



Introduction to Computer Forensics

David Nardoni CISSP, EnCE
dnardoni@firstresponseconsulting.com

Chi So
chiso@usc.edu



Overview

Introduction to computer systems and computer networks

- Introduction to Computers
- Introduction to Windows systems
- Introduction to Linux systems
- Introduction to computer networking
- Introduction to internet and email



Introduction to Computers

- CPU: Central Processing Unit: Brain of the computer, processes instructions once it receives power from the power supply.
- BIOS: Basic input output system, moves data around the computer to and from the CPU
- POST: Power on self test. CPU receives power and BIOS runs POST program to test components. This is where we can interrupt the boot process
- CMOS: Complementary Metal Oxide Silicon configuration tool. This program retains the date, time and hard drive parameters when the power is off. It retains this information with the help of a CMOS battery.

We use the CMOS to determine the date and time of the system as well as the boot order



Windows File Systems

Windows File systems: FAT NTFS

FAT

The File Allocation Table (FAT) file system is a simple file system originally designed for small disks and simple folder structures. The FAT file system is named for its method of organization, the file allocation table, which resides at the beginning of the volume. To protect the volume, two copies of the table are kept, in case one becomes damaged. In addition, the file allocation tables and the root folder must be stored in a fixed location so that the files needed to start the system can be correctly located.

Different versions of FAT: FAT12, FAT16, FAT32



NTFS File Systems

- The Windows NT file system (NTFS) provides a combination of performance, reliability, and compatibility not found in the FAT file system. It is designed to quickly perform standard file operations such as read, write, and search — and even advanced operations such as file-system recovery — on very large hard disks.
- Formatting a volume with the NTFS file system results in the creation of several system files and the Master File Table (MFT), which contains information about all the files and folders on the NTFS volume.
- The first information on an NTFS volume is the Partition Boot Sector, which starts at sector 0 and can be up to 16 sectors long. The first file on an NTFS volume is the Master File Table (MFT).



Windows File Structure

Documents and settings: Settings for all users and their corresponding profiles

%ProfileName%: A folder for each user that logs on to the system is created and their individual settings are stored in this location.

Program Files: Location where program installs are stored

Temp: Location where temporary files are created and deleted

Windows: Location where operating system files and folders are installed



Registry, Control Panel, Search, Help

- Windows registry: Database where all information about a computer is stored. OS, hardware, user, application and security related information
- The Control Panel: This is where all system configuration tools are located.
- Search: Tool to find files or folders based on search expressions.
- Help: System to aid user in finding answers to questions.



File Permissions and access controls (ACL)

- **Read:** Allows files or folders to be opened as read-only and to be copied.
- **Write:** Allows the creation of files and folders; allows data to be added to or removed from files.
- **List Folder Contents:** As per Read but also allows navigation of sub-folders.
- **Read and Execute:** As per Read but also allows users to run executable files.
- **Modify:** All the above as well as the permission to delete the file or folder.
- **Full Control:** Full Control -- including the ability to change ACLs.

All settings have an allow or deny checkbox associated with each user or group that is given associated with the ACL

NTFS file systems allow for much more granular based access controls such as file level permissions, where FAT file systems only allow folder level ACL's



Windows auditing

All audit logs in windows are kept in event logs

Event logs are located in

`%systemdrive%\windows\system32\config\`

There are three different event logs

- AppEvent.evt: Stores information, warnings and errors relating to applications on system
- SecEvent.evt: Stores security success and failure related events
- SysEvent.evt: Stores information, warnings and errors relating to OS and services on system



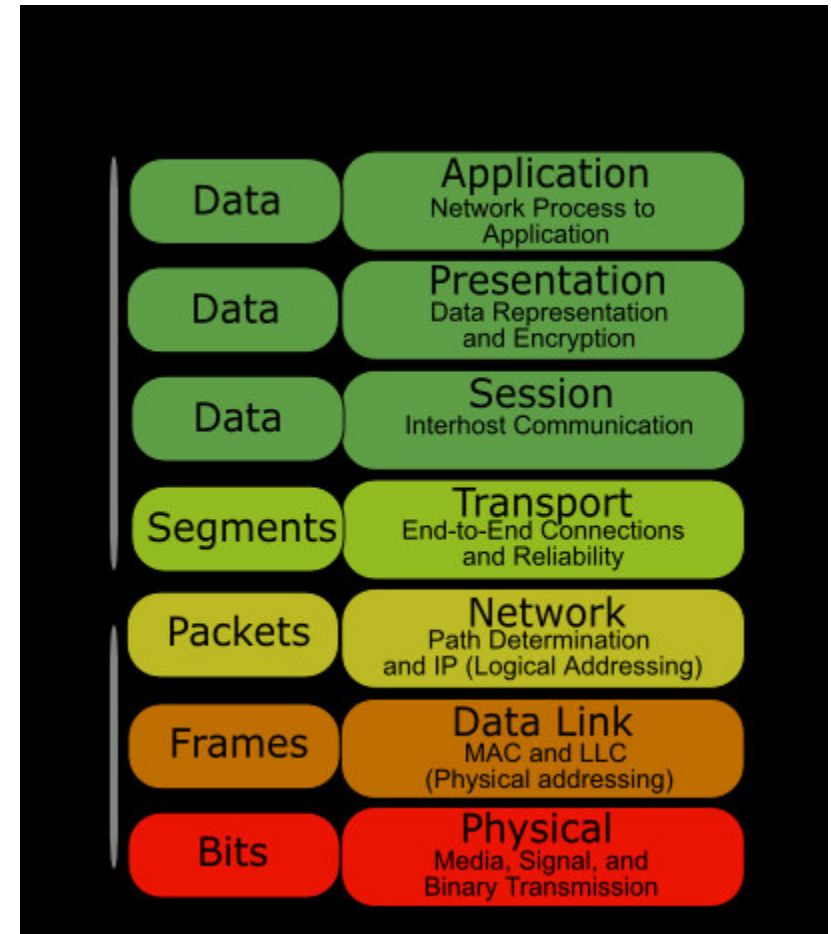
Networking

Basic networking protocols

TCP/IP: Most all systems use this protocol to connect to each other

IPX/SPX: Novell systems use IPX for connectivity

Appletalk: Apple Systems use appletalk for connectivity





Basic commands

From the Run command: cmd – will open a DOS prompt to allow you to run command line based commands

- Command + “/?” Will list command options
- Dir: list directory contents
- Mkdir: make directory
- Del: delete file
- Ipconfig: lists TCP/IP information
- Netstat: lists open connections and their corresponding remote Ip’s and ports
- Ping: sends an ICMP packet to a system to test connectivity
- Telnet: allows you to connect remotely to a system based on the port you supply



Sample Log Files

Sample firewall log excerpt

```
Jul 25 20:23:02 sophie kernel: Packet log: input REJECT eth0 PROTO=17 203.79.72.254:63004
202.0.36.148:137 L=257 S=0x00 I=48927 F=0x0000 T=7 (#48)
Jul 25 20:23:03 sophie kernel: Packet log: input REJECT eth0 PROTO=17 203.79.72.254:63004
202.0.36.148:137 L=257 S=0x00 I=48927 F=0x0000 T=7 (#48)
Jul 25 20:23:03 sophie kernel: Packet log: input REJECT eth0 PROTO=17 203.79.72.254:63004
202.0.36.148:137 L=257 S=0x00 I=48927 F=0x0000 T=6 (#48)
```

Sample email header excerpt

```
Received: from NIH2WAAF (mail6.foo1.csi.com [149.xxx.183.75]) by
Fubarino.com (8.8.3/8.6.9) with ESMTP id XAA20854 for
<galf...@Fubarino.com>; Sun, 27 Apr 1997 23:07:01 GMT
Received: from CISPPP - 199.xxx.193.176 by csi.com with Microsoft SMTPSVC;
Sun, 27 Apr 1997 22:53:36 -0400
Message-Id: <2.2.16.19970428082132.2cdf5...@fubar.com>
X-Sender: cmei...@fubar.com
X-Mailer: Windows Eudora Pro Version 2.2 (16)
Mime-Version: 1.0
Content-Type: text/plain; charset="us-ascii"
To: galf...@Fubarino.com
From: "Carolyn P. Meinel" <cmei...@techbroker.com>
Subject: Sample header
Date: 27 Apr 1997 22:53:37 -0400
```




Choosing Linux Distro.

[Linux Distribution Chooser](#)

<http://www.zegeniestudios.net/ldc/>

Beginner: [Mandriva](#), [Ubuntu](#), [Xandros](#), [Linspire](#)

Intermediate: [Red Hat](#), [SuSE](#), [Fedora](#)

Advance: [FreeBSD](#), [Gentoo](#), [Debian](#), [Slackware](#)

Live CDs: [Penguin Sleuth Bootable CD](#), [Helix](#), [Plan-B](#)



Linux Filesystems

The Linux kernel supports various filesystems. We'll explain ext2, ext3, ReiserFS, XFS and JFS as these are the most commonly used filesystems on Linux systems.

- **ext2** is the tried and true Linux filesystem but doesn't have metadata journaling, which means that routine ext2 filesystem checks at startup time can be quite time-consuming. There is now quite a selection of newer-generation journaled filesystems that can be checked for consistency very quickly and are thus generally preferred over their non-journaled counterparts. Journaled filesystems prevent long delays when you boot your system and your filesystem happens to be in an inconsistent state.
- **ext3** is the journaled version of the ext2 filesystem, providing metadata journaling for fast recovery in addition to other enhanced journaling modes like full data and ordered data journaling. ext3 is a very good and reliable filesystem. It has an additional hashed b-tree indexing option that enables high performance in almost all situations. You can enable this indexing by adding `-O dir_index` to the `mke2fs` command. In short, ext3 is an excellent filesystem.



Linux Filesystem (Con't)

- **ReiserFS** is a B*-tree based filesystem that has very good overall performance and greatly outperforms both ext2 and ext3 when dealing with small files (files less than 4k), often by a factor of 10x-15x. ReiserFS also scales extremely well and has metadata journaling. As of kernel 2.4.18+, ReiserFS is solid and usable as both general-purpose filesystem and for extreme cases such as the creation of large filesystems, the use of many small files, very large files and directories containing tens of thousands of files.
- **XFS** is a filesystem with metadata journaling which comes with a robust feature-set and is optimized for scalability. We only recommend using this filesystem on Linux systems with high-end SCSI and/or fibre channel storage and an uninterruptible power supply. Because XFS aggressively caches in-transit data in RAM, improperly designed programs (those that don't take proper precautions when writing files to disk and there are quite a few of them) can lose a good deal of data if the system goes down unexpectedly.
- **JFS** is IBM's high-performance journaling filesystem. It has recently become production-ready and there hasn't been a sufficient track record to comment positively nor negatively on its general stability at this point.



File Structure

- **root** - home directory for root user
- **home** - contain users home directory along directory for services
- **bin** - commands needed during bootup; might be needed by normal users
- **sbin** - light bin but command is not intended for normal users
- **proc** - this file system is not on a disc, a virtual file system that exists in the kernel's imagination, which is memory



File Structures (Con't)

- ***usr*** - contains all commands, libraries, man pages, games, and static files for normal operation
- ***boot*** - files used by the bootstrap loader
- ***lib*** - share libraries needed by programs on the root file system
- ***dev*** - device files
- ***etc*** - configuration files



File Structures (Con't)

- *var* - contains files that change for mail, news, printer log files, man pages, temp files
- *mnt* - mount points for temporary mounts by the sys admin
- *tmp* - temporary files



Man – Linux help

- man
- [cmd] –help

[FreeBSD Hypertext Man Page](http://www.freebsd.org/cgi/man.cgi)

<http://www.freebsd.org/cgi/man.cgi>



Linux Run Levels

- rc1.d - Single User Mode
- rc2.d - Single User Mode with Networking
- rc3.d - Multi-User Mode - boot up in text mode
- rc4.d - Not yet Defined
- rc5.d - Multi-User Mode - boot up in X Windows
- rc6.d - Shutdown



Logging

- syslog
- [syslog.conf – Linux Command – Unix Command](http://linux.about.com/od/commands/l/blcmdl5_syslogc.htm)
http://linux.about.com/od/commands/l/blcmdl5_syslogc.htm



File Permissions

```
$ ls -lu /etc/shadow
```

```
-r----- 1 root  root  573 Apr 22 21:04 /etc/shadow
```

```
$ chmod a+r etc/shadow
```

u: user

g: group

o: other

a: all

r: read

w: write

x: execute



Network Management

- **arp** - this program let's the user read or modify their arp cache
- **ifconfig** - configure network interface
- **netconf** - (red hat only) interactive program to configure network
- **ping** - send ICMP ECHO_REQUEST packets



Cron

Cron Entry:

minute hour dom month dow user cmd

Examples:

01 * * * * root echo "This command is run at one min past every hour"

17 8 * * * root echo "This command is run daily at 8:17 am"

17 20 * * * root echo "This command is run daily at 8:17 pm"

00 4 * * 0 root echo "This command is run at 4 am every Sunday"

*** 4 * * Sun root echo "So is this"**

42 4 1 * * root echo "This command is run 4:42 am every 1st of the month"

01 * 19 07 * root echo "This command is run hourly on the 19th of July"



Cron (Con't)

- **minute** This controls what minute of the hour the command will run on, and is between '0' and '59'
- **hour** This controls what hour the command will run on, and is specified in the 24 hour clock, values must be between 0 and 23 (0 is midnight)
- **dom** This is the Day of Month, that you want the command run on, e.g. to run a command on the 19th of each month, the dom would be 19.
- **month** This is the month a specified command will run on, it may be specified numerically (0-12), or as the name of the month (e.g. May)
- **dow** This is the Day of Week that you want a command to be run on, it can also be numeric (0-7) or as the name of the day (e.g. sun).
- **user** This is the user who runs the command.
- **cmd** This is the command that you want run. This field may contain multiple words or spaces.



User Management

```
$ cat /etc/passwd
```

```
sallym:x:501:501:Sally Mer:/home/sallym:/bin/csh
```

```
$ cat /etc/shadow
```

```
smithj:Ep6mckr0LChF.:10063:0:99999:7:::
```

```
$ useradd -m -G users,wheel,audio -s /bin/bash / john
```

```
$ passwd john
```