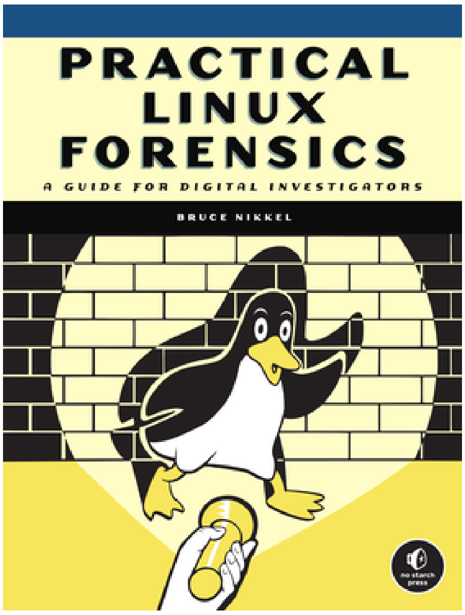
Practical Linux Forensics
A Guide for Digital Investigators: Appendix

by Bruce Nikkel

July 17, 2021



This PDF contains a list of common files and directories found on popular Linux systems together with a description for digital forensic investigators. It is an updated version of the appendix to my book *Practical Linux Forensics: A Guide for Digital Investigators*, published by Nostarch Press (2021).

Files and directories found in most Linux systems are described in two man pages: hier(7) and file-hierarchy(7). Depending on the Linux distro, local custom configuration, and installed packages, some files listed in this document may or may not exist on the forensic image you are analyzing. If you are aware of additional files that would be interesting from an investigative or forensics perspective, please email me at nikkel@digitalforensics.ch and I'll consider adding them.

The latest version of this document is published on my website: https://digitalforensics.ch/linux/

Contents

/

/	top or root directory of the system, all additional filesystems or pseudo-filesystems are mounted on a sub-directory within this tree.
./	every directory contains a dot sub-directory that refers to itself
../	every directory contains a double-dot sub-directory that refers to its parent directory
/bin/	contains executable files, often symlinked to /usr/bin/
/boot/	directory containing boot loader files (grub, etc.) and possibly the EFI mountpoint
/cdrom/	traditional generic mount point for temporarily mounted removable media such as CD or DVD discs, likely empty on a forensic image
/desktopfs-pkgs.txt /rootfs-pkgs.txt	Manjaro initial package install lists
/dev/	location of device files, usually dynamically created (and removed) by the udev daemon, likely empty on a forensic image
/etc/	directory for storing system-wide configuration data, helps reconstruct how a system was configured
/home/	the home directories of normal users on the system, contains most evidence of user activity
/initrd.img	symlink to a initial ram disk image (usually from /boot/), may also have initrd.img.old if initrd was updated
/lib32/	contains 32bit compatible libraries and executables, may be symlinked to /usr/lib32/
/lib64/	contains 64bit compatible libaries, may be symlinked to /usr/lib64/
/lib/	contains libraries and executables, often symlinked to /usr/lib/
/libx32/	contains compatible libraries and executtables for the x32 ABI (64 bit instructions, 32 bit pointers), may be symlinked to /usr/libx32/
/lost+found/	directory for orphan files (files without a parent directory) found during filesystem repair. This may exist at the root of any mounted filesystem.

/media/	directory for dynamically created mount points for removable media (USB sticks, SD cars, CD/DVD discs, etc.), likely empty on a forensic image
/mnt/	traditional generic mount point for temporarily mounted filesystems, likely empty on a forensic image
/opt/	directory containing ”optional” or add-on software
/proc/	mountpoint for a pseudo-filesystem interface for information about running processes, likely empty on a forensic image
/root/	the root user’s home directory (deliberately located outside /home/)
/run/	mountpoint for a tmpfs filesystem with runtime data, maybe symlinked with /var/run/, likely empty on a forensic image
/sbin/	contains executable files , often symlinked to /usr/sbin/ or /usr/bin (if bin and sbin have been merged)
/snap/	directory for snap software package symlinks and mount points, may be symlinked to /var/lib/snapd/snap
/srv/	directory used for storing served content (http, ftp, tftp, etc.)
/swapfile	an file-based alternative to a separate swap partition, may contain fragments of memory from the last time the system was running or a hibernation memory image
/sys/	mountpoint for a pseudo-filesystem interface to the running kernel, likely empty on a forensic image
/tmp/	mountpoint for a tmpfs filesystem for temporary files (lost on reboot), likely empty on a forensic image
/usr/	intended to be a directory of read-only files that can be shared by multiple systems, today mostly contains static files from installed packages
/var/	directory for storing variable system and application data, normally persistant across reboots, contains evidence stored in log files
/vmlinuz	symlink to a kernel image (usually from /boot/), may also have vmlinuz.old if kernel was updated

/boot/

/boot/amd-ucode.img	AMD CPU microcode updates (archive containing files)
/boot/cmdline.txt	kernel parameters on Raspberry PI
/boot/config-*	kernel configuration
/boot/initramfs.*	initial RAM disk (archive containing files)
/boot/initrd.*	initial RAM disk (archive containing files)
/boot/intel-ucode.img	Intel CPU microcode updates (archive containing files)
/boot/System.map-*	kernel symbol table
/boot/vmlinuz-*	Linux kernel image file

/boot/grub/

/boot/grub/custom.cfg	additional GRUB customization
/boot/grub/grub.cfg	GRUB configuration file (can also be in the EFI/ directory)
/boot/grub/grubenv	GRUB Environment Block, 1024 bytes fixed size
/boot/grub/i386-pc/	32bit GRUB modules
/boot/grub/ /boot/grub2/	GRUB directory for boot loader files
/boot/grub/x86_64-efi/	64bit GRUB modules

/boot/loader/

/boot/loader/	systemd's boot loader (systemd-boot, formerly gummiboot)
/boot/loader/loader.conf	overall systemd-boot configuration
/boot/loader/entries/*.conf	boot entries configuration files

EFI/

EFI/	EFI System Partition (ESP), FAT filesystem, typically mounted on /boot/efi/ or /efi/
EFI/BOOT/BOOT64.EFI EFI/BOOT/BOOTX64.EFI	a common default 64-bit EFI boot loader
EFI/BOOT/BOOTIA32.EFI	common default 32-bit EFI boot loader
EFI/fedora/ EFI/ubuntu/ EFI/debian/	examples of distro-specific EFI directories
EFI/*/grubx64.efi	GRUB's EFI boot loader

EFI/*/shim.efi EFI/*/shimx64.efi EFI/*/shimx64-fedora.efi	signed binaries for secure boot

/etc/

/etc/.updated	systemd may create this file on update, it contains a timestamp
/etc/lsb-release /etc/machine-info /etc/release /etc/version /etc/*.release /etc/*-release /etc/*_version	information about the installed Linux distro
/etc/abrt/	automated bug reporting tool configuration
/etc/acpi/	ACPI events and handler scripts
/etc/adduser.conf	configuration file for adduser and addgroup commands
/etc/adjtime	information about hardware clock and drift
/etc/aliases /etc/aliases.d/	email address alias files
/etc/alternatives	configuration of alternative commands
/etc/anaconda/	Fedora installer configuration
/etc/apache2/	apache webserver configuration
/etc/apparmor.d/	apparmor configuration and profiles
/etc/apport/	Ubuntu crash reporter configuration
/etc/appstream.conf	AppStream universal package manager configuration
/etc/apt/	Debian APT configuration
/etc/audit/audit.rules /etc/audit/rules.d/*.rules	Linux audit system rules
/etc/authselect/	Fedora authselect configuration
/etc/autofs/ /etc/autofs.*	configure auto mounting filesystems on demand
/etc/avahi/	avahi (zero-conf) daemon configuration
/etc/bash.bash_logout	bash shell system wide logout script
/etc/bashrc /etc/bash.bashrc	bash shell system wide login script
/etc/binfmt.d/*.conf	configure additional binary formats for executables at boot
/etc/bluetooth/*.conf	Bluetooth configuration files
/etc/ca-certificates/ /etc/ca-certificates.conf	system wide certificate authorities (trusted and blocked)

/etc/casper.conf	config file for initramfs-tools to boot live systems
/etc/chrony*	configuration for Chrony alternative time sync daemon
/etc/conf.d/	Arch Linux config files
/etc/cron*	cron scheduling configuration
/etc/crontab /etc/anacrontab /etc/cron.*	sheduled cron jobs
/etc/crypttab	specifies how to mount cryptographic filesystems
/etc/ctdb/	Manjaro's crash handler configuration
/etc/cups/	CUPS printer configuration files
/etc/dbus-1/	D-Buse configuration (system and session)
/etc/dconf/	dconf configuration database
/etc/debconf.conf	the Debian configuration system
/etc/default/	default configuration files for various daemons and subsystems
/etc/defaultdomain	default NIS domainname
/etc/deluser.conf	config file for deluser and delgroup commands
/etc/dhclient*.conf /etc/dhcp*	configure DHCP
/etc/dnf/	Fedora DNF package management configuration
/etc/dnsmasq.conf /etc/dnsmasq.d/	settings for DNSMasq DNS and DHCP server
/etc/dpkg/	Debian configuration settings
/etc/dracut.conf /etc/dracut.conf.d/	Dracut config for creating initramfs image
/etc/environment /etc/environment.d/	set environment variables for systemd user instance
/etc/ethertypes	Ethernet frame types
/etc/exports	NFS filesystem exports
/etc/fake-hwclock.data	contains a recent timestamp for systems without a clock (Raspberry PIs)
/etc/firewalld/	configuration files for firewalld daemon
/etc/flatpak/	flatpak configuration and repos
/etc/fscrypt.conf	cryptgraphic file systems mounted at boot
/etc/fstab	file systems mounted at boot
/etc/ftpusers	list of forbidden ftp users
/etc/fuse3.conf /etc/fuse.conf	configure the usersspace filesystem
/etc/fwupd/*.conf	configure firmware update daemon
/etc/gconf/	GNOME2 configuration database

/etc/gdm/ /etc/gdm3/	configuration for the GNOME display manager GDM
/etc/geoclue/geoclue.conf	configuration of GeoClue geo-location service
/etc/gnupg/gpgconf.conf	default configuration of GnuPG
/etc/group /etc/group-	files with group information
/etc/gshadow	group shadow file (contains hashed passwords
/etc/hostapd/	configuratio for Linux as a WiFi access point
/etc/hostid	a unique identifier for a system
/etc/hostname	hostname defined for a system (this is not globally unqiue)
/etc/hosts	a list of hosts and matching IPs
/etc/hosts.allow /etc/hosts.deny	tcpwrappers access control files
/etc/init.d/	traditional System V init scripts
/etc/init/* /etc/rc*.d/	legacy init system
/etc/initcpio/ /etc/mkinitcpio.conf /etc/mkinitcpio.d/ /etc/initramfs-tools/*	configuration and files for initramfs creation
/etc/inittab	traditional System V init and runlevel configuration
/etc/issue /etc/issue.d/ /etc/issue.net	banners displayed during network login
/etc/iwd/	iNet Wireless Daemon configuration
/etc/linuxmint/info /etc/mintSystem.conf	Linux Mint specific information
/etc/locale.conf	contains variables defining the locale settings
/etc/locale.gen	contains list of locales to be included
/etc/localtime	symbolic link to a timezone file in /usr/share/zoneinfo/*
/etc/login.defs	system wide configuration for the login program
/etc/logrotate.conf /etc/logrotate.d/	log rotation configuration
/etc/lvm/*	Linux Volume Manager configuration and profiles
/etc/machine-id	unique identifier for the system
/etc/magic /etc/magic.mime /etc/mime.types /etc/mailcap	files that identify and associate content with programs

/etc/mail.rc	commands run by the BSD mail or mailx programs
/etc/mdadm.conf /etc/mdadm.conf.d/	Linux software RAID configuration
/etc/modprobe.d/ /modules /etc/modules-load.d/	kernel modules loaded at boot
/etc/motd	traditional Unix message of the day, displayed at login
/etc/netconfig	network protocol definitions
/etc/netctl/	netctl network manager configuration files
/etc/netgroup	NIS network groups file
/etc/netplan/	Ubuntu netplan network configuration files
/etc/network/	Debian network configuration directory
/etc/NetworkManager/system-connections/	network connections, including WiFi and VPNs
/etc/networks	associates names to IP networks
/etc/nftables.conf	common file for specifying nftables rules
/etc/nscd.conf	name service cache daemon configuration file
/etc/nsswitch.conf	name service switch configuration file
/etc/ntp.conf	Network Time Protocol configuration file
/etc/openvpn/	OpenVPN client and server configuration
/etc/ostree/* /etc/ostree-mkinitcpio.conf	OSTree versioned filesystem tree configuration
/etc/PackageKit/*	PackageKit configuration files
/etc/pacman.conf /etc/pacman.d/	Arch Linux Pacman package manager configuration
/etc/pam.conf /etc/pam.d/	Pluggable Authentication Modules (PAM)
/etc/pamac.conf	Arch Linux graphical package manager configuration
/etc/papersize /etc/paperspecs	default papersize and specifications
/etc/passwd /etc/passwd- /etc/passwd.YaST2save	files with user account information
/etc/polkit-1/	Policy Kit rules and configuration
/etc/products.d/	SUSE Zypper products information
/etc/profile /etc/profile.d/	startup file for login shells
/etc/protocols	list of protocol numbers
/etc/resolv.conf /etc/resolvconf.conf	resolver configuration files

/etc/rpm/	Redhat Package Manager configuration
/etc/rsyslog.conf /etc/rsyslog.d/*.conf	rsyslog daemon configuration
/etc/sane.d/*.conf	SANE scanner configuration files
/etc/securetty	terminals where root is allowed to login
/etc/security/	directory where packages can store security configuration
/etc/services	list of TCP and UDP port numbers with associated names
/etc/shadow /etc/shadow- /etc/shadow.YaST2save	shadowed password files (contains encrypted passwords)
/etc/shells	list of valid login shells
/etc/skel/	default files for a new user (including . files)
/etc/ssh/	Secure Shell server and client configuration
/etc/ssl/	SSL/TLS configuration and keys
/etc/sssd/	System Security Services Daemon configuration
/etc/sudoers /etc/sudoers.d/ /etc/sudo.conf	sudo configuration files
/etc/swid/	Software Identification tags
/etc/sysconfig/	system configuration files typically for Redhat or SUSE
/etc/sysctl.conf /etc/sysctl.d/	values to be read in by sysctl at boot or by command
/etc/syslog-ng.conf /etc/syslog.conf	syslog-ng and traditional syslog config files
/etc/systemd/*.conf	configuration files for systemd daemons
/etc/systemd/network/	systemd link, netdev, and network (ini-style) configuration files
/etc/systemd/system/ /usr/lib/systemd/system/	systemd unit files for system instance
/etc/systemd/user/ /usr/lib/systemd/user/ /.config/systemd/user/	systemd unit files for user instance
/etc/tcsd.conf	trouSerS trusted computing daemon config file (TPM module)
/etc/tlp.conf /etc/tlp.d/	configuration for the laptop power tool
/etc/trusted-key.key	DNSSEC trust anchor keys
/etc/ts.conf	configuration for touch screen library
/etc/udev/	systemd-udev rules and configuration
/etc/udisks2/modules.conf.d/ /etc/udisks2.conf	udisks disk manager configuration
/etc/ufw/	Uncomplicated FireWall rules and configuration

/etc/update-manager/	configuration for update-manager graphical tool
/etc/updatedb.conf	configuration for mlocate database
/etc/vconsole.conf	configuratoin file for the virtual console
/etc/wgetrc	configuration for wget tool to download files
/etc/wicked/	configuration files for SUSE wicked network manager
/etc/wireguard/	configuration files for WireGuard VPN
/etc/wpa_supplicant.conf	WPA supplicant daemon configuration file
/etc/X11/	configuration for Xorg (xinitrc, xserverrc, Xsession, etc.)
/etc/xattr.conf	owned by attr, for XFS extended attributes
/etc/xdg/	XDG system wide desktop configuration files (including autostart, user-dirs.defaults)
/etc/YaST2/*	SUSE YAST system wide configuration
/etc/yum.repos.d/	Fedora YUM repository configuration data
/etc/zsh/ /etc/zshrc /etc/zprofile /etc/zlogin /etc/zlogout	login and logout files for Z shell
/etc/zypp/	SUSE Zypper package management configuration

/home/*/

Files in this section refer to the configured users (typically people). Some of these file may also exist in /root/, the root user's home directory.

XDG and FreeDesktop directories

.cache/	non-essential persistent user cache data ($XDG_CACHE_HOME)
.config/	persistent user configuration data ($XDG_CONFIG_HOME)
.local/share/	persistent user application data ($XDG_DATA_HOME)
Documents/	office documents
Downloads/	default location for downloaded content
Desktop/	regular files and *.desktop definition files which appear on the desktop
Music/	music and audio files
Pictures/	photographs and pictures
Templates/	application templates (office docs, etc.)

Videos/	video files

.cache/

.cache/clipboard-indicator@tudmotu.com/registry.txt	clipboard history
.cache/flatpak/	user cached flatpak data
.cache/gnome-software/shell-extensions/	user installed GNOME extensions
.cache/libvirt/qemu/log/linux.log	QEMU virtual machine activity
.cache/sessions/	desktop session state data
.cache/simple-scan/simple-scan.log	scan application log (may contain file names of saved scans)
.cache/thumbnails/ .cache/thumbs-*/	cached thumbnail images
.cache/tracker/ .cache/tracker3/	GNOME search index files
.cache/xfce4/clipman/textsrc	XFCE clipboard history
.cache/*/	any other application that may cache persistent data for performance or efficiency reasons

.config/

.config/autostart/	autostarting *.desktop programs and plugins
.config/baloofilerc	Baloo desktop search configuration
.config/dconf/user	dconf user configuration database
.config/goa-1.0/accounts.conf	GNOME online accounts configuration
.config/g*rc	GNOME override configuration files beginning with g and ending with rc
.config/Jitsi Meet/	cache, state, preferences, logs, etc. from Jitsi video calls
.config/kdeglobals	KDE global override settings
.config/k*rc .config/plasma*rc	KDE/Plasma override configuration files beginning with k and ending with rc
.config/libaccounts-glib/accounts.db	KDE configured cloud account data
.config/mimeapps.list	user default applications for file types
.config/Qlipper/qlipper.ini	clipboard data (Lubuntu)
.config/session/gnome-session/	saved state of desktop and applications
.config/systemd/user/	user systemd unit files
.config/user-dirs.dirs	user defined default FreeDesktop directories
.config/xsettingsd/xsettingsd.conf	X11 settings configuration
.config/*/	any other application that may save user configuration data

.local/

.local/lib/python/site-packages	user installed python modules
.local/share/akonadi/	KDE/Plasma Akonadi personal information manager search database
.local/share/baloo/	KDE/Plasma Baloo file search database
.local/share/dbus-1/	user configured D-Bus session services
.local/share/flatpak/	user installed flatpak software packages
.local/share/gvfs-metadata/	GNOME virtual filesystem artifacts
.local/share/kactivitymanagerd/	KDE Kactivities manager
.local/share/keyrings/	GNOME keyring files
.local/share/klipper/history2.lst	KDE clipboard history
.local/share/kwalletd/	KDE Wallet files
.local/share/modem-manager-gui/	application for mobile networks (SMS)
.local/share/RecentDocuments/	*.desktop files with recent documents information
.local/share/recently-used.xbel	recently used files
.local/share/Trash/	Trash directory from the FreeDesktop.org specification
.local/share/xorg/Xorg.0.log	Xorg startup log
.local/user-places.xbel	recently visited locations
.local/cache/*/	any other application that may save data

other dot files and directories

.bash_history	bash shell history file
.bash_logout	bash shell logout script
.bash_profile .profile .bashrc	bash shell login scripts
.ecryptfs/	common default directory for encrypted Ecryptfs tree
.gnome2/keyrings/	legacy GNOME2 keyrings
.gnupg/	GnuPG directory with configuration and keys
.john/	John the Ripper password cracker
.mozilla/	Firefox browser directory, includes profiles, configuration, etc
.ssh/	Secure Shell directory with configuration, keys, known hosts
.thumbnails/	legacy thumbnail image directory
.thunderbird/ Thunderbird email client directory, includes profiles, configuration, cached emails, etc.	
.Xauthority	X11 MIT Magic Cookie file
.xinitrc	user customized X11 session startup script

.xsession-errors .xsession-errors.old	X11 current and previous session error log

/usr/

/usr/bin/ /usr/sbin/	contains executable files, symlinked if bin and sbin have been merged
/usr/games/	directory for game programs
/usr/include/	system C header (*.h) files
/usr/lib/ /usr/lib64/ /usr/lib32/ /usr/libx32/	contains libraries and executables, architecture dependent libraries in separate directories
/usr/local/ /usr/local/opt/	directories for optional add-on software packages
/usr/opt/	alternative location for add-on packages
/usr/src/	system source code

/usr/lib/

/usr/lib/	static and dynamic libraries and supporting files for system wide use
/usr/libexec/	executables for daemons and system components (not administrators)
/usr/lib/locale/locale-archive	binary file built with configured locales
/usr/lib/modules/ /usr/lib/modprobe.d/ /usr/lib/modules-load.d/	kernel modules and configuration files
/usr/lib/os-release	file containing information about installed distro
/usr/lib/python*/	system wide python modules and support files
/usr/lib/sysctl.d/	default sysctl configuration files
/usr/lib/udev/	udev support files and rules (rules.d/)
/usr/lib/tmpfiles.d/	configuration for temporary files and directories

/usr/lib/systemd/

/lib/systemd/system/	default system unit files
/lib/systemd/user/	default user unit files
/usr/lib/systemd/*generators*/	generator programs to create unit files
/usr/lib/systemd/network/	default network, link, netdev files
/usr/lib/systemd/systemd*	systemd executables

/usr/local/, /usr/opt/

/usr/local/	directory was the traditional Unix location for locally installed binaries, and not from a network mounted directory. Linux systems may use it for add-on packages.
/usr/local/bin/ /usr/local/sbin/	local binaries
/usr/local/etc/	local configuration
/usr/local/doc/ /usr/local/man/	local documentation and man pages
/usr/local/games/	local games
/usr/local/lib/ /usr/local/lib64/ /usr/local/libexec/	associated local files
/usr/local/include/ /usr/local/src/	header files and source code
/usr/local/share/	architecture independent files

/usr/share/

/usr/share/	files shared between software packages or different architectures
/usr/share/dbus-1/	default system and session D-Bus configuration data
/usr/share/factory/etc/	initially installed defaults of some /etc/ files
/usr/share/hwdata/pci.ids	list of PCI vendors, devices, and subsystems
/usr/share/hwdata/usb.ids	list of USB vendors, devices, and interfaces
/usr/share/hwdata/pnp.ids	list of product vendor name abbreviations
/usr/share/i18n/ /usr/share/locale/	internationalization data
/usr/share/metainfo/	XML files with Appstream metadata
/usr/share/polkit-1/	PolicyKit rules and actions
/usr/share/zoneinfo/	time zone data files for different regions
/usr/share/accounts/	service and provider files for KDE online accounts
/usr/share/doc/	software package supplied documentation
/usr/share/help/	GNOME help files with translations
/usr/share/man/	man pages with translations
/usr/share/src/ /usr/share/include/	source code, C header (*.h) files

/var/

/var/backups/	Debian backup data of packages, alternatives, passwd/group files
/var/games/	variable data from installed games, may contain high-score files with names and dates
/var/local/	variable data for software installed in /usr/local/
/var/opt/	variable data for software installed in /usr/opt/
/var/run/	runtime data, usually empty on a forensic image
/var/tmp/	temporary files, persistent across boots
/var/crash/	crash dumps, stack traces, and reports
/var/mail/	locally spooled email (some distros like Ubuntu and Fedora don’t setup a mail subsystem by default anymore)
/var/www/	a default location for storing html pages
/var/db/sudo/lectured/	empty files indicating a user has been ”lectured” about using sudo

/var/cache/

/var/cache/	persistent cached system-wide data
/var/cache/apt/	cached downloads of Debian packages
/var/cache/cups/	CUPS printing system
/var/cache/cups/job.cache	print job cache with file names, timestamps, printer names
/var/cache/cups/job.cache.*	rotated versions of job.cache
/var/cache/debconf/	system wide cached Debian data
/var/cache/debconf/passwords.dat	contains system generated passwords
/var/cache/dnf/	system wide cached Fedora DNF package data
/var/cache/PackageKit/	Distro-independent system wide cached PackageKit package data
/var/cache/pacman/	system wide cached Arch Linux Pacman package data
/var/cache/snapd/	system wide Ubuntu SNAP package cached data
/var/cache/zypp/	system wide cached SuSe Zypper package data

/var/log/

/var/log/alternatives.log	Debian alternative command name system
/var/log/anaconda/	Fedora Anaconda initial installer logs

/var/log/apache2/	default apache webserver logs
/var/log/apport.log	Ubuntu crash handling system log
/var/log/apt/	Debian APT package manager logs
/var/log/aptitude	Debian Aptitude actions logged
/var/log/archinstall/install.log	Arch Linux initial install log
/var/log/audit/	Linux Audit system logs
/var/log/boot.log	Plymouth Splash console output
/var/log/btmp	log of failed (bad) login attmpts
/var/log/Calamares.log	Calamares initial installation log
/var/log/cups/	CUPS printing system access, error, and page logs
/var/log/daemon.log	common syslog file for daemon related logs
/var/log/	default location for system wide log files
/var/log/dmesg	log of kernel ring buffer
/var/log/dnf.log	Fedora DNF package manager logs
/var/log/dpkg.log	Debian dpkg package manager logs
/var/log/firewalld	firewalld daemon logs
/var/log/hawkey.log	Fedora Anaconda log
/var/log/installer/	Debian initial installer logs
/var/log/journal/	systemd journal logs (system and user)
/var/log/kern.log	common syslog file for kernel related logs (ring buffer)
/var/log/lastlog	log of last logins with origin information
/var/log/lightdm/	Lightdm display manager logs
/var/log/mail.err	common syslog file for mail related errors
/var/log/messages	traditional Unix log file with syslog messages
/var/log/mintsystem.log, mintsystem.timestamps	Linux Mint specific logs
/var/log/openvpn/	Open VPN system logs
/var/log/pacman.log	Arch Linux Pacman package manager logs
/var/log/sddm.log	SDDM display manager log
/var/log/tallylog	PAM tally state file for failed login attempts
/var/log/ufw.log	Uncomplicated FireWall logs
/var/log/updateTestcase-*/	SUSE bug report data
/var/log/wtmp	traditional system login records
/var/log/Xorg.0.log	Xorg startup log
/var/log/YaST2	SUSE YaST logs
/var/log/zypper.log	SUSE Zypper package manager logs
/var/log/zypp/history	SUSE Zypper package manager history
/var/log/*	other logs created by applications or system components

/var/lib/

/var/lib/	persistent variable data for installed software
/var/lib/abrt/	automated bug reporting tool data
/var/lib/AccountsService/icons/*	user's choosen login icons
/var/lib/AccountsService/users/*	user's default or last session login settings
/var/lib/alternatives/	symlinks to alternative command names
/var/lib/bluetooth/	bluetooth adapters and paired bluetooth devices
/var/lib/ca-certificates/	system wide CA certificate repository
/var/lib/dnf/	Fedora DNF install package information
/var/lib/dpkg/ /var/lib/apt/	Debian installed package information
/var/lib/flatpak/	Flatpak installed package information
/var/lib/fprint/	fingerprint reader data, including enrolled user fingerprints
/var/lib/gdm3/	GNOME3 display manager settings and data
/var/lib/iwd/	iNet Wireless Daemon, including access point information, passwords
/var/lib/lightdm/	Lightdm display manager settings and data
/var/lib/linuxmint/mintsystem/	Linux Mint system wide settings
/var/lib/mlocate/mlocate.db	file database for the locate search command
/var/lib/NetworkManager/	Network Manager data, including leases, bssid's, and more
/var/lib/PackageKit/	PackageKit transactions.db
/var/lib/pacman/	Arch Linux pacman data
/var/lib/polkit-1/	Policy Kit data
/var/lib/rpm/	RPM sqlite package database
/var/lib/sddm/	SDDM display manager data
/var/lib/selinux/	SELinux modules, locks, and data
/var/lib/snapd/	Ubuntu installed SNAP package information
/var/lib/systemd/	system wide systemd data
/var/lib/systemd/coredump/	systemd core dump data
/var/lib/systemd/pstore/	crash dump data saved by pstore
/var/lib/systemd/timers/	systemd timer unit files
/var/lib/systemd/timesync/clock	empty file, mtime can be used to set approx time on systems without a hardware clock
/var/lib/ucf	Update Configuration File data
/var/lib/upower/	power history files (charging/discharging on laptops)
/var/lib/whoopsie/whoopsie-id	unique identifier for crash data sent to Ubuntu/Canonical servers
/var/lib/wicked/	wicked network manager data
/var/lib/YaST2/	SUSE YAST configuration data

/var/lib/zypp/AnonymousUniqueId	unique identifier for contacting SUSE servers
/var/lib/zypp/	SUSE Zypper package manager data

/var/spool/

/var/spool/	location for daemons using a spool directory for jobs
/var/spool/abrt/ /var/tmp/abrt	crash reporting data sent to Fedora
/var/spool/at/	scheduled at jobs to run
/var/spool/cron/ /var/spool/anacron/	scheduled cron jobs to run
/var/spool/cups/	CUPS printing spool directorp
/var/spool/lpd/	traditional line printer daemon spool directory
/var/spool/mail/	see /var/mail/