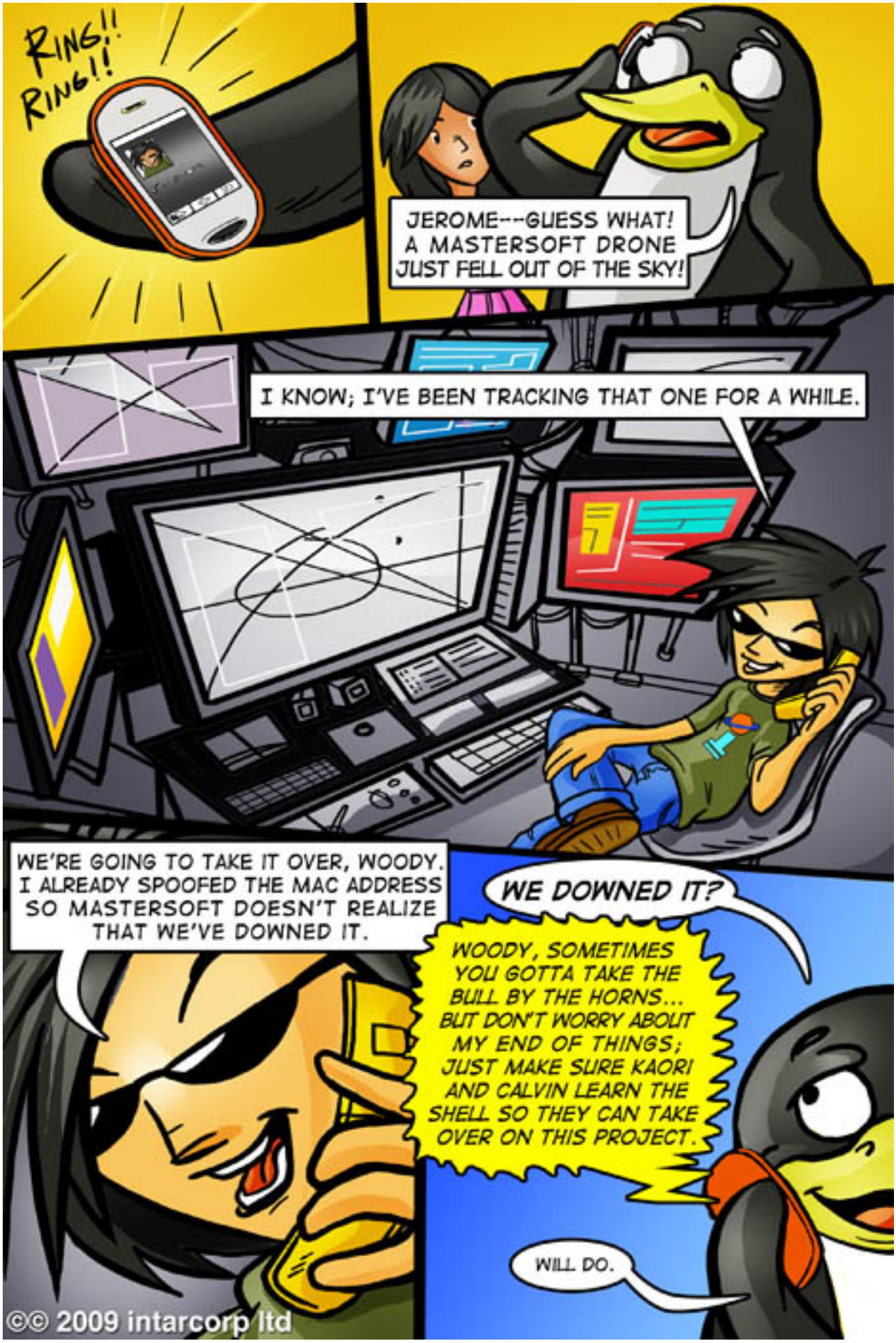
Licensed under a Creative Commons license:
Attribution-Noncommercial-No Derivative Works 3.0 United States
http://creativecommons.org/licenses/by-nc-nd/3.0/us/


Puff Puff
THIS IS NOT WHAT WE NEEDED!
WHAT? WHAT IS IT, WOODY?
A MASTERSOFT SPY DRONE.
A WHAT?
LOOK, IT'S AN OPEN SECRET THAT MASTERSOFT SERFWARE IS FULL OF HOLES THAT CAN BE EXPLOITED BY HACKERS. THEY DON'T EVEN NEED TO BE AT YOUR COMPUTER; THEY CAN INFECT IT AND CONTROL YOUR SYSTEM FROM ANYWHERE.
WOAH!
©© 2009 intarcorp ltd

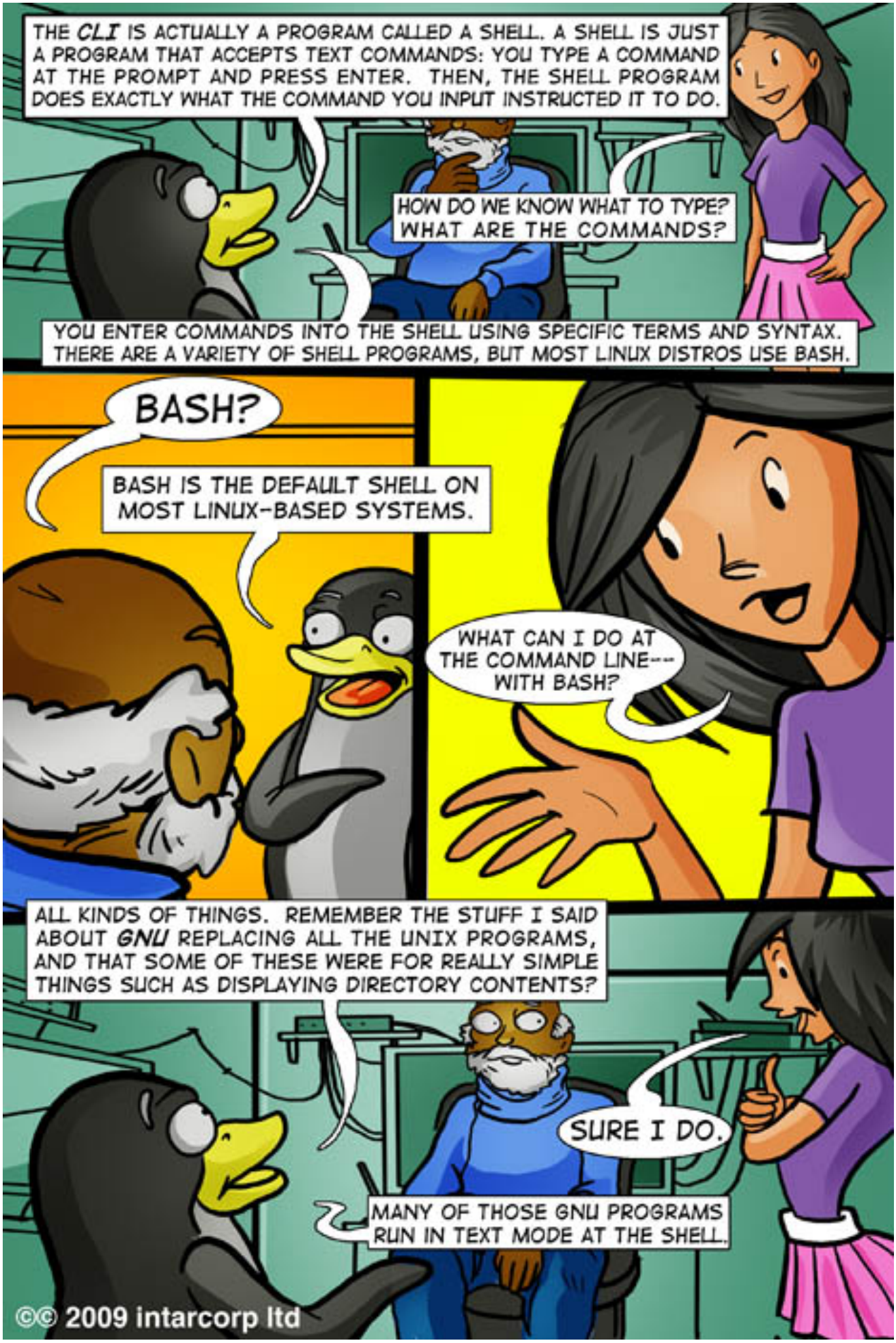

WHAT'S WORSE IS THAT TENS OF MILLIONS OF SYSTEMS AROUND THE WORLD HAVE BEEN INFECTED, AND USERS DON'T EVEN REALIZE IT.
WOA--WAIT A MINUTE. WHAT DOES THIS HAVE TO DO WITH THE SPACESHIP?
I'M GETTING THERE. THESE HACKED SYSTEMS ARE CALLED BOTS, AND THEY WORK TOGETHER AS GROUPS OF SYSTEMS CALLED BOTNETS. THE MEDIA CLAIMS BOTNETS ARE BEING RUN BY INTERNATIONAL HACKER GANGS, BUT THE TRUTH IS FAR, FAR MORE SINISTER THAN THAT.
IN FACT, THIS IS ALL RELATED TO WHY JEROME AND I BOUGHT INTERPLANETARY PICTURES IN THE FIRST PLACE; IT'S TIME FOR US TO UNMASK THE TRUTH BEHIND BOTNETS.
WHICH IS...?
OH RIGHT.
©© 2009 intarcorp ltd

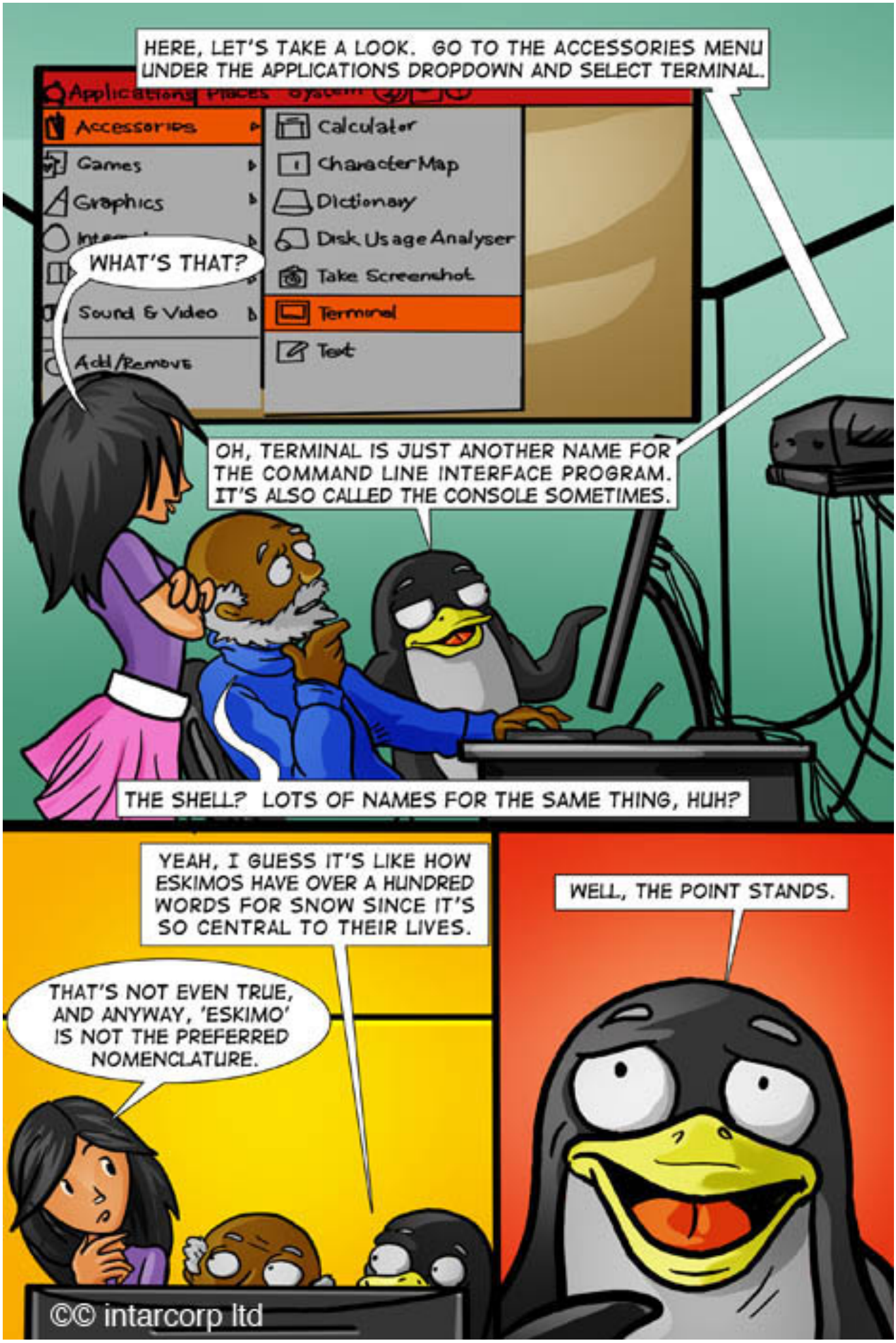

THE LEGIONS OF HACKED SYSTEMS--THESE BOTNETS--ARE REALLY BEING RUN BY MASTERSOFT. FOR YEARS, THEY'VE BEEN TRYING TO IMPLEMENT A TECHNOLOGY CALLED 'TRUSTED COMPUTING.' IN TRUSTED COMPUTING, MASTERSOFT WILL BE IN CONTROL OF YOUR SYSTEM AND ONLY LET YOU RUN SOFTWARE THEY APPROVE.
Skzzt!!
Skzzt!!
WOW... BUT WHAT DOES THAT HAVE TO DO WITH THIS SPACESHIP?
©© 2009 intarcorp ltd
SINCE MASTERSOFT HAS BEEN HAVING TROUBLE GETTING PEOPLE TO ACCEPT TRUSTED COMPUTING, IT HAS BEEN LAUNCHING SPY DRONES INTO LOW ORBIT. THESE DRONES CONNECT TO THE MAJOR INTERNET SERVICE PROVIDERS ON EARTH AND ISSUE COMMANDS TO ALL THE BOTNETS. MOREOVER, THESE SPY DRONES SCAN THE NET FOR SYSTEMS RUNNING LINUX, SO THEY CAN REPORT THEM AS ILLEGAL HACKERS TO LAW ENFORCEMENT GROUPS.
BUT I THOUGHT YOU SAID LINUX WASN'T A CRIMINAL OPERATING SYSTEM.
Skzzt!!
Skzzt!!


THAT'S JUST IT! LINUX ISN'T AT ALL CRIMINAL. MASTERSOFT JUST CAN'T HANDLE COMPETITION SO IT USES LIES AND DECEPTION TO ADVANCE ITS AGENDA OF CONTROL AND DOMINATION.
I CAN'T BELIEVE IT.
READY FOR THE REAL SHOCKER?
THERE'S MORE??
YAH. SINCE MASTERSOFT SERFWARE IS SUCH A SHODDY PLATFORM, THE DRONES THEMSELVES RUN LINUX--
--SO THAT WHEN INVESTIGATORS TRY TO FIGURE OUT WHO'S DOING ALL THE HACKING, IT LOOKS LIKE IT'S LINUX USERS WHO CONTROL AND HERD ALL THE BOTNETS.
NOW YOU'RE CATCHING ON.
©© 2009 intarcorp ltd


RING!!
RING!!
JEROME---GUESS WHAT! A MASTERSOFT DRONE JUST FELL OUT OF THE SKY!
I KNOW; I'VE BEEN TRACKING THAT ONE FOR A WHILE.
WE'RE GOING TO TAKE IT OVER, WOODY. I ALREADY SPOOFED THE MAC ADDRESS SO MASTERSOFT DOESN'T REALIZE THAT WE'VE DOWNED IT.
WE DOWNED IT?
WOODY, SOMETIMES YOU GOTTA TAKE THE BULL BY THE HORNS... BUT DON'T WORRY ABOUT MY END OF THINGS; JUST MAKE SURE KAORI AND CALVIN LEARN THE SHELL SO THEY CAN TAKE OVER ON THIS PROJECT.
WILL DO.
©© 2009 intarcorp ltd

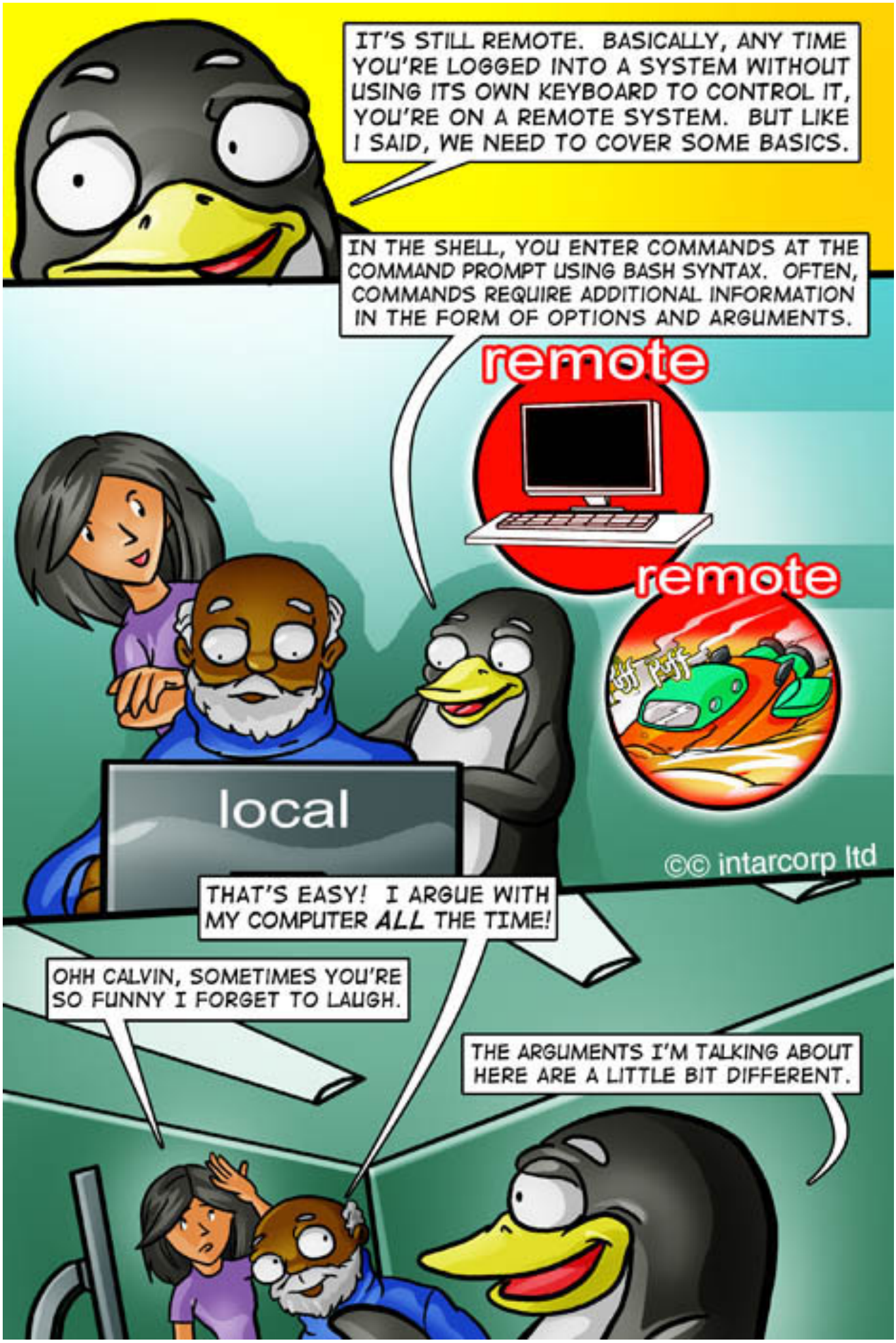

WHAT'S ALL THE RUCKUS? WHAT IS HAPPENING OUT THERE?
A MASTERSOFT SPY DRONE JUST CRASHED IN OUR YARD!
PROVIDING US WITH A PERFECT OPPORTUNITY TO LEARN TO HOW TO USE THE BASH SHELL!
WOAH...WHAT?
YOU KNOW, CALVIN, THE HACKER STUFF!
YEAH--WELL, THE TEXT-BASED STUFF AT ANY RATE.
ALL THE STUFF I'VE SHOWN YALL GUYS SO FAR IS IN THE GUI--THE GRAPHICAL USER INTERFACE. WHICH IS GREAT; YOU CAN DO TONS OF STUFF FROM THE GUI, BUT FOR THIS PROJECT, YOU'LL NEED TO USE THE COMMAND LINE INTERFACE--OFTEN REFERRED TO AS THE CLI OR SHELL.
SOUNDS SCARY.
RIGHT?
NOT AT ALL; ONCE YOU GET THE HANG OF IT, YOU'LL PREFER IT FOR ALL KINDS OF TASKS.
©© 2009 intarcorp ltd

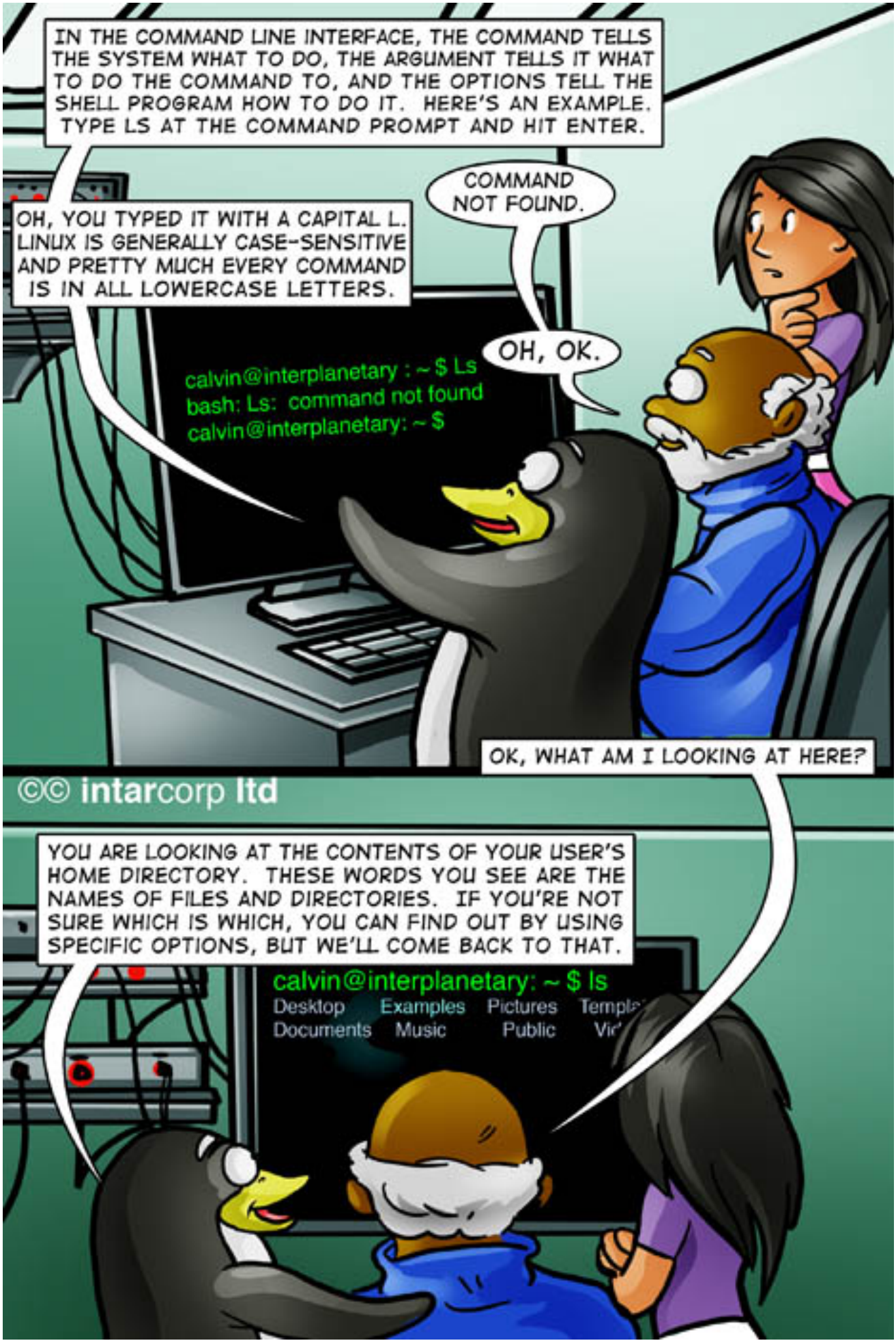

THE CLI IS ACTUALLY A PROGRAM CALLED A SHELL. A SHELL IS JUST A PROGRAM THAT ACCEPTS TEXT COMMANDS: YOU TYPE A COMMAND AT THE PROMPT AND PRESS ENTER. THEN, THE SHELL PROGRAM DOES EXACTLY WHAT THE COMMAND YOU INPUT INSTRUCTED IT TO DO.
HOW DO WE KNOW WHAT TO TYPE? WHAT ARE THE COMMANDS?
YOU ENTER COMMANDS INTO THE SHELL USING SPECIFIC TERMS AND SYNTAX. THERE ARE A VARIETY OF SHELL PROGRAMS, BUT MOST LINUX DISTROS USE BASH.
BASH?
BASH IS THE DEFAULT SHELL ON MOST LINUX-BASED SYSTEMS.
WHAT CAN I DO AT THE COMMAND LINE--- WITH BASH?
ALL KINDS OF THINGS. REMEMBER THE STUFF I SAID ABOUT GNU REPLACING ALL THE UNIX PROGRAMS, AND THAT SOME OF THESE WERE FOR REALLY SIMPLE THINGS SUCH AS DISPLAYING DIRECTORY CONTENTS?
SURE I DO.
MANY OF THOSE GNU PROGRAMS RUN IN TEXT MODE AT THE SHELL.
©© 2009 intarcorp ltd

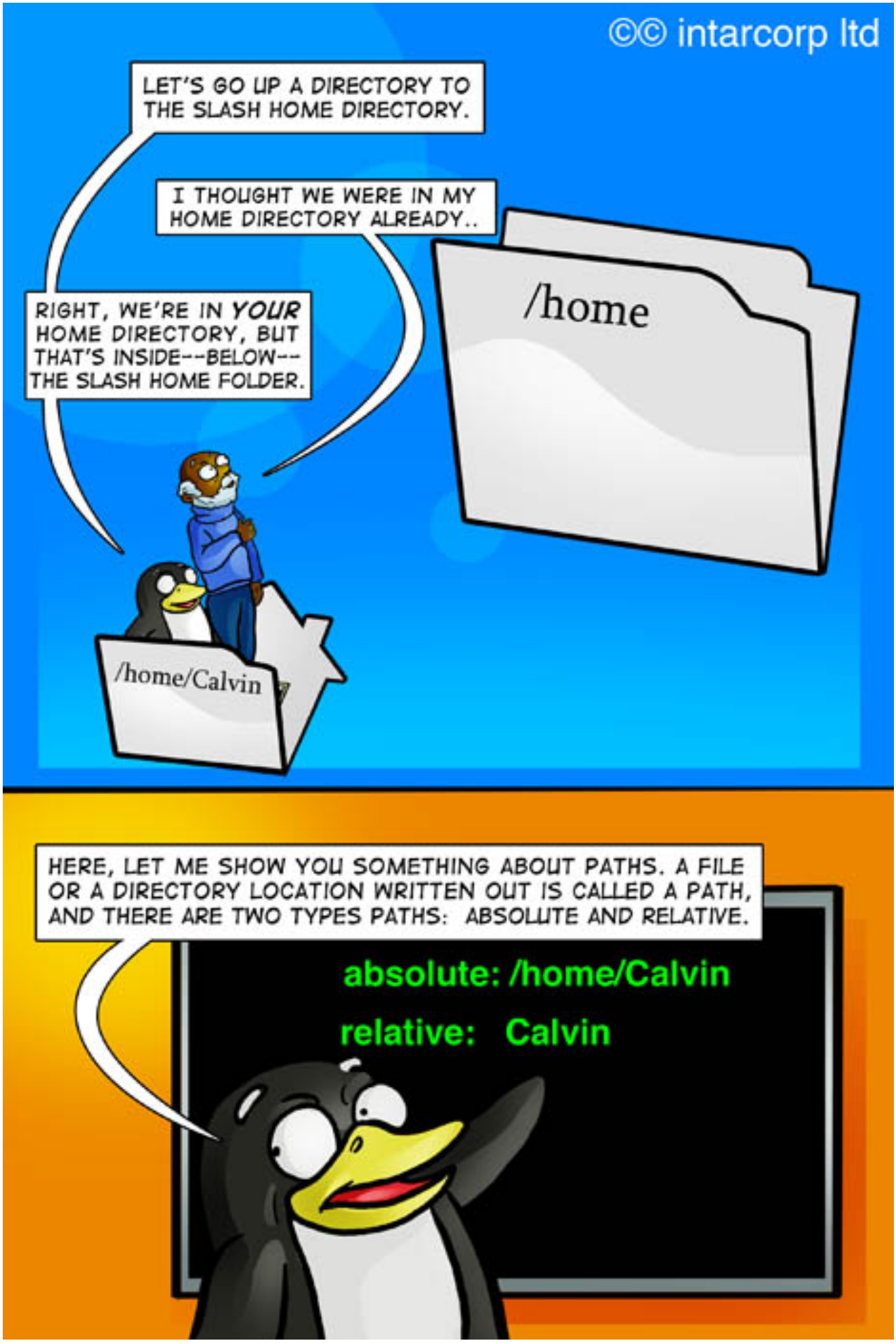

HERE, LET'S TAKE A LOOK. GO TO THE ACCESSORIES MENU UNDER THE APPLICATIONS DROPDOWN AND SELECT TERMINAL.
Accessories
Games
Graphics
Sound & Video
Add/Remove
Calculator
Character Map
Dictionary
Disk Usage Analyser
Take Screenshot
Terminal
Text
WHAT'S THAT?
OH, TERMINAL IS JUST ANOTHER NAME FOR THE COMMAND LINE INTERFACE PROGRAM. IT'S ALSO CALLED THE CONSOLE SOMETIMES.
THE SHELL? LOTS OF NAMES FOR THE SAME THING, HUH?
YEAH, I GUESS IT'S LIKE HOW ESKIMOS HAVE OVER A HUNDRED WORDS FOR SNOW SINCE IT'S SO CENTRAL TO THEIR LIVES.
THAT'S NOT EVEN TRUE, AND ANYWAY, 'ESKIMO' IS NOT THE PREFERRED NOMENCLATURE.
WELL, THE POINT STANDS.
©© intarcorp ltd

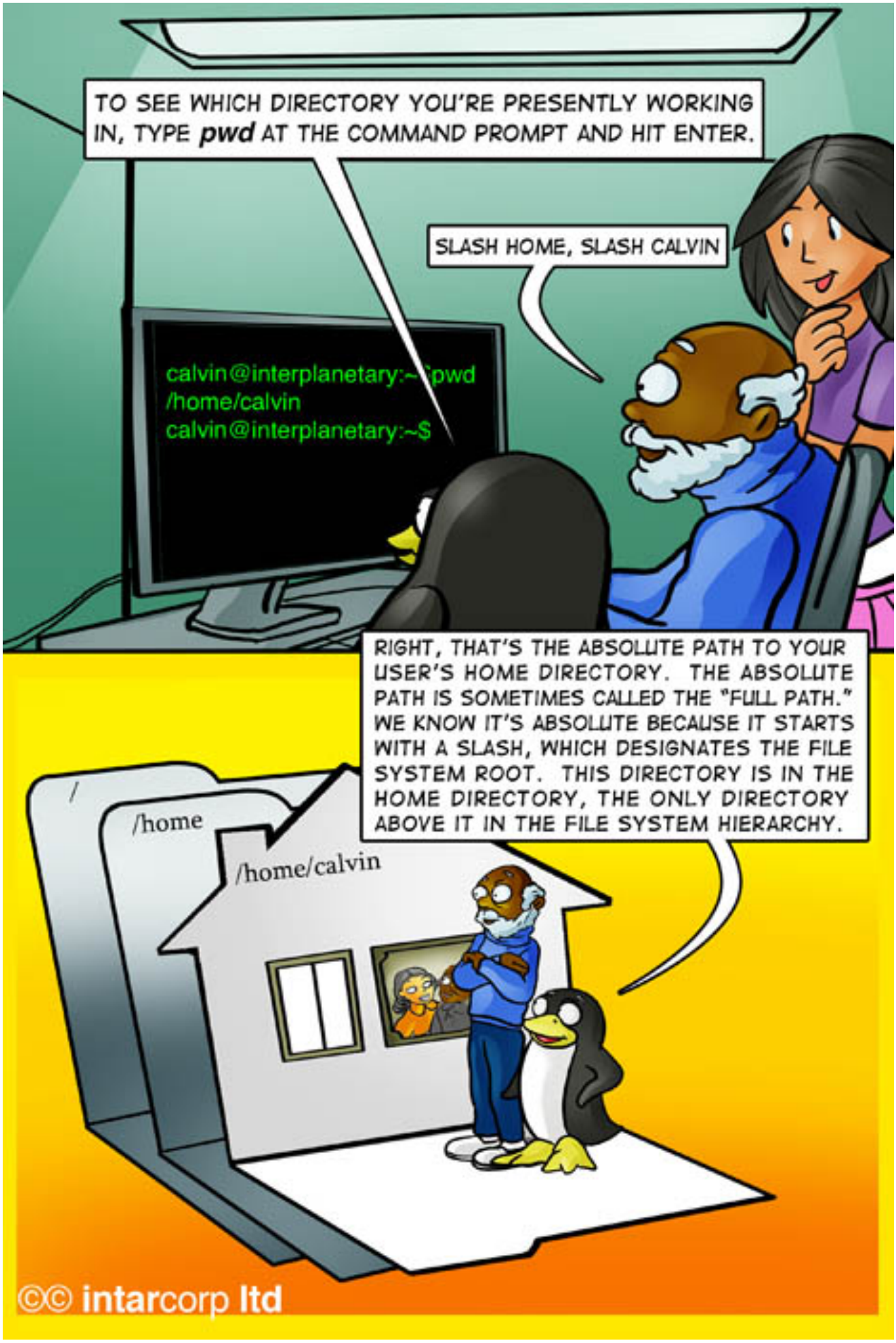

[calvin@interplanetary1 ~] $_
SO ...DOLLAR SIGN... WHAT DO I DO HERE?
BRACE YOURSELF; WE'VE GOT A LOT TO COVER AND NOT A LOT OF TIME.
THAT DOLLAR SIGN IS THE COMMAND PROMPT. THAT'S WHERE YOU TYPE WHAT YOU WANT THE COMPUTER TO DO. WHEN YOU'RE LOGGED IN AS A REGULAR USER, YOU'LL SEE A DOLLAR SIGN, AND WHEN YOU'RE LOGGED IN AS ROOT, YOU WILL SEE A POUND SIGN, OR HASH, INSTEAD.
©© intarcorp ltd
lanetary1 ~] $_
OK, BUT HOW DO I KNOW WHAT TO TYPE?

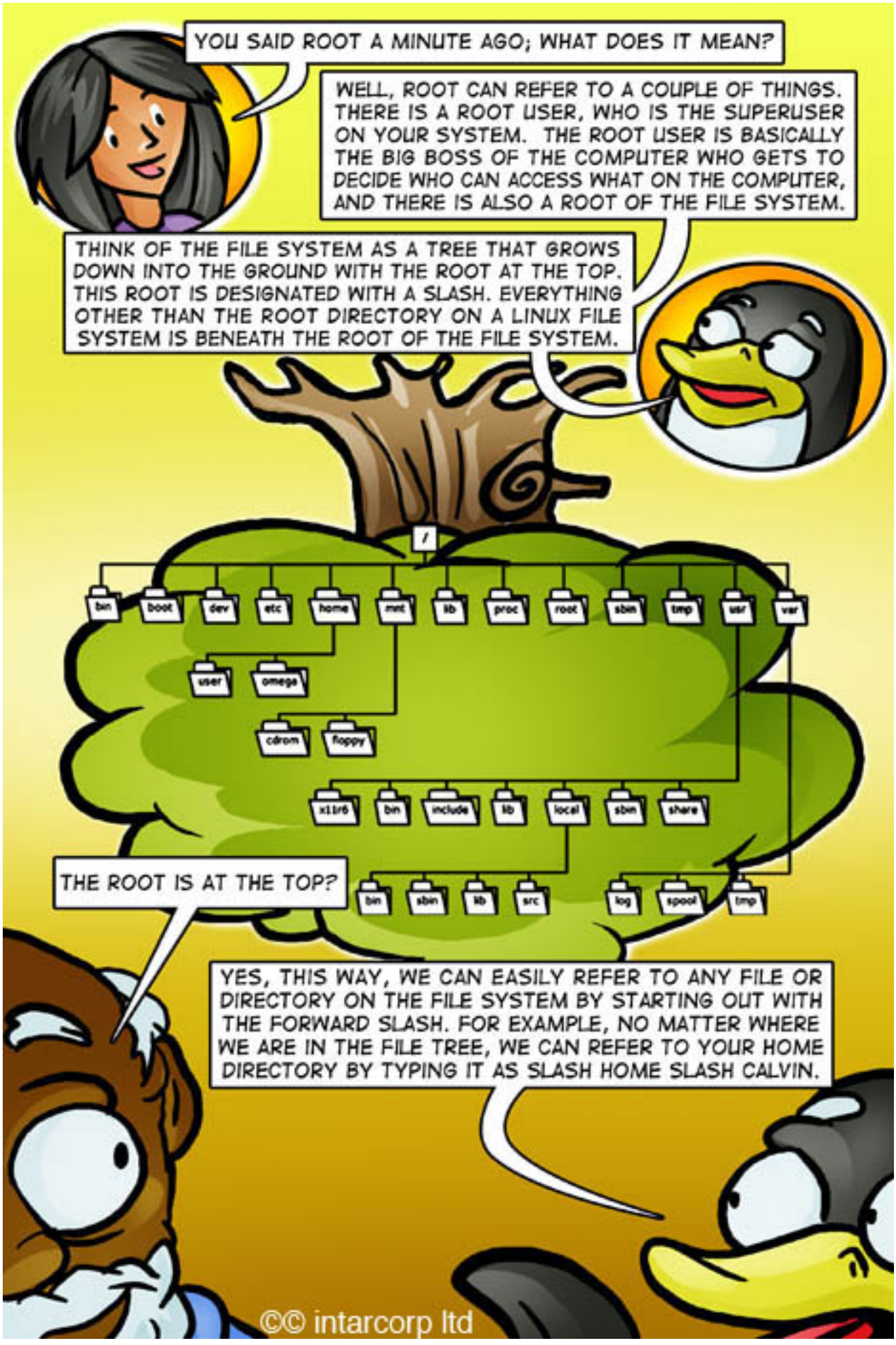

THE SHELL WANTS YOU TO GIVE IT STANDARD INPUT, AND IT WILL GIVE YOU STANDARD OUTPUT IN RETURN.
STANDARD INPUT AND OUTPUT?
©© intarcorp ltd
THAT JUST MEANS IT EXPECTS YOU TO ENTER COMMANDS IN PLAIN TEXT, AND IT WILL GIVE YOU BACK PLAIN TEXT OUTPUT. IN OTHER WORDS, THERE ARE NO GRAPHICS AND YOU JUST USE THE KEYBOARD.
HOW DO I GET INTO THE DRONE?
WELL, YOU SHOULD LEARN SOME FUNDAMENTALS BEFORE YOU GO LOGGING INTO A REMOTE SERVER.
IT'S NOT REMOTE. IT'S RIGHT OUTSIDE.

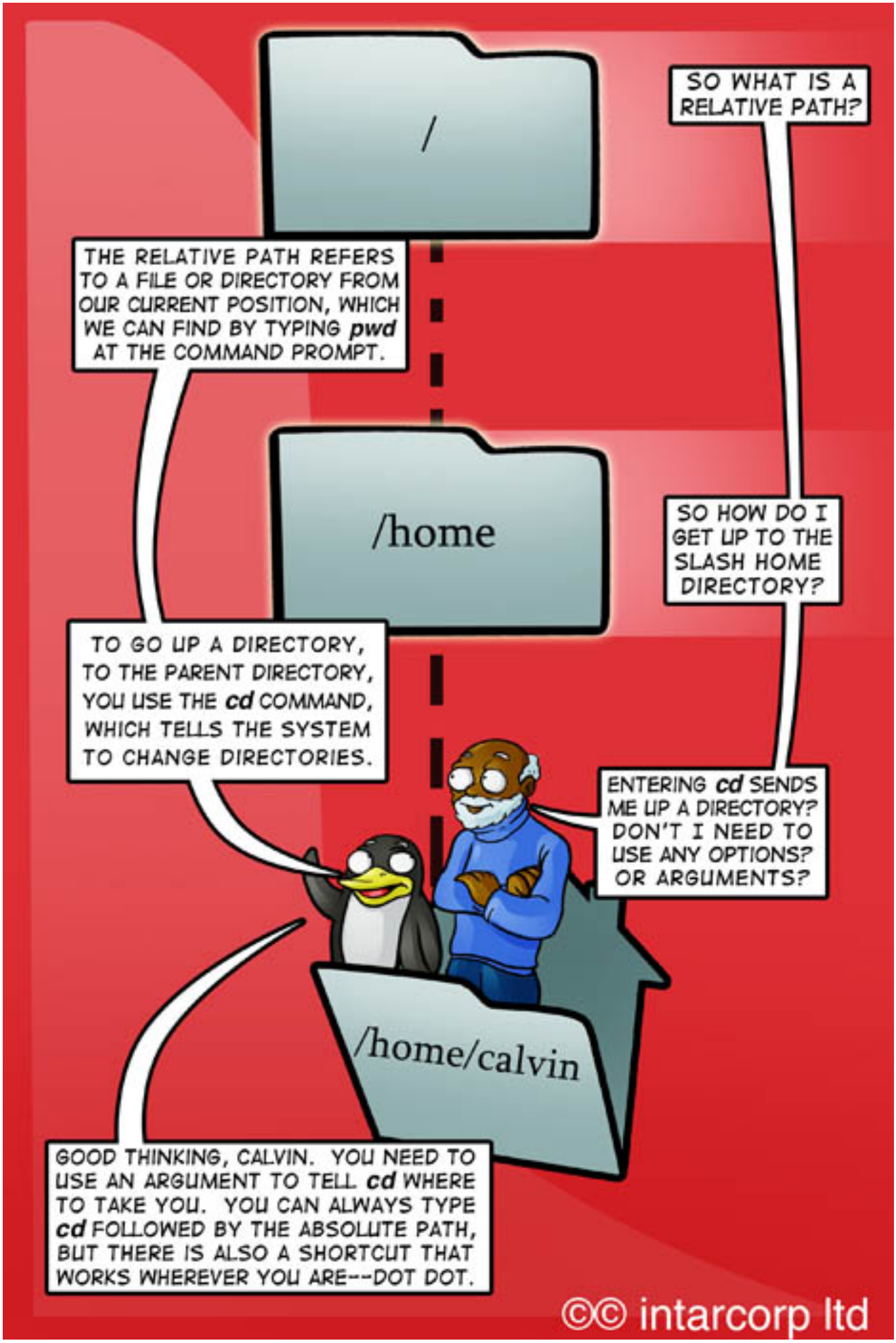

IT'S STILL REMOTE. BASICALLY, ANY TIME YOU'RE LOGGED INTO A SYSTEM WITHOUT USING ITS OWN KEYBOARD TO CONTROL IT, YOU'RE ON A REMOTE SYSTEM. BUT LIKE I SAID, WE NEED TO COVER SOME BASICS.
IN THE SHELL, YOU ENTER COMMANDS AT THE COMMAND PROMPT USING BASH SYNTAX. OFTEN, COMMANDS REQUIRE ADDITIONAL INFORMATION IN THE FORM OF OPTIONS AND ARGUMENTS.
remote
remote
local
©© intarcorp ltd
THAT'S EASY! I ARGUE WITH MY COMPUTER ALL THE TIME!
OHH CALVIN, SOMETIMES YOU'RE SO FUNNY I FORGET TO LAUGH.
THE ARGUMENTS I'M TALKING ABOUT HERE ARE A LITTLE BIT DIFFERENT.

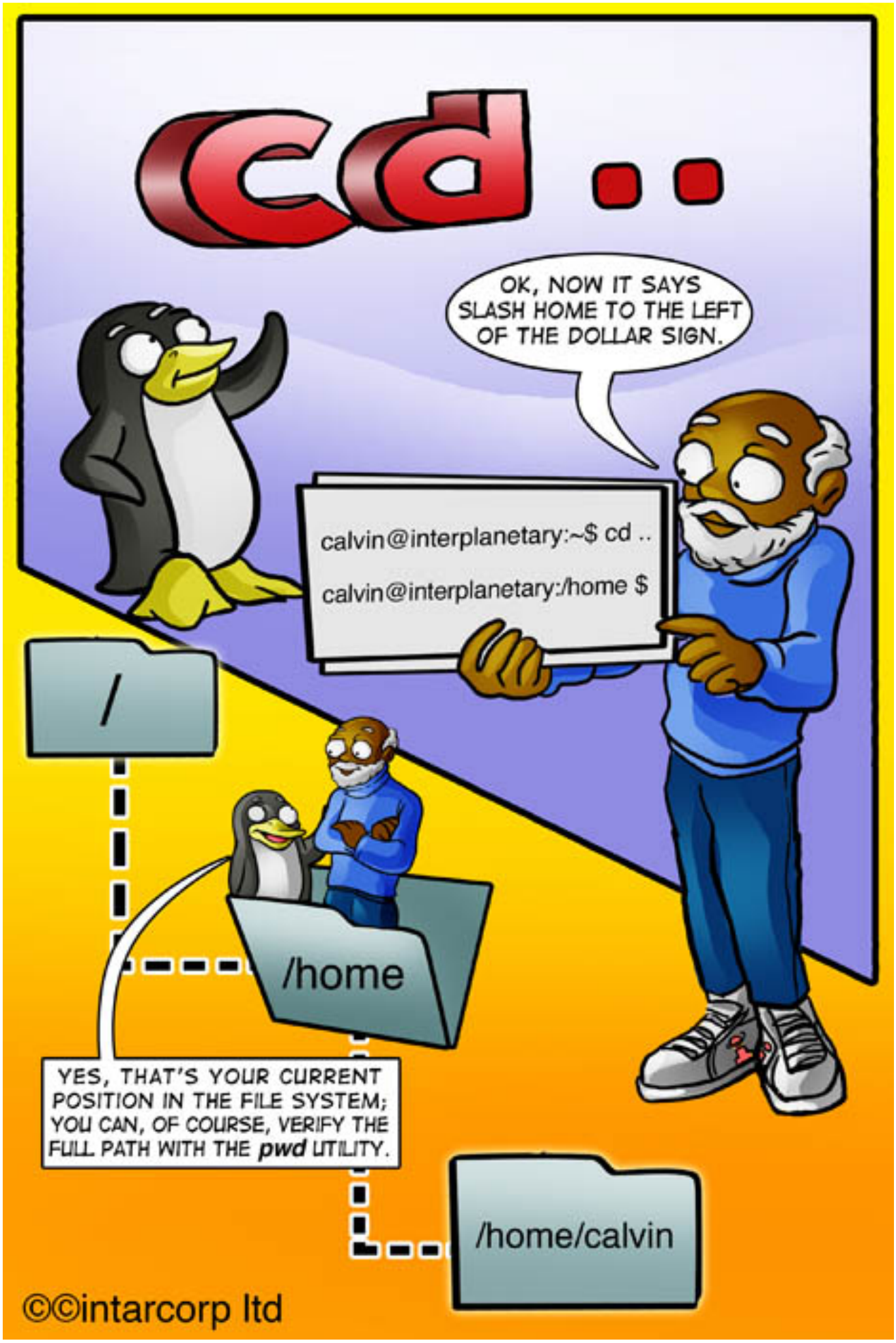

IN THE COMMAND LINE INTERFACE, THE COMMAND TELLS THE SYSTEM WHAT TO DO, THE ARGUMENT TELLS IT WHAT TO DO THE COMMAND TO, AND THE OPTIONS TELL THE SHELL PROGRAM HOW TO DO IT. HERE'S AN EXAMPLE. TYPE LS AT THE COMMAND PROMPT AND HIT ENTER.
OH, YOU TYPED IT WITH A CAPITAL L. LINUX IS GENERALLY CASE-SENSITIVE AND PRETTY MUCH EVERY COMMAND IS IN ALL LOWERCASE LETTERS.
COMMAND NOT FOUND.
OH, OK.
calvin@interplanetary : ~ $ Ls
bash: Ls: command not found
calvin@interplanetary: ~ $
OK, WHAT AM I LOOKING AT HERE?
©© intarcorp ltd
YOU ARE LOOKING AT THE CONTENTS OF YOUR USER'S HOME DIRECTORY. THESE WORDS YOU SEE ARE THE NAMES OF FILES AND DIRECTORIES. IF YOU'RE NOT SURE WHICH IS WHICH, YOU CAN FIND OUT BY USING SPECIFIC OPTIONS, BUT WE'LL COME BACK TO THAT.
calvin@interplanetary: ~ $ ls
Desktop Examples Pictures
Documents Music Public

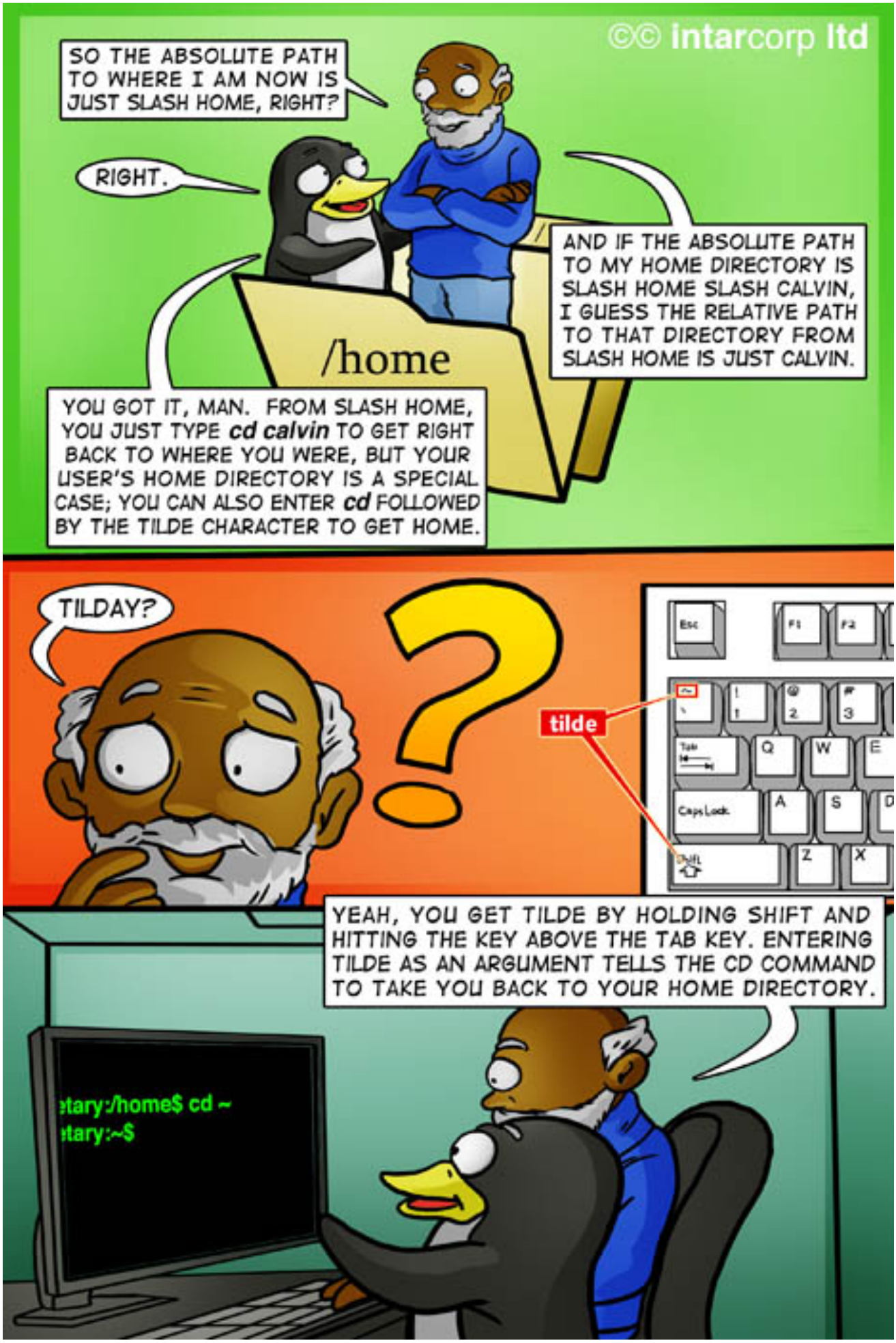

©© intarcorp ltd
LET'S GO UP A DIRECTORY TO THE SLASH HOME DIRECTORY.
I THOUGHT WE WERE IN MY HOME DIRECTORY ALREADY..
RIGHT, WE'RE IN YOUR HOME DIRECTORY, BUT THAT'S INSIDE--BELOW-- THE SLASH HOME FOLDER.
/home
/home/Calvin
HERE, LET ME SHOW YOU SOMETHING ABOUT PATHS. A FILE OR A DIRECTORY LOCATION WRITTEN OUT IS CALLED A PATH, AND THERE ARE TWO TYPES PATHS: ABSOLUTE AND RELATIVE.
absolute: /home/Calvin
relative: Calvin

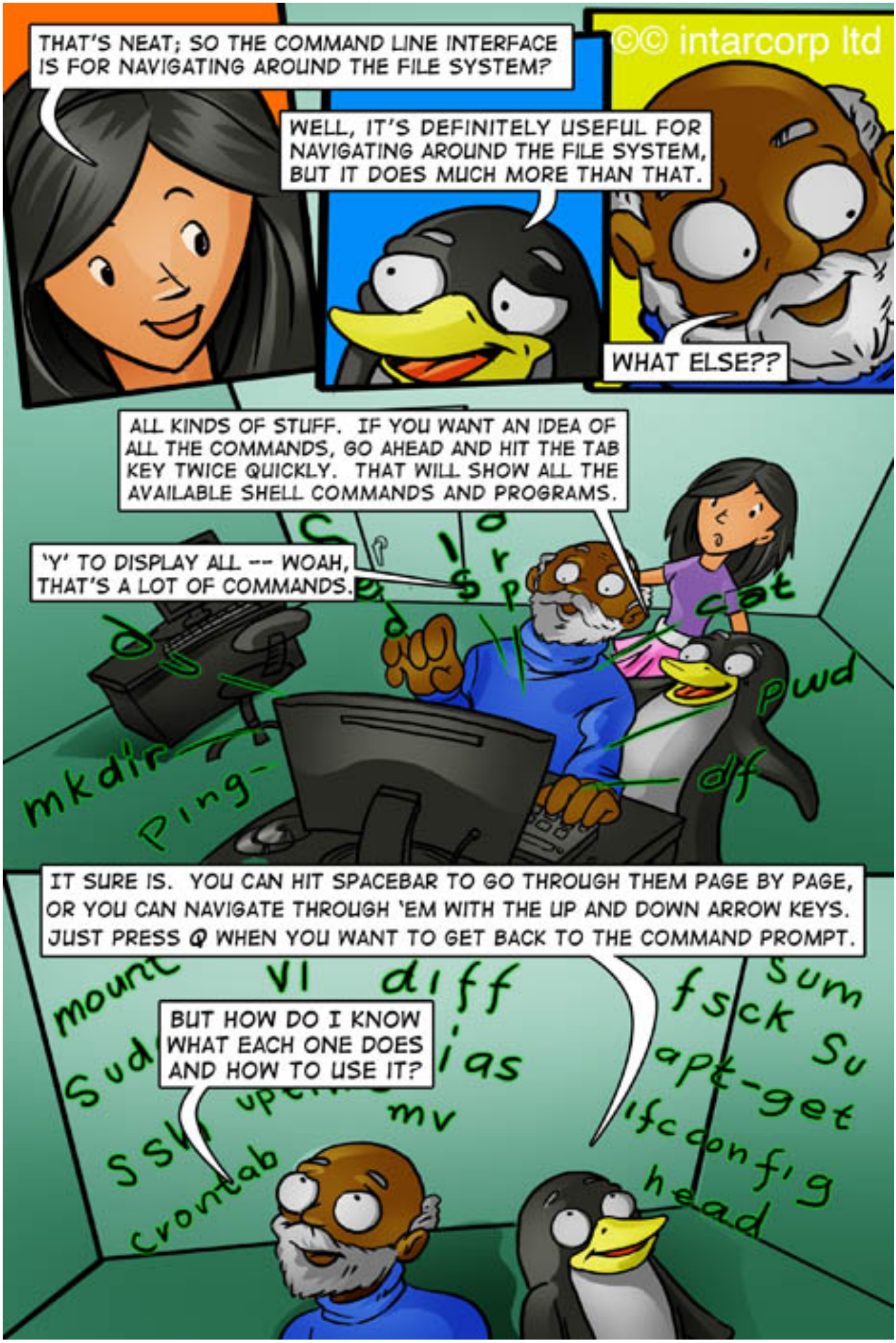

TO SEE WHICH DIRECTORY YOU'RE PRESENTLY WORKING IN, TYPE pwd AT THE COMMAND PROMPT AND HIT ENTER.
SLASH HOME, SLASH CALVIN
calvin@interplanetary:~$pwd
/home/calvin
calvin@interplanetary:~$
RIGHT, THAT'S THE ABSOLUTE PATH TO YOUR USER'S HOME DIRECTORY. THE ABSOLUTE PATH IS SOMETIMES CALLED THE "FULL PATH." WE KNOW IT'S ABSOLUTE BECAUSE IT STARTS WITH A SLASH, WHICH DESIGNATES THE FILE SYSTEM ROOT. THIS DIRECTORY IS IN THE HOME DIRECTORY, THE ONLY DIRECTORY ABOVE IT IN THE FILE SYSTEM HIERARCHY.
/
/home
/home/calvin
©© intarcorp ltd

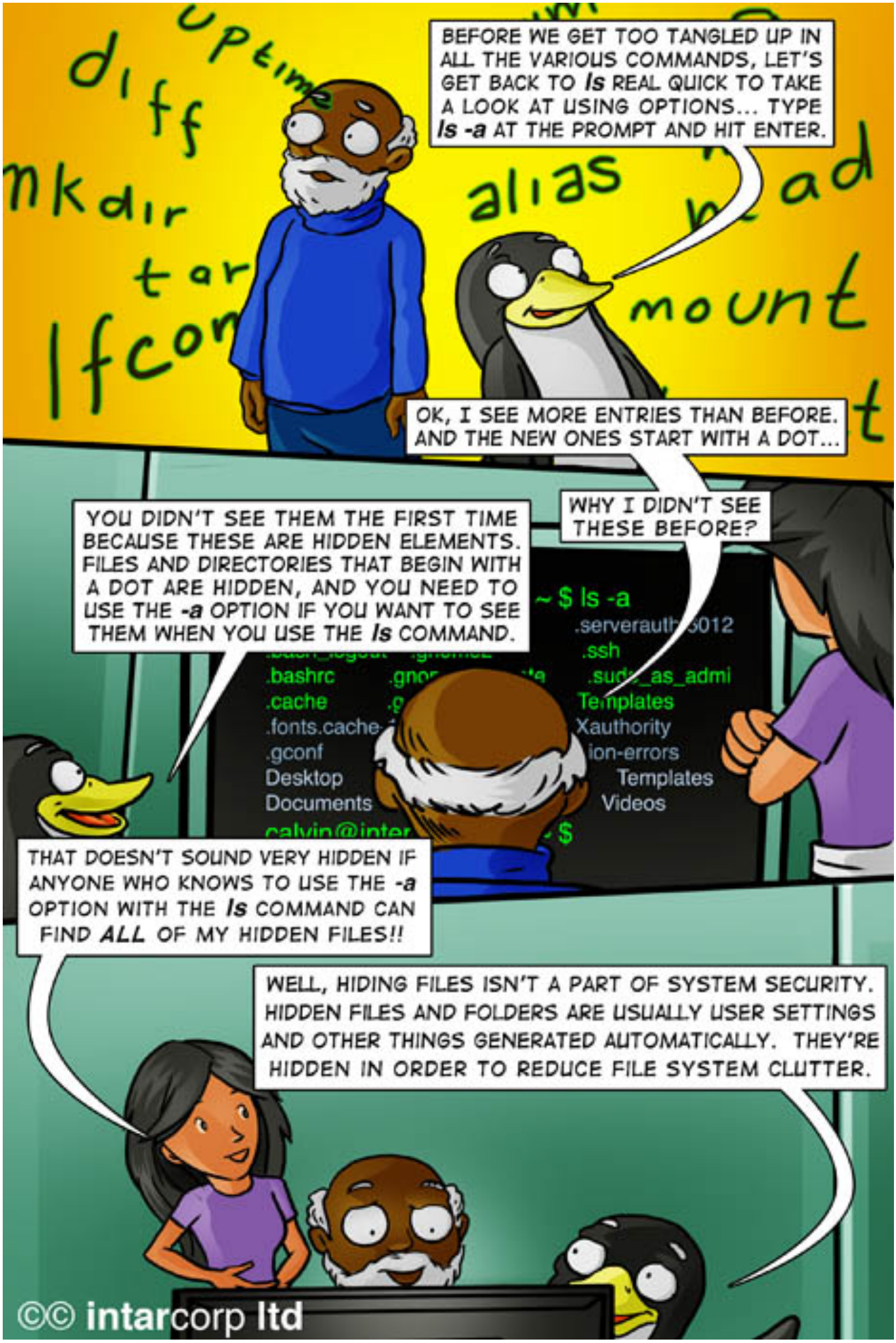

YOU SAID ROOT A MINUTE AGO; WHAT DOES IT MEAN?
WELL, ROOT CAN REFER TO A COUPLE OF THINGS. THERE IS A ROOT USER, WHO IS THE SUPERUSER ON YOUR SYSTEM. THE ROOT USER IS BASICALLY THE BIG BOSS OF THE COMPUTER WHO GETS TO DECIDE WHO CAN ACCESS WHAT ON THE COMPUTER, AND THERE IS ALSO A ROOT OF THE FILE SYSTEM.
THINK OF THE FILE SYSTEM AS A TREE THAT GROWS DOWN INTO THE GROUND WITH THE ROOT AT THE TOP. THIS ROOT IS DESIGNATED WITH A SLASH. EVERYTHING OTHER THAN THE ROOT DIRECTORY ON A LINUX FILE SYSTEM IS BENEATH THE ROOT OF THE FILE SYSTEM.
/
bin
boot
dev
etc
home
mnt
lib
proc
root
sbin
tmp
usr
var
user
omega
cdrom
floppy
X11R6
bin
include
lib
local
sbin
share
bin
sbin
lib
src
log
spool
tmp
THE ROOT IS AT THE TOP?
YES, THIS WAY, WE CAN EASILY REFER TO ANY FILE OR DIRECTORY ON THE FILE SYSTEM BY STARTING OUT WITH THE FORWARD SLASH. FOR EXAMPLE, NO MATTER WHERE WE ARE IN THE FILE TREE, WE CAN REFER TO YOUR HOME DIRECTORY BY TYPING IT AS SLASH HOME SLASH CALVIN.
©© intarcorp ltd


/
SO WHAT IS A RELATIVE PATH?
THE RELATIVE PATH REFERS TO A FILE OR DIRECTORY FROM OUR CURRENT POSITION, WHICH WE CAN FIND BY TYPING pwd AT THE COMMAND PROMPT.
/home
SO HOW DO I GET UP TO THE SLASH HOME DIRECTORY?
TO GO UP A DIRECTORY, TO THE PARENT DIRECTORY, YOU USE THE cd COMMAND, WHICH TELLS THE SYSTEM TO CHANGE DIRECTORIES.
ENTERING cd SENDS ME UP A DIRECTORY? DON'T I NEED TO USE ANY OPTIONS? OR ARGUMENTS?
/home/calvin
GOOD THINKING, CALVIN. YOU NEED TO USE AN ARGUMENT TO TELL cd WHERE TO TAKE YOU. YOU CAN ALWAYS TYPE cd FOLLOWED BY THE ABSOLUTE PATH, BUT THERE IS ALSO A SHORTCUT THAT WORKS WHEREVER YOU ARE--DOT DOT.
©© intarcorp ltd

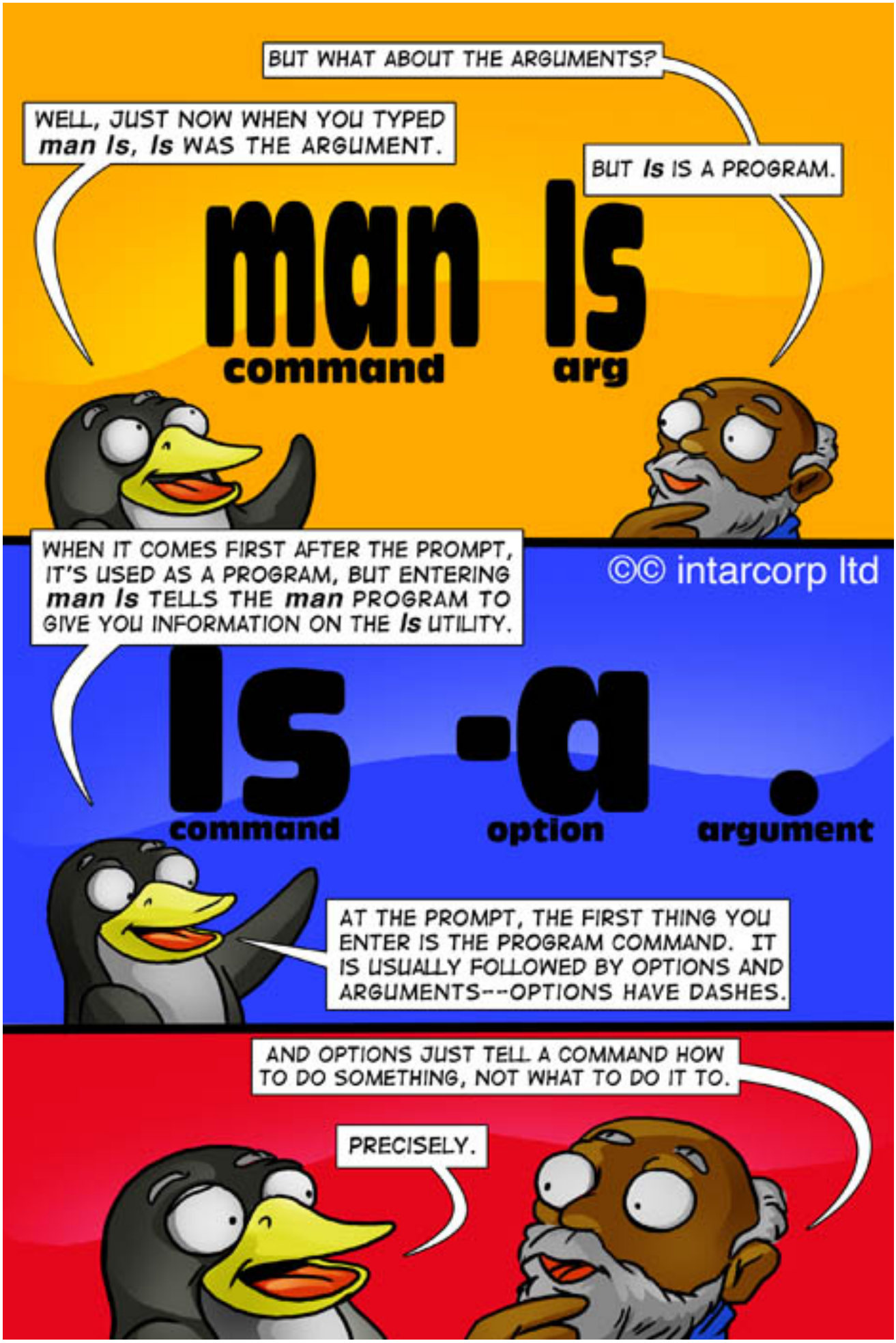

cd ..
OK, NOW IT SAYS SLASH HOME TO THE LEFT OF THE DOLLAR SIGN.
calvin@interplanetary:~$ cd ..
calvin@interplanetary:/home $
/
/home
YES, THAT'S YOUR CURRENT POSITION IN THE FILE SYSTEM; YOU CAN, OF COURSE, VERIFY THE FULL PATH WITH THE pwd UTILITY.
/home/calvin
©©intarcorp ltd

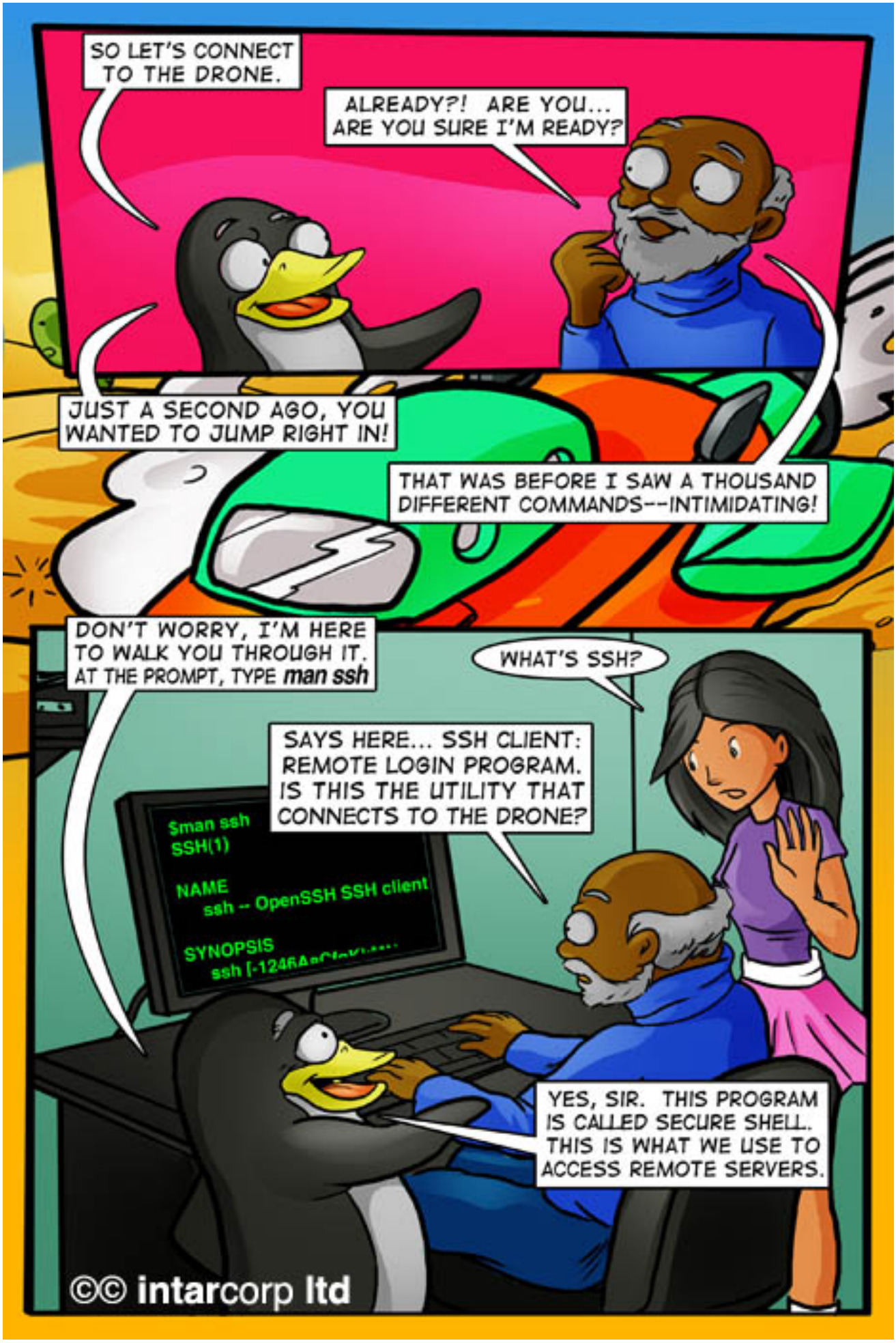

©© intarcorp ltd
SO THE ABSOLUTE PATH TO WHERE I AM NOW IS JUST SLASH HOME, RIGHT?
RIGHT.
AND IF THE ABSOLUTE PATH TO MY HOME DIRECTORY IS SLASH HOME SLASH CALVIN, I GUESS THE RELATIVE PATH TO THAT DIRECTORY FROM SLASH HOME IS JUST CALVIN.
/home
YOU GOT IT, MAN. FROM SLASH HOME, YOU JUST TYPE cd calvin TO GET RIGHT BACK TO WHERE YOU WERE, BUT YOUR USER'S HOME DIRECTORY IS A SPECIAL CASE; YOU CAN ALSO ENTER cd FOLLOWED BY THE TILDE CHARACTER TO GET HOME.
TILDAY?
tilde
YEAH, YOU GET TILDE BY HOLDING SHIFT AND HITTING THE KEY ABOVE THE TAB KEY. ENTERING TILDE AS AN ARGUMENT TELLS THE CD COMMAND TO TAKE YOU BACK TO YOUR HOME DIRECTORY.
tary:/home$ cd ~
tary:~$

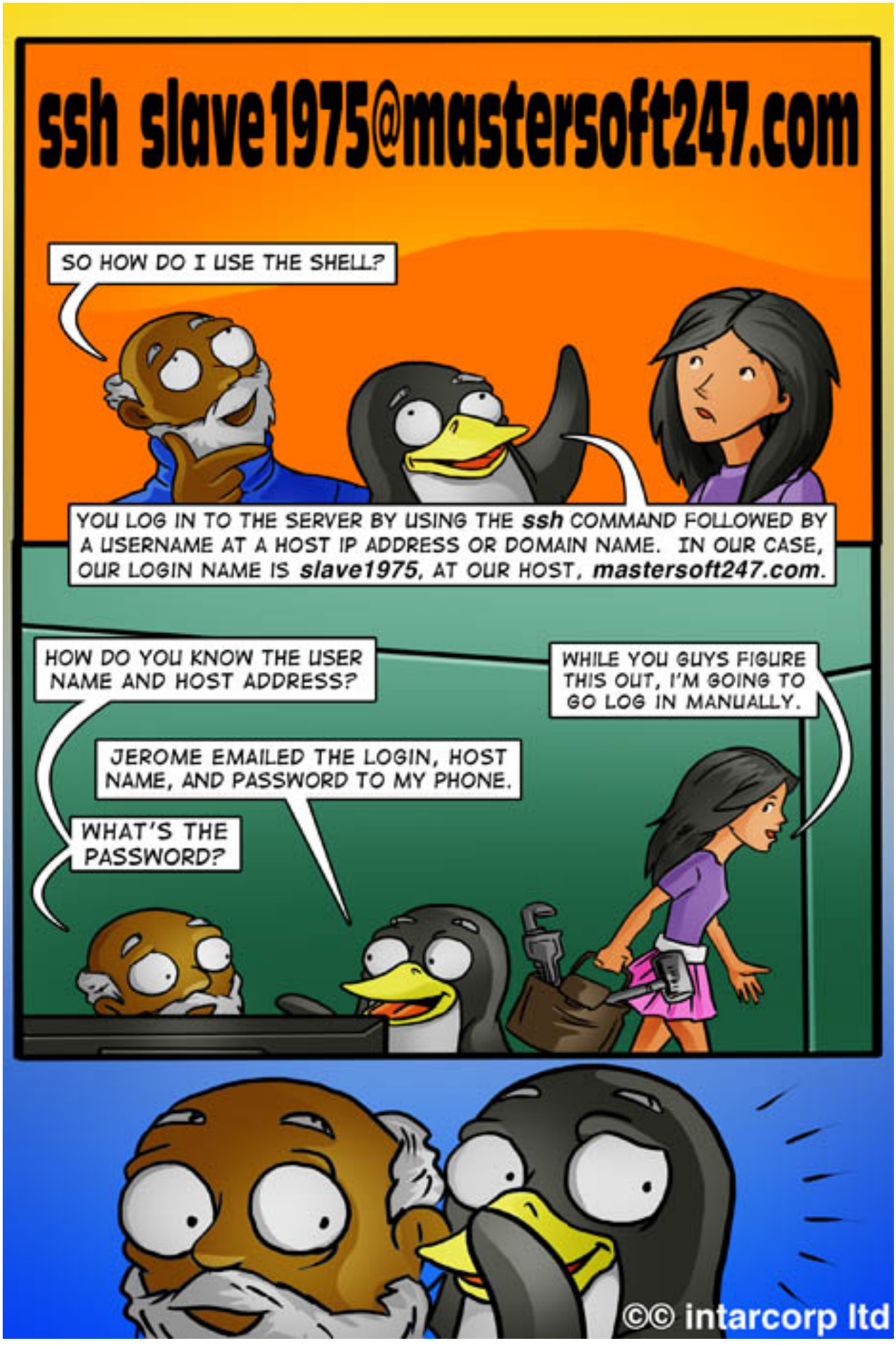

THAT'S NEAT; SO THE COMMAND LINE INTERFACE IS FOR NAVIGATING AROUND THE FILE SYSTEM?
WELL, IT'S DEFINITELY USEFUL FOR NAVIGATING AROUND THE FILE SYSTEM, BUT IT DOES MUCH MORE THAN THAT.
© intarcorp ltd
WHAT ELSE??
ALL KINDS OF STUFF. IF YOU WANT AN IDEA OF ALL THE COMMANDS, GO AHEAD AND HIT THE TAB KEY TWICE QUICKLY. THAT WILL SHOW ALL THE AVAILABLE SHELL COMMANDS AND PROGRAMS.
'Y' TO DISPLAY ALL -- WOAH, THAT'S A LOT OF COMMANDS.
cat
pwd
mkdir
Ping
df
IT SURE IS. YOU CAN HIT SPACEBAR TO GO THROUGH THEM PAGE BY PAGE, OR YOU CAN NAVIGATE THROUGH 'EM WITH THE UP AND DOWN ARROW KEYS. JUST PRESS Q WHEN YOU WANT TO GET BACK TO THE COMMAND PROMPT.
BUT HOW DO I KNOW WHAT EACH ONE DOES AND HOW TO USE IT?
mount
vi
diff
fsck
Sum
apt-get
ifconfig
head
mv
Crontab

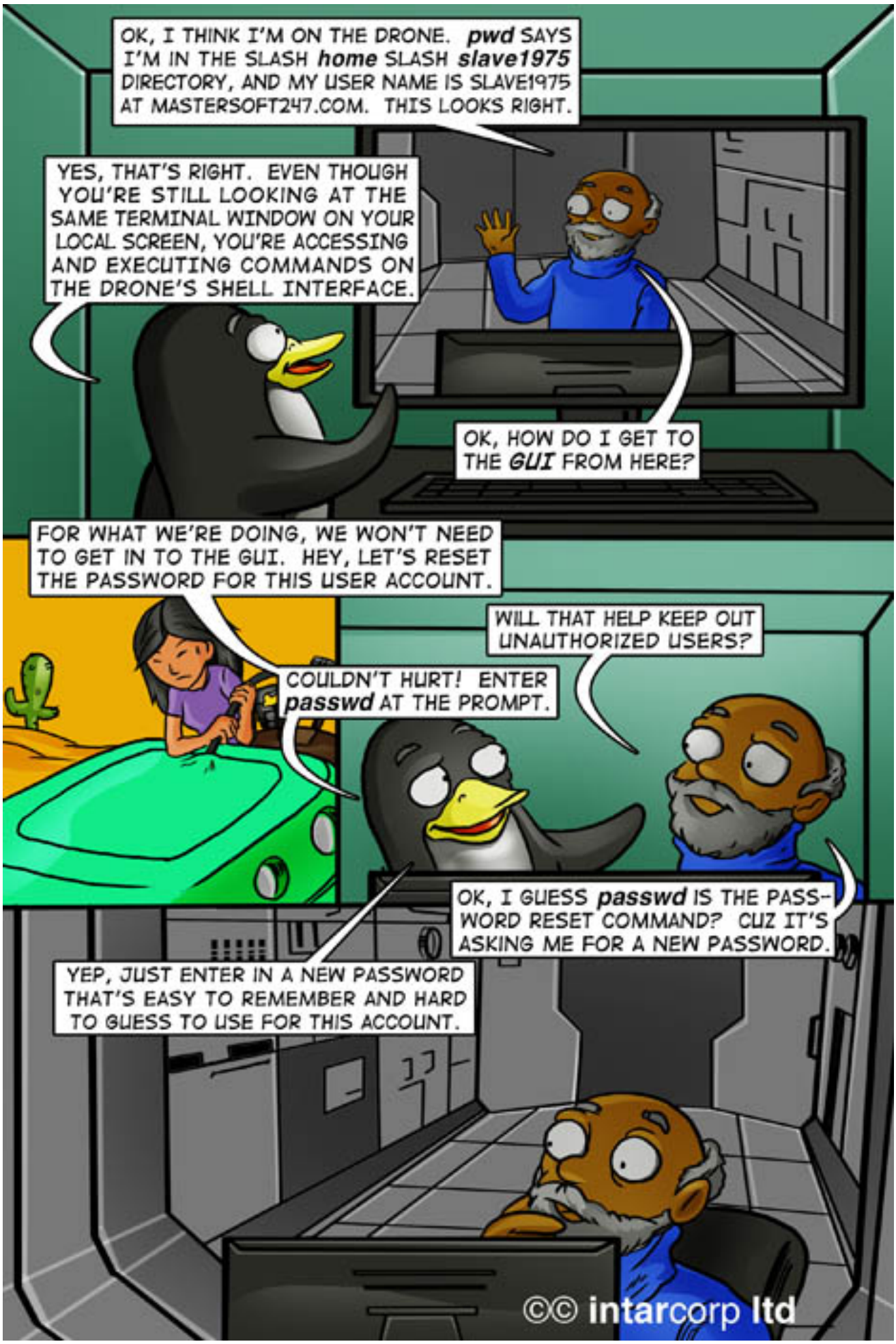

BEFORE WE GET TOO TANGLED UP IN ALL THE VARIOUS COMMANDS, LET'S GET BACK TO ls REAL QUICK TO TAKE A LOOK AT USING OPTIONS... TYPE ls -a AT THE PROMPT AND HIT ENTER.
OK, I SEE MORE ENTRIES THAN BEFORE. AND THE NEW ONES START WITH A DOT...
WHY I DIDN'T SEE THESE BEFORE?
YOU DIDN'T SEE THEM THE FIRST TIME BECAUSE THESE ARE HIDDEN ELEMENTS. FILES AND DIRECTORIES THAT BEGIN WITH A DOT ARE HIDDEN, AND YOU NEED TO USE THE -a OPTION IF YOU WANT TO SEE THEM WHEN YOU USE THE ls COMMAND.
~ $ ls -a
.ssh
.bashrc
.cache
.fonts.cache
.gconf
Desktop
Documents
Templates
Xauthority
Templates
Videos
THAT DOESN'T SOUND VERY HIDDEN IF ANYONE WHO KNOWS TO USE THE -a OPTION WITH THE ls COMMAND CAN FIND ALL OF MY HIDDEN FILES!!
WELL, HIDING FILES ISN'T A PART OF SYSTEM SECURITY. HIDDEN FILES AND FOLDERS ARE USUALLY USER SETTINGS AND OTHER THINGS GENERATED AUTOMATICALLY. THEY'RE HIDDEN IN ORDER TO REDUCE FILE SYSTEM CLUTTER.
©© intarcorp ltd


OK, I UNDERSTAND. SO THE -a OPTION TELLS THE SYSTEM TO SHOW EVERYTHING, INCLUDING HIDDEN FILES AND DIRECTORIES?
-a
©© intarcorp ltd
YES. WELL, SORTA. WITH THE ls COMMAND, THE -a OPTION WILL INCLUDE HIDDEN FILES IN THE DIRECTORY, BUT DIFFERENT OPTIONS DO DIFFERENT THINGS WITH DIFFERENT COMMANDS.
THEN HOW WILL I KNOW WHICH OPTIONS TO USE?
OPTIONS
LUCKY FOR YOU, THERE'S A COMMAND LINE MANUAL PROGRAM YOU CAN USE CALLED "MAN." TYPE man ls AND PRESS ENTER.
INTERESTING. SO THESE ARE THE OPTIONS FOR THE ls PROGRAM. AND EACH OF THESE OPTIONS DOES SOMETHING DIFFERENT, HUH?
YEP, THE OPTION STARTS WITH A DASH, AND TO THE RIGHT OF EACH OPTION IS ITS DEFINITION.
NAME
SYNOPS
DESCRI
List nformation about the FILEs (the directory by fault).
Sort ntries alphabetically if none o nor --s t.
Mandato arguments to long options for short options
-a, --all
do not igno rting wi
-A --almost-
do not list

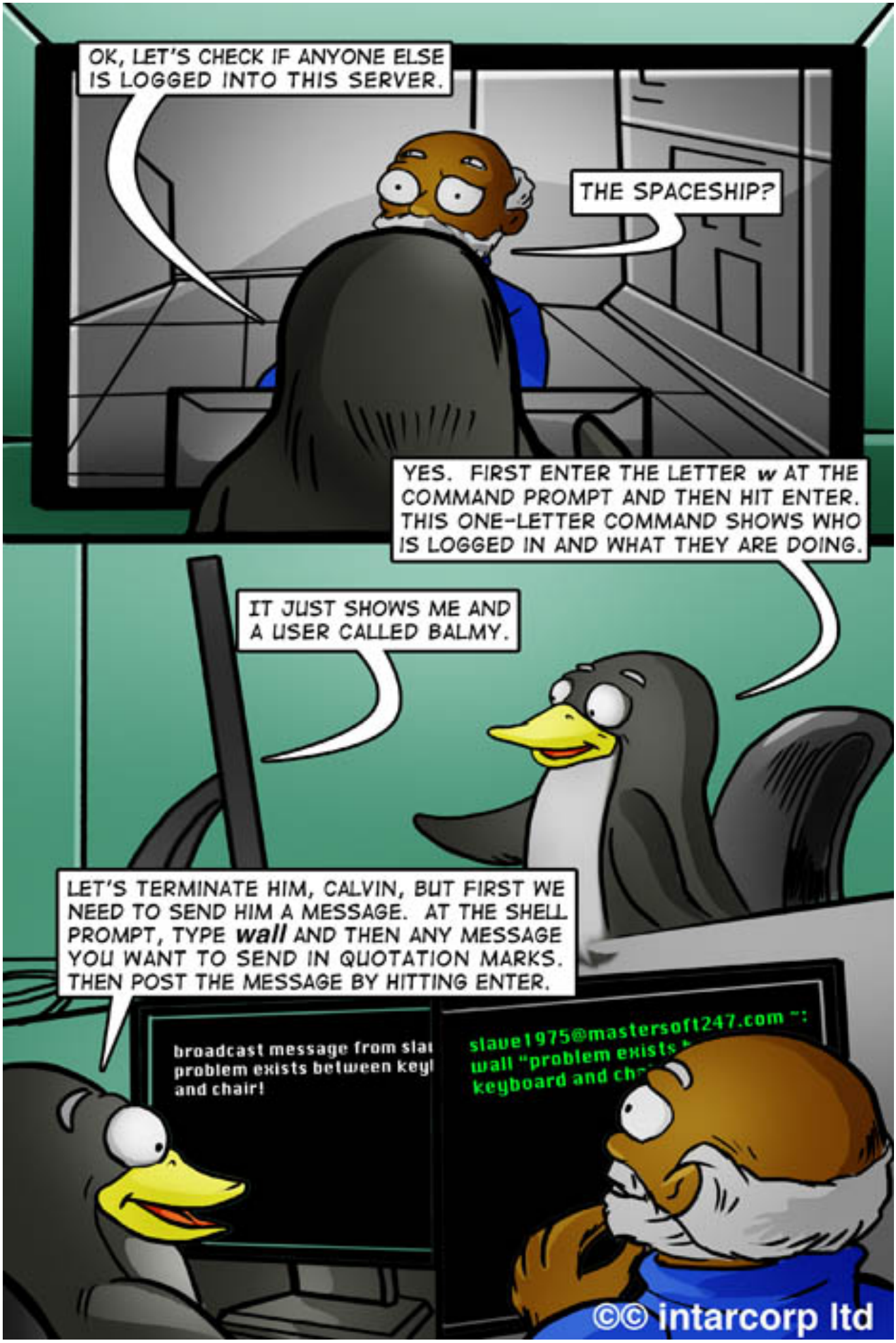

BUT WHAT ABOUT THE ARGUMENTS?
WELL, JUST NOW WHEN YOU TYPED man ls, ls WAS THE ARGUMENT.
BUT ls IS A PROGRAM.
man ls
command
arg
WHEN IT COMES FIRST AFTER THE PROMPT, IT'S USED AS A PROGRAM, BUT ENTERING man ls TELLS THE man PROGRAM TO GIVE YOU INFORMATION ON THE ls UTILITY.
©© intarcorp ltd
ls -a .
command
option
argument
AT THE PROMPT, THE FIRST THING YOU ENTER IS THE PROGRAM COMMAND. IT IS USUALLY FOLLOWED BY OPTIONS AND ARGUMENTS--OPTIONS HAVE DASHES.
AND OPTIONS JUST TELL A COMMAND HOW TO DO SOMETHING, NOT WHAT TO DO IT TO.
PRECISELY.

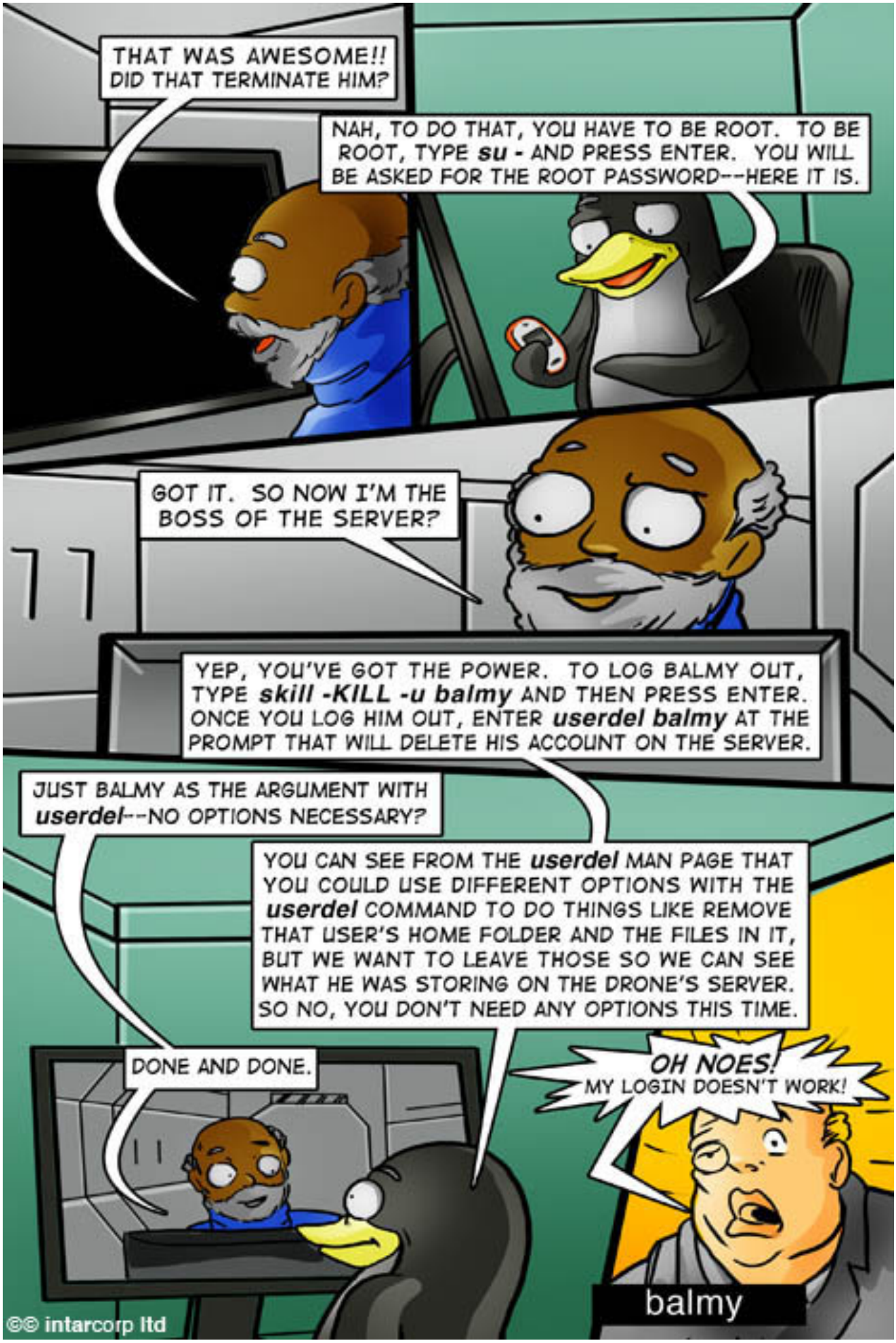

SO LET'S CONNECT TO THE DRONE.
ALREADY?! ARE YOU... ARE YOU SURE I'M READY?
JUST A SECOND AGO, YOU WANTED TO JUMP RIGHT IN!
THAT WAS BEFORE I SAW A THOUSAND DIFFERENT COMMANDS--INTIMIDATING!
DON'T WORRY, I'M HERE TO WALK YOU THROUGH IT. AT THE PROMPT, TYPE man ssh
WHAT'S SSH?
SAYS HERE... SSH CLIENT: REMOTE LOGIN PROGRAM. IS THIS THE UTILITY THAT CONNECTS TO THE DRONE?
$man ssh
SSH(1)
NAME
ssh -- OpenSSH SSH client
SYNOPSIS
YES, SIR. THIS PROGRAM IS CALLED SECURE SHELL. THIS IS WHAT WE USE TO ACCESS REMOTE SERVERS.
©© intarcorp ltd

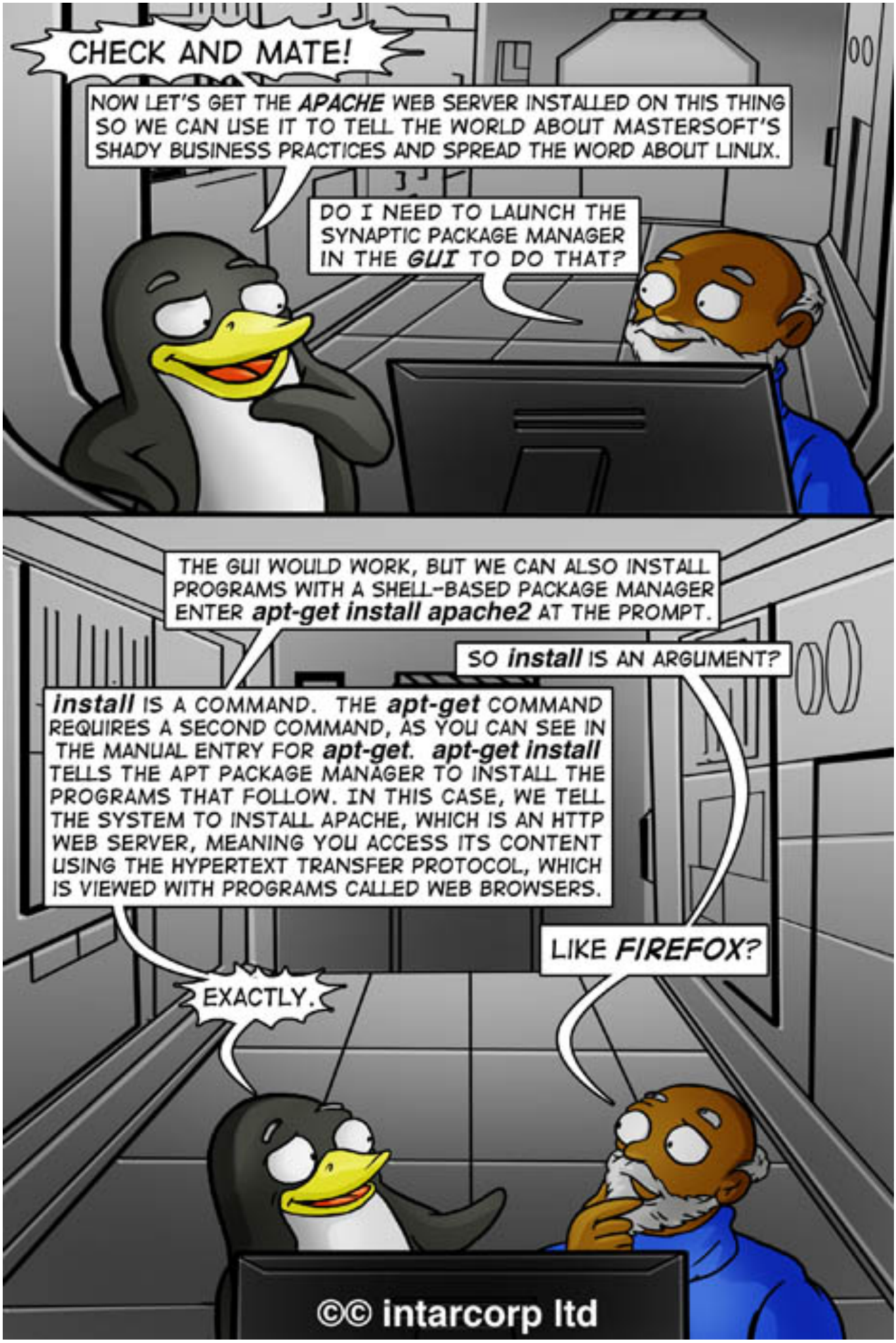

ssh slave1975@mastersoft247.com
SO HOW DO I USE THE SHELL?
YOU LOG IN TO THE SERVER BY USING THE ssh COMMAND FOLLOWED BY A USERNAME AT A HOST IP ADDRESS OR DOMAIN NAME. IN OUR CASE, OUR LOGIN NAME IS slave1975, AT OUR HOST, mastersoft247.com.
HOW DO YOU KNOW THE USER NAME AND HOST ADDRESS?
JEROME EMAILED THE LOGIN, HOST NAME, AND PASSWORD TO MY PHONE.
WHAT'S THE PASSWORD?
WHILE YOU GUYS FIGURE THIS OUT, I'M GOING TO GO LOG IN MANUALLY.
©© intarcorp ltd

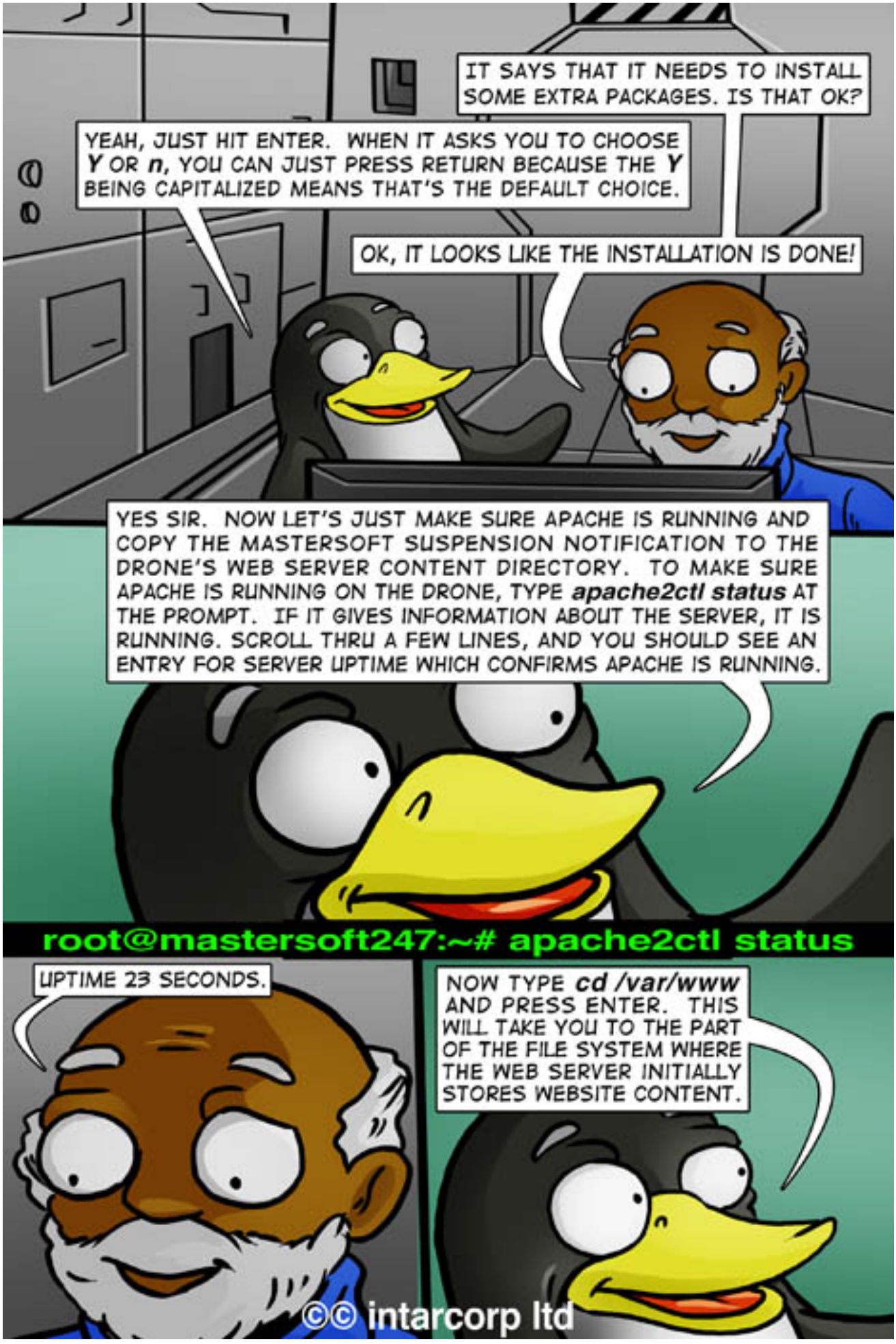

OK, I THINK I'M ON THE DRONE. pwd SAYS I'M IN THE SLASH home SLASH slave1975 DIRECTORY, AND MY USER NAME IS SLAVE1975 AT MASTERSOFT247.COM. THIS LOOKS RIGHT.
YES, THAT'S RIGHT. EVEN THOUGH YOU'RE STILL LOOKING AT THE SAME TERMINAL WINDOW ON YOUR LOCAL SCREEN, YOU'RE ACCESSING AND EXECUTING COMMANDS ON THE DRONE'S SHELL INTERFACE.
OK, HOW DO I GET TO THE GUI FROM HERE?
FOR WHAT WE'RE DOING, WE WON'T NEED TO GET IN TO THE GUI. HEY, LET'S RESET THE PASSWORD FOR THIS USER ACCOUNT.
WILL THAT HELP KEEP OUT UNAUTHORIZED USERS?
COULDN'T HURT! ENTER passwd AT THE PROMPT.
OK, I GUESS passwd IS THE PASS-WORD RESET COMMAND? CUZ IT'S ASKING ME FOR A NEW PASSWORD.
YEP, JUST ENTER IN A NEW PASSWORD THAT'S EASY TO REMEMBER AND HARD TO GUESS TO USE FOR THIS ACCOUNT.
©© intarcorp ltd

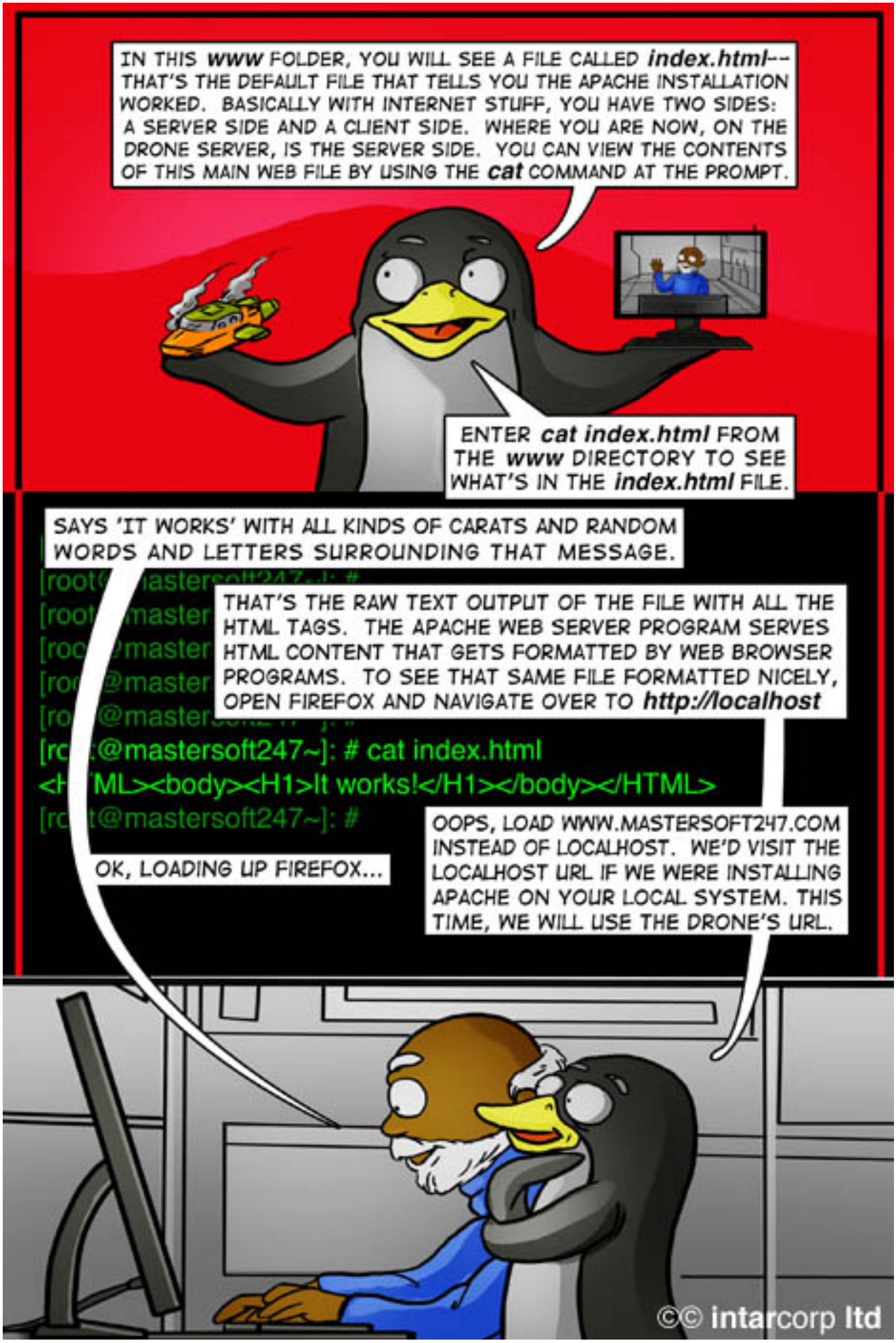

TOK!!!
TOK!!
SKWIRK!
SKWIRK!
©© intarcorp ltd
CLANK!
THUMP!


OK, LET'S CHECK IF ANYONE ELSE IS LOGGED INTO THIS SERVER.
THE SPACESHIP?
YES. FIRST ENTER THE LETTER w AT THE COMMAND PROMPT AND THEN HIT ENTER. THIS ONE-LETTER COMMAND SHOWS WHO IS LOGGED IN AND WHAT THEY ARE DOING.
IT JUST SHOWS ME AND A USER CALLED BALMY.
LET'S TERMINATE HIM, CALVIN, BUT FIRST WE NEED TO SEND HIM A MESSAGE. AT THE SHELL PROMPT, TYPE wall AND THEN ANY MESSAGE YOU WANT TO SEND IN QUOTATION MARKS. THEN POST THE MESSAGE BY HITTING ENTER.
broadcast message from slav
problem exists between keyl
and chair!
slave1975@mastersoft247.com ~:
wall "problem exists
keyboard and ch
©© intarcorp ltd

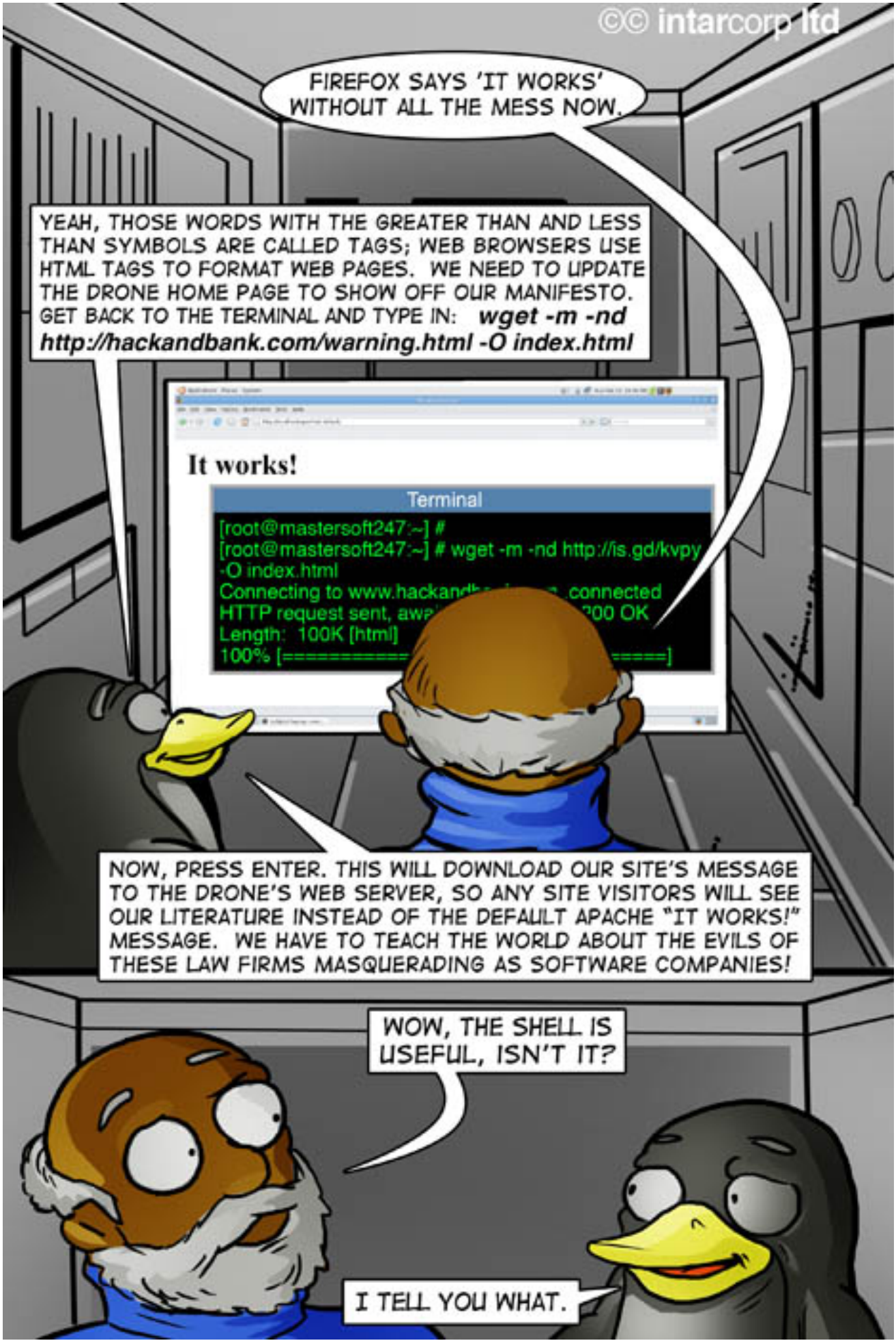

THAT WAS AWESOME!! DID THAT TERMINATE HIM?
NAH, TO DO THAT, YOU HAVE TO BE ROOT. TO BE ROOT, TYPE **su** - AND PRESS ENTER. YOU WILL BE ASKED FOR THE ROOT PASSWORD--HERE IT IS.
GOT IT. SO NOW I'M THE BOSS OF THE SERVER?
YEP, YOU'VE GOT THE POWER. TO LOG BALMY OUT, TYPE **skill -KILL -u balmy** AND THEN PRESS ENTER. ONCE YOU LOG HIM OUT, ENTER **userdel balmy** AT THE PROMPT THAT WILL DELETE HIS ACCOUNT ON THE SERVER.
JUST BALMY AS THE ARGUMENT WITH **userdel**--NO OPTIONS NECESSARY?
YOU CAN SEE FROM THE **userdel** MAN PAGE THAT YOU COULD USE DIFFERENT OPTIONS WITH THE **userdel** COMMAND TO DO THINGS LIKE REMOVE THAT USER'S HOME FOLDER AND THE FILES IN IT, BUT WE WANT TO LEAVE THOSE SO WE CAN SEE WHAT HE WAS STORING ON THE DRONE'S SERVER. SO NO, YOU DON'T NEED ANY OPTIONS THIS TIME.
DONE AND DONE.
OH NOES! MY LOGIN DOESN'T WORK!
balmy
©© intarcorp ltd


CHECK AND MATE!
NOW LET'S GET THE APACHE WEB SERVER INSTALLED ON THIS THING SO WE CAN USE IT TO TELL THE WORLD ABOUT MASTERSOFT'S SHADY BUSINESS PRACTICES AND SPREAD THE WORD ABOUT LINUX.
DO I NEED TO LAUNCH THE SYNAPTIC PACKAGE MANAGER IN THE GUI TO DO THAT?
THE GUI WOULD WORK, BUT WE CAN ALSO INSTALL PROGRAMS WITH A SHELL-BASED PACKAGE MANAGER ENTER apt-get install apache2 AT THE PROMPT.
SO install IS AN ARGUMENT?
install IS A COMMAND. THE apt-get COMMAND REQUIRES A SECOND COMMAND, AS YOU CAN SEE IN THE MANUAL ENTRY FOR apt-get. apt-get install TELLS THE APT PACKAGE MANAGER TO INSTALL THE PROGRAMS THAT FOLLOW. IN THIS CASE, WE TELL THE SYSTEM TO INSTALL APACHE, WHICH IS AN HTTP WEB SERVER, MEANING YOU ACCESS ITS CONTENT USING THE HYPERTEXT TRANSFER PROTOCOL, WHICH IS VIEWED WITH PROGRAMS CALLED WEB BROWSERS.
LIKE FIREFOX?
EXACTLY.
©© intarcorp ltd


IT SAYS THAT IT NEEDS TO INSTALL SOME EXTRA PACKAGES. IS THAT OK?
YEAH, JUST HIT ENTER. WHEN IT ASKS YOU TO CHOOSE Y OR n, YOU CAN JUST PRESS RETURN BECAUSE THE Y BEING CAPITALIZED MEANS THAT'S THE DEFAULT CHOICE.
OK, IT LOOKS LIKE THE INSTALLATION IS DONE!
YES SIR. NOW LET'S JUST MAKE SURE APACHE IS RUNNING AND COPY THE MASTERSOFT SUSPENSION NOTIFICATION TO THE DRONE'S WEB SERVER CONTENT DIRECTORY. TO MAKE SURE APACHE IS RUNNING ON THE DRONE, TYPE apache2ctl status AT THE PROMPT. IF IT GIVES INFORMATION ABOUT THE SERVER, IT IS RUNNING. SCROLL THRU A FEW LINES, AND YOU SHOULD SEE AN ENTRY FOR SERVER UPTIME WHICH CONFIRMS APACHE IS RUNNING.
root@mastersoft247:~# apache2ctl status
UPTIME 23 SECONDS.
NOW TYPE cd /var/www AND PRESS ENTER. THIS WILL TAKE YOU TO THE PART OF THE FILE SYSTEM WHERE THE WEB SERVER INITIALLY STORES WEBSITE CONTENT.
©© intarcorp ltd

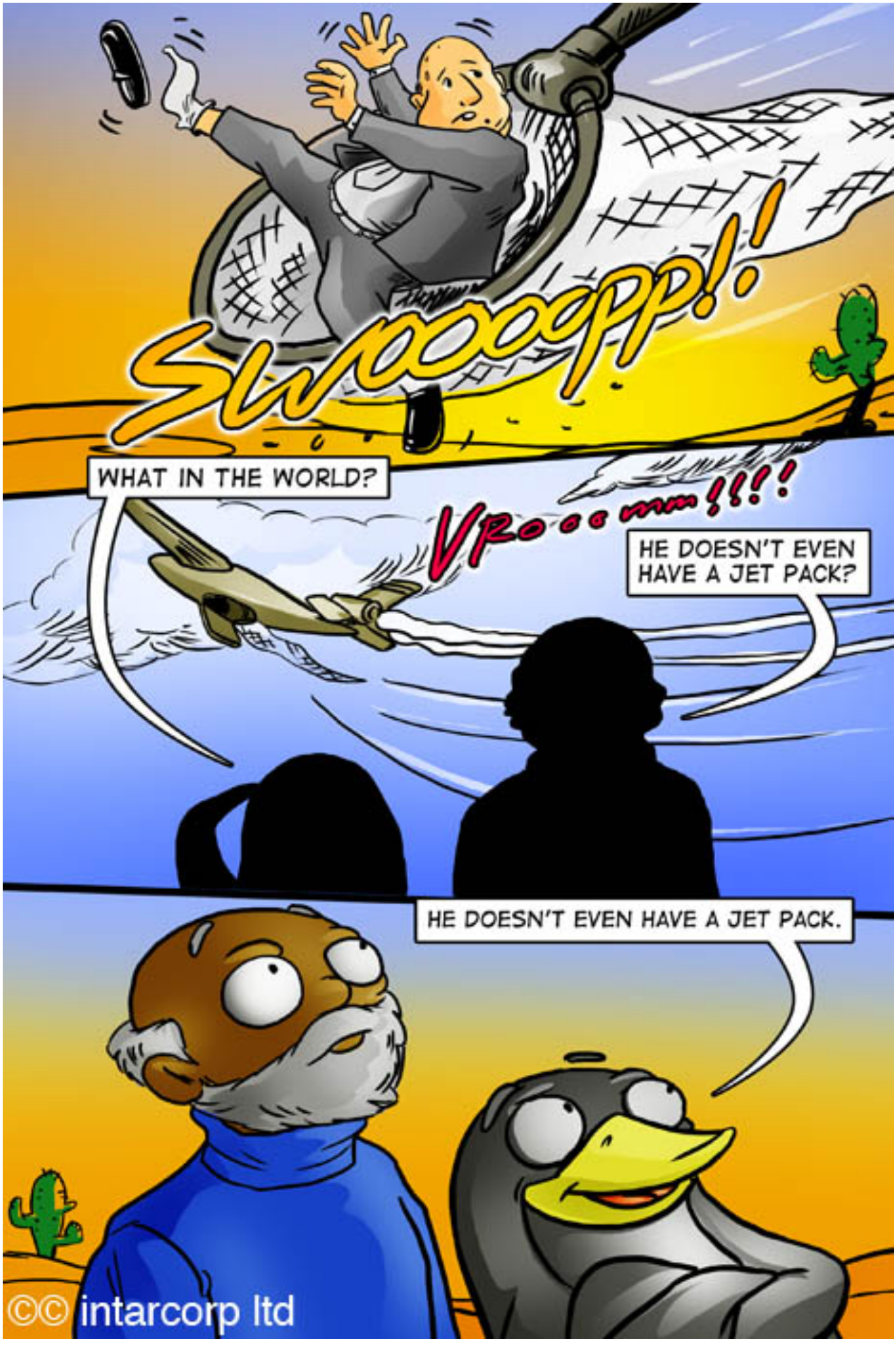

IN THIS www FOLDER, YOU WILL SEE A FILE CALLED index.html-- THAT'S THE DEFAULT FILE THAT TELLS YOU THE APACHE INSTALLATION WORKED. BASICALLY WITH INTERNET STUFF, YOU HAVE TWO SIDES: A SERVER SIDE AND A CLIENT SIDE. WHERE YOU ARE NOW, ON THE DRONE SERVER, IS THE SERVER SIDE. YOU CAN VIEW THE CONTENTS OF THIS MAIN WEB FILE BY USING THE cat COMMAND AT THE PROMPT.
ENTER cat index.html FROM THE www DIRECTORY TO SEE WHAT'S IN THE index.html FILE.
SAYS 'IT WORKS' WITH ALL KINDS OF CARATS AND RANDOM WORDS AND LETTERS SURROUNDING THAT MESSAGE.
THAT'S THE RAW TEXT OUTPUT OF THE FILE WITH ALL THE HTML TAGS. THE APACHE WEB SERVER PROGRAM SERVES HTML CONTENT THAT GETS FORMATTED BY WEB BROWSER PROGRAMS. TO SEE THAT SAME FILE FORMATTED NICELY, OPEN FIREFOX AND NAVIGATE OVER TO http://localhost
@mastersoft247~]: # cat index.html
ML><body><H1>It works!</H1></body></HTML>
@mastersoft247~]: #
OK, LOADING UP FIREFOX...
OOPS, LOAD WWW.MASTERSOFT247.COM INSTEAD OF LOCALHOST. WE'D VISIT THE LOCALHOST URL IF WE WERE INSTALLING APACHE ON YOUR LOCAL SYSTEM. THIS TIME, WE WILL USE THE DRONE'S URL.
©© intarcorp ltd

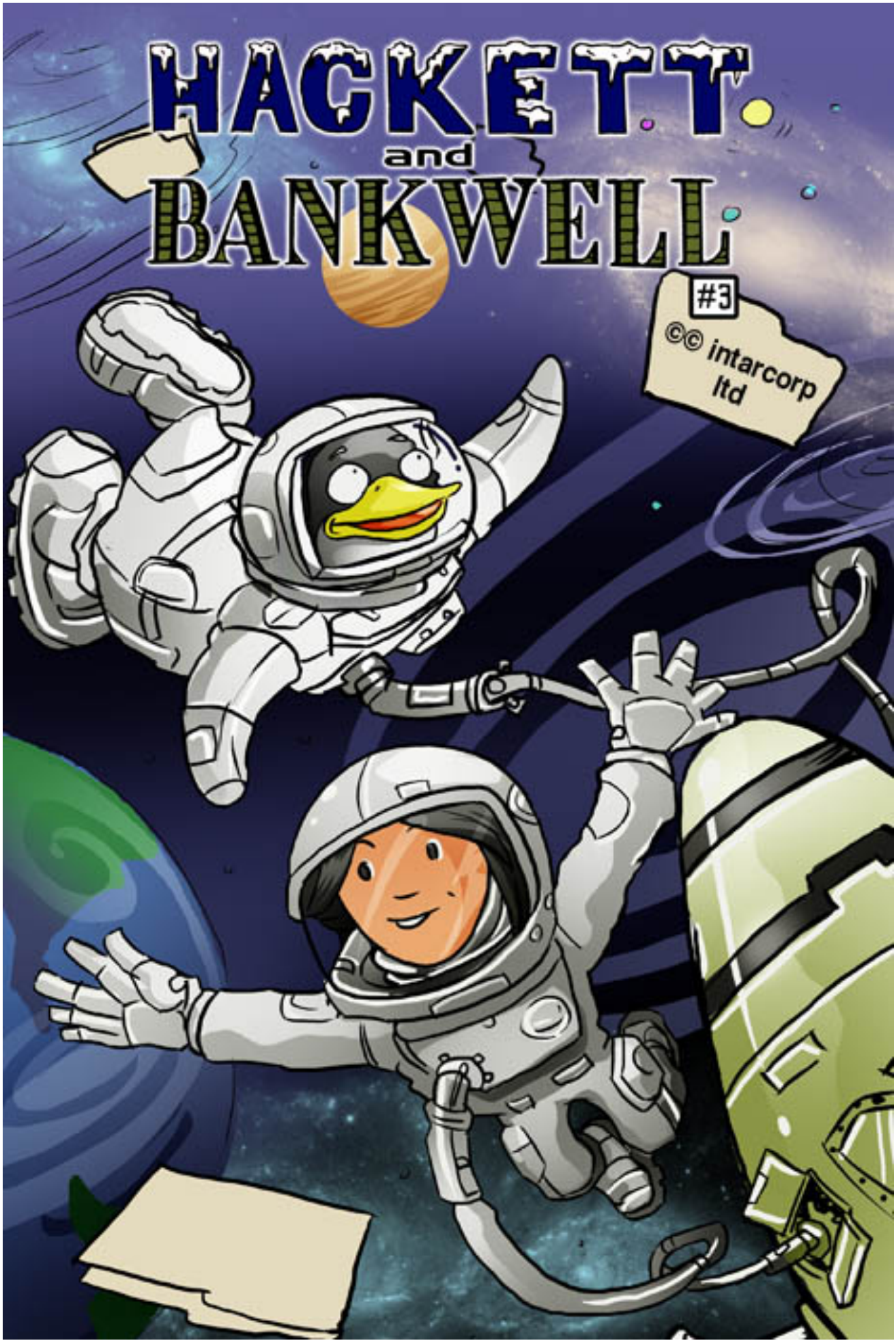
©© intarcorp ltd




SO... DID IT WORK?
WELL, IF YOU CAT THE FILE AGAIN ON THE SERVER, IT WILL DEFINITELY LOOK DIFFERENT. BUT YOU CAN ALSO SEE THE CHANGES JUST BY REFRESHING THE PAGE IN FIREFOX.
THIS SITE HAS BEEN REMEDIATED BY HACKETT
OH MY.
WHAT HAVE WE DONE?
WE HAVE TURNED THE MALICIOUS CORPORATE BOTNET ON ITS HEAD AND TAKEN OUR MESSAGE TO THE PEOPLE! TO EXIT THE ROOT ACCOUNT, JUST TYPE exit AND HIT ENTER. TO GET OUT OF THE DRONE, ENTER exit AGAIN.
©© intarcorp ltd


YES.
WE DID IT!
hmmpff!!
hmmpff!!
WHAT IN THE WORLD?
huh!!
huh!!
©© intarcorp ltd


Swoooopp!!
WHAT IN THE WORLD?
VRoooomm!!!!
HE DOESN'T EVEN HAVE A JET PACK?
HE DOESN'T EVEN HAVE A JET PACK.
©© intarcorp ltd


HACKETT
and
BANKWELL
#3
©© intarcorp ltd