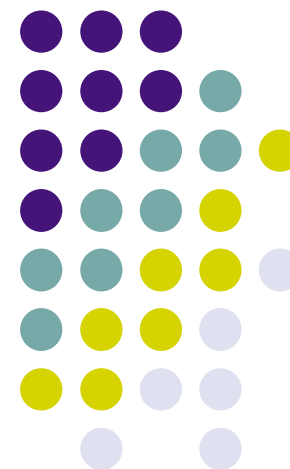
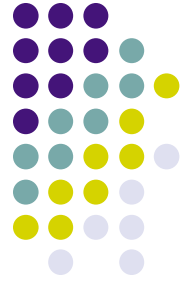


An Introduction to Linux as a Tool for Digital Investigation and Analysis

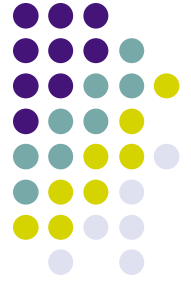
Paul Burke / Chris Marberry
National Center for Forensic Science





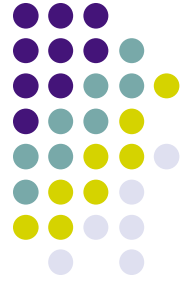
Introduction to Linux

- Why should I care about Linux?
 - Linux has an estimated 29 million users
 - Large presence in the server/enterprise market
 - Used in PDAs, cell phones, home Internet routers
 - Exceedingly powerful for computer examinations; provides an alternative to expensive Windows suites
 - Free!
- Target audiences:
 - People who haven't used Linux before
 - Casual Linux users who want to know more



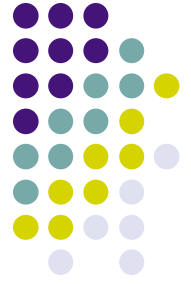
Introduction to Linux

- What is Linux?
 - Origins, open source, GNU
- Linux fundamentals: how does it work?
 - UNIX philosophy
- Basic command-line usage
 - Working with files, simple programs in the shell



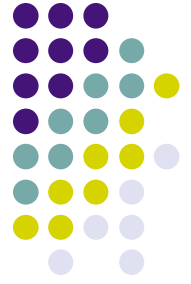
What is Linux?

- Linux is a *kernel*: core of an operating system
- Kernel arbitrates hardware access, provides a Hardware Abstraction Layer (HAL)
- Sits between applications and the hardware
- Knows how to talk to each device attached through the use of drivers
- Without programs, a kernel is useless (more on this later)



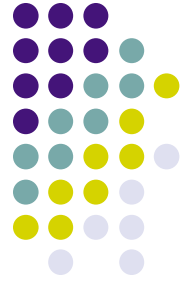
What is Linux?

- Linux was created by Linus Torvalds in 1991 as a hobby kernel to run on his 386
- Modeled after Minix, which in turn was modeled after UNIX
- Released on the Internet, where people contributed to it
- Licensed under the GNU GPL, an open source license



Open Source

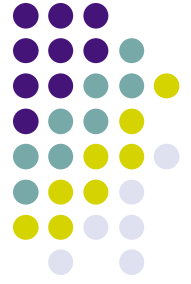
- Open source software: everyone can download and read the source code
- What is source code?
- Different licenses have different stipulations (BSD vs. GPL)
- The GNU General Public License (GPL): If you make changes and release the binary program, you must release the source code to the public and it must be under the GPL
 - So-called “viral” license



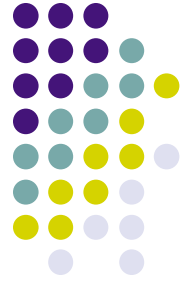
Open Source

- This sharing encourages contribution; thousands have contributed directly to the Linux kernel to date (via patches)
- Does this make Linux dangerous to use?
 - No! “Many eyes” ideology
- If you need a feature, you code it and submit it
 - Security-Enhanced Linux (SELinux) contributed by the NSA
 - NASA created FlightLinux for spacecraft use

GNU/Linux Operating System

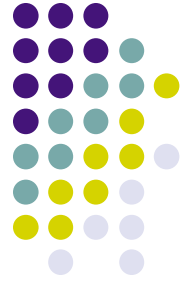


- We mentioned a kernel is useless without programs
- A Linux system typically uses a base set of programs from the Free Software Foundation's GNU (GNU's Not UNIX) project
- GNU Project: Create a Free (GPL) Unix clone
- Coupled with a GNU base system, the resultant operating system is technically called "GNU/Linux" (but few bother with this term)



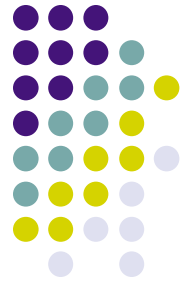
GNU/Linux

- Now we have an OS, but little else
- Distributions: A full package including Linux, GNU utilities, a graphical interface, and other programs (office software, etc)
- Offer package management and configuration utilities as well
- Red Hat (Fedora Core), Debian, SUSE, Gentoo, Mandriva, KNOPPIX



UNIX Philosophy

- What is UNIX?
- Operating system developed in 1960s and 1970s
- Philosophy: multi-user, multi-tasking, portable
- Numerous small utilities which can interact to perform complex tasks
- Everything is a file
- Text and text files are central to the operation of the system
- Linux generally adheres to these design goals



Linux Fundamentals

- Linux can run without a Graphical User Interface (GUI)
- Command-Line Interface (CLI): Like DOS, but more powerful
- Interact with the computer through a “shell” (interpreter)

```
deacon:~ pburke$ █  
pburke@deacon:~$ █
```



Linux Fundamentals

- The CLI is powerful!
- Let's take the Windows Search function as an example:
 - Search certain drives, modification date, size, type, etc...
- A search for a file with a modification date within the past year (next)

Search Results

File Edit View Favorites Tools Help

Back Forward Search Folders

Address Search Results Go

Search Companion

Search by any or all of the criteria below.

All or part of the file name:
win32

A word or phrase in the file:

Look in:
Local Hard Drives (C:)

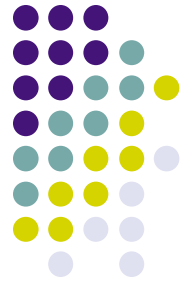
When was it modified?

Don't remember
 Within the last week
 Past month
 Within the past year

Search

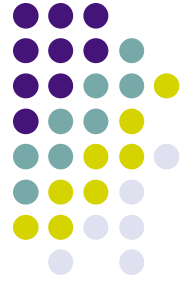
Name	In Folder
Azureus_2.3.0.4_Win32.setu...	C:\Documents and Settings\Student
dnetc-win32-x86	C:\Documents and Settings\Student
dnetc-win32-x86.zip	C:\Documents and Settings\Student
vnc-4_1_1-x86_win32_view...	C:\Documents and Settings\Student
vorbis-tools-1.0.1-win32	C:\Documents and Settings\Student
dcfldd-1.2.3-2.x86win32.zip	C:\Documents and Settings\Student
README-WIN32	C:\Documents and Settings\Student
vorbis-tools-1.0.1-win32	C:\Documents and Settings\Student
Win32	C:\Documents and Settings\Craiger'

9 objects



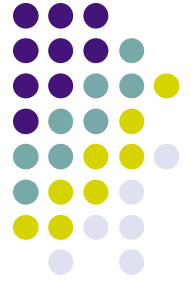
Linux Fundamentals

- Now let's do that on the command line using the 'find' program:
 - `find / -mtime -365 -iname '*win32*`
- What else could you do?
- Find any files that were modified in the past 7 days, which are more than 5 megabytes in size, owned by user 'pburke', which have the .jpg filename extension
 - `find / -type f -mtime -7 -iname '*.jpg' -size +5M -user pburke`



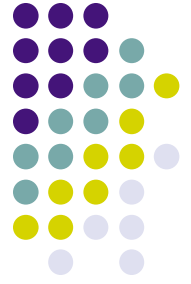
Linux Fundamentals

- Linux is a multi-user system
 - Many users can be logged in at once (at console, over the network)
 - Every file and directory has an owner and permissions (access control)
 - Users can be classified into groups with similar permissions
- Superuser (root) versus regular users
- File permissions: read, write, execute (rwx) for owner, group, everyone



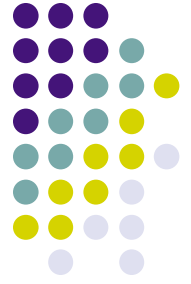
Linux Fundamentals

- Linux is case-sensitive
 - Bork, bork, BORK, bORk are different files or commands
- Successful commands usually do not return notification
- UNIX geeks are lazy typists
 - ls, cat, chmod, ifconfig
 - /usr, /src, /tmp
- Everything is a file!
 - Hard disk drives, floppy drives, serial/parallel ports can be interacted with directly (send raw data)



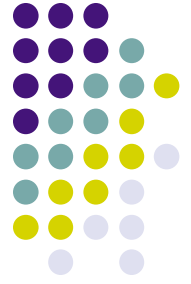
Linux Fundamentals

- Filesystem structure
 - Directories, not folders
 - Everything extends off of / (root directory)
 - /bin: Vital system programs
 - /sbin: Vital system programs for root user
 - /usr/bin: Programs
 - /etc: Configuration files
 - /home: Home directories for each user
 - /var: Volatile files (Web pages, mail spool)
 - /tmp: Temporary files
 - /dev: Device entries



Linux Fundamentals

- Filesystem structure
 - Relative paths
 - Single dot '.' represents current directory, double dot '..' represents directory above current
- Moving on: Command line usage



Basic Linux Commands

- Shells: sh, ksh, bash, csh, tcsh (and more)
 - Linux usually uses bash (Bourne-again Shell)
 - Shell takes commands and executes programs
 - Provides other features (tab-completion, history, globbing)
 - For basic use, most modern shells are more or less the same
 - Command flags/switches, command arguments
 - Shell scripting



Basic Linux Commands

- Common Commands
 - ls: list files (add -l to make it a long listing)

```
deacon:~/linux pburke$ ls
borkbork      chocolate      moose
deacon:~/linux pburke$ ls -l
total 8
-rw-r--r--   1 pburke  admin   50 Jul 13 13:55 borkbork
-rwxrwxrwx   1 pburke  pburke   0 Jul 13 14:01 chocolate
drwx-----  2 pburke  pburke  68 Jul 13 14:01 moose
deacon:~/linux pburke$
```



Basic Linux Commands

- mv: Move a file or folder (also for renaming)

A screenshot of an rxvt terminal window. The window title is "rxvt". The terminal shows the following sequence of commands and output:

```
deacon:~/linux pburke$ ls
borkbork      chocolate      moose
deacon:~/linux pburke$ mv borkbork duckduck
deacon:~/linux pburke$ ls
chocolate    duckduck      moose
deacon:~/linux pburke$
```

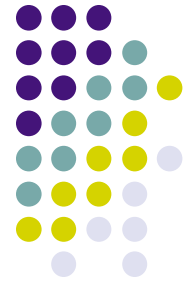


Basic Linux Commands

- cat: Dump contents of file to screen

A screenshot of an rxvt terminal window. The window title is 'rxvt'. The prompt is 'deacon:~/linux pburke\$'. The command 'cat borkbork' has been executed, resulting in the following output:

```
deacon:~/linux pburke$ cat borkbork
BORK BORK BORK BORK BORK
(new line!) BORK
Spiffy.
deacon:~/linux pburke$
```



Basic Linux Commands

- cp: Copy a file to another

```
deacon:~/linux pburke$ cat borkbork
deacon:~/linux pburke$ ls -l
total 8
-rw-r--r--  1 pburke  admin   50 Jul 13 13:55 borkbork
-rwxrwxrwx  1 pburke  pburke   0 Jul 13 14:01 chocolate
drwx----- 2 pburke  pburke  68 Jul 13 14:01 moose
deacon:~/linux pburke$ cp borkbork cheese
deacon:~/linux pburke$ ls -l
total 16
-rw-r--r--  1 pburke  admin   50 Jul 13 13:55 borkbork
-rw-r--r--  1 pburke  pburke  50 Jul 16 13:29 cheese
-rwxrwxrwx  1 pburke  pburke   0 Jul 13 14:01 chocolate
drwx----- 2 pburke  pburke  68 Jul 13 14:01 moose
deacon:~/linux pburke$
```



Basic Linux Commands

- rm: Remove a file (no undelete command!)

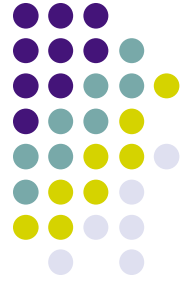
```
deacon:~/linux pburke$ ls -l
total 16
-rw-r--r--  1 pburke  admin   50 Jul 13 13:55 borkbork
-rw-r--r--  1 pburke  pburke  50 Jul 16 13:38 cheese
-rwxrwxrwx  1 pburke  pburke   0 Jul 13 14:01 chocolate
drwx-----  2 pburke  pburke  68 Jul 13 14:01 moose
deacon:~/linux pburke$ rm cheese
deacon:~/linux pburke$ ls -l
total 8
-rw-r--r--  1 pburke  admin   50 Jul 13 13:55 borkbork
-rwxrwxrwx  1 pburke  pburke   0 Jul 13 14:01 chocolate
drwx-----  2 pburke  pburke  68 Jul 13 14:01 moose
deacon:~/linux pburke$
```



Basic Linux Commands

- cd: Change directory

```
deacon:~/linux pburke$ cd moose
deacon:~/linux/moose pburke$ ls
deer    elk    yak
deacon:~/linux/moose pburke$ cd ..
deacon:~/linux pburke$ ls
borkbork      chocolate      moose
deacon:~/linux pburke$
```



Basic Linux Commands

- Other common commands:
 - mkdir: Create a directory
 - touch: Create an empty file
 - chown: Change the owner of a file
 - chmod: Change the permissions (mode) of a file
 - echo: Prints to the screen the content that is fed



Basic Linux Commands

- Why is “echo” useful?
 - Can feed text to a file
- Shell redirection: > <

A screenshot of an rxvt terminal window. The window title is "rxvt". The terminal shows the following commands and output:

```
deacon:~/linux pburke$ echo "Duck Soup"
Duck Soup
deacon:~/linux pburke$ echo "Duck Soup" > harpo
deacon:~/linux pburke$ ls
borkbork      harpo
chocolate    moose
deacon:~/linux pburke$ cat harpo
Duck Soup
deacon:~/linux pburke$
```



Basic Linux Commands

- Redirection redirects data to a file
- Piping redirects data to another program

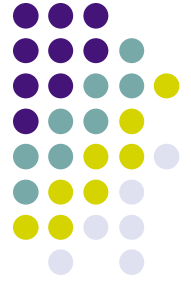
```
deacon:~/linux pburke$ cat unsorted
3 Bees
1 Goose
2 Buffalo
deacon:~/linux pburke$ cat unsorted | sort > sorted
deacon:~/linux pburke$ cat sorted
1 Goose
2 Buffalo
3 Bees
deacon:~/linux pburke$
```



Basic Linux Commands

- How does the shell know where to look for programs?
 - Path: List of directories with executables in them
 - Stored in shell variable \$PATH

```
deacon:~/linux pburke$ echo $PATH
/usr/bin:/bin:/usr/sbin:/sbin:/usr/X11R6/bin
deacon:~/linux pburke$
```



Linux Documentation

- man: Access manual pages
 - Type “man” and then the command you want help with
 - Most programs have man pages which describe their operation and options
 - Use the direction keys to navigate, type “q” when you are done

```
LS(1) User Commands LS(1)
NAME
  ls - list directory contents
SYNOPSIS
  ls [OPTION]... [FILE]...
DESCRIPTION
  List information about the FILES (the current directory by default).
  Sort entries alphabetically if none of -cftuSUX nor --sort.

  Mandatory arguments to long options are mandatory for short options
  too.

-a, --all
  do not hide entries starting with .

-A, --almost-all
  do not list implied . and ..

--author
  print the author of each file
Manual page ls(1) line 1
```

TCPDUMP(8)

TCPDUMP(8)

NAME

tcpdump - dump traffic on a network

SYNOPSIS

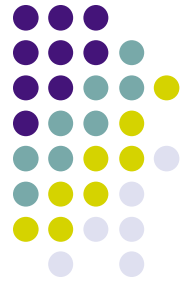
```
tcpdump [ -AdDeflLnNOpqRStuVvxX ] [ -c count ]
        [ -C file_size ] [ -F file ]
        [ -i interface ] [ -m module ] [ -r file ]
        [ -s snaplen ] [ -T type ] [ -w file ]
        [ -E spi@ipaddr algo:secret,+++ ]
        [ -y datalinktype ]
        [ expression ]
```

DESCRIPTION

Tcpdump prints out the headers of packets on a network interface that match the boolean expression. It can also be run with the w flag, which causes it to save the packet data to a file for later analysis, and/or with the r flag, which causes it to read from a saved packet file rather than to read packets from a network interface. In all cases, only packets that match expression will be processed by tcpdump.

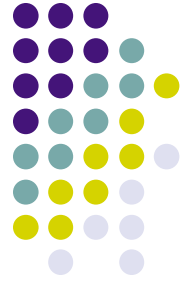
Tcpdump will, if not run with the c flag, continue capturing packets

Manual page tcpdump(8) line 1



Other Linux Resources

- Rute User's Tutorial and Exposition
 - <http://www.icon.co.za/~psheer/book/index.html.gz>
- A Basic UNIX Tutorial (isu.edu)
 - <http://www.isu.edu/departments/comcom/unix/workshop/unixindex.html>
- UNIX For Beginners
 - <http://wolfram.schneider.org/bsd/7thEdManVol2/beginners/beginners.html>
- Google Linux
 - <http://www.google.com/linux>



Conclusion

- What did we learn?
 - What Linux is
 - Where it came from
 - How UNIX fits into the picture
 - Basic command-line usage
 - Where to learn more