Identify File System:

lsblk -f	CentOS systems
df -Th	Docker with Ubuntu installedv(Noisy)
lsblk -f	For Ubuntu Less Noisy

Fdeadbox forensics, you have options like	
cat /etc/fstab	filesystem table,

Identify Timestamp:

File Copy

- FILE MAC times change to time of file copy
- DIRECTORY MC times change to time of file copy

File Move

- FILE C time changes to time of move
- DIRECTORY MC times changes to time of move

Key Directories of Linux:

/sbin		stores executable files typically used by the system administrator. Examples include fdisk and shutdown
/bin	/usr/bin	holds the executable files user-commands, such as ls, grep
/etc		configuration data for applications and startup/shutdown shell scripts
/dev	/dev/sda1	Mounted disks appear here
/mnt		traditionally used to mount additional filesystems
/var	/var/log	contains files which are expected to change size significantly
/tmp		Temporary files
/usr	/usr/bin /usr/sbin /usr/lib	Location commands user's generally run. less, awk, sed etc files run by administrators (cron, useradd etc.) executables which aren't directly invoked.
/home		where most "personal" data and files are stored.

/lib		shared objects used by executable files in /bin and /sbin (and /usr/bin & /usr/sbin)
/opt		Optional/Add-on files
/media		Removable media devices, hold USB devices, CD/DVD
/srv		Service data, location related to running services

Log File Location:

/var/log/: Main directory for system logs.

/var/run/: Contains volatile data for live systems

CentOS/RHEL;

/var/log/messages	general system messages, including some authentication events.
/var/log/secure:	contains authentication and authorization logs, including su

Ubuntu systems

/var/log/syslog	records a wide range of system activities
/var/log/auth.log:	stores user authorization data, including SSH logins

Authentication and Authorization Logs

/var/log/secure	(CentOS/RHEL)
/var/log/auth.log	(Ubuntu)

Binary Login Logs

/var/run/utmp	users and sessions currently logged in
/var/log/wtmp	Contains historical data of login sessions.
/var/log/btmp	Logs failed login attempts.

Note: The utmp file is located in /var/run/, which is volatile and only exists on live systems.

Viewing Binary Login Files
last -f /var/run/utmp
last -f /var/log/wtmp
last -f /var/log/btmp

convert binary log files into human-readable format
utmpdump /var/run/utmp
utmpdump /var/log/wtmp
utmpdump /var/log/btmp

Note: Using **lastb** to view the btmp file can quickly provide a summary of failed login attempts.

Last and faillog

lastlog: **Reads the lastlog file, showing the last login for each user.**

lastlog	
lastlog -u <username>	# For a specific user

faillog: **Reads the faillog, showing failed login attempts.**

faillog -a	# View all failed logins
faillog -u <username>	# Specific user account

Audit Logs:

Directory: **/var/log/audit/audit.log**

Audit configuration: **/etc/audit/rules.d/audit.rules**

- **ausearch:** A powerful tool for searching specific terms

ausearch -f <file-name>	# Search events related to a file
ausearch -p <pid>	# Search events related to a process ID
ausearch -ui <user-id>	# Search events related to a specific user

- **aureport: I***t's less granular than ausearch but provides a broader view that can help identify unusual behavior.*

Application Logs

/var/log/apache2 /var/log/httpd /var/log/nginx	Webserver (Apache/HTTPd/Nginx)
/var/log/mail	Mail Server
/var/log/mysqld.log /var/log/mysql.log /var/log/mariadb/*	Database

- /var/log/apache2 (Ubuntu)
- /var/log/httpd (CentOS)
- /var/log/nginx (for Nginx servers)

Example Commands for Webserver Log Analysis

Command will display a count of unique pages requested, making it easy to spot anomalies or repeated access to specific files.

- `cat access_log* | cut -d '"' -f2 | cut -d ' ' -f2 | sort | uniq -c | sort -n`

filter all POST requests, which can be indicative of webshells or exploits that use POST to upload or execute files.

- `cat access_log* | cut -d '"' -f6 | sort | uniq -c | sort -n`

Key Directories:

Authentication Logs	Check auth.log, secure, utmp, wtmp, and btmp for failed logins.
/etc/passwd	Review user accounts, modification times, and shell access.
/etc/shadow	Check for unexpected accounts and modification times.
/etc/group	Review group membership for privileged accounts **(Wheel, Sudo, Adm).**
/etc/sudoers	Validate modification times and check for users with excessive privileges.
/etc/sudoers.d/	Same as /etc/sudoers—attackers prefer this location as it survives system updates.

SSH Keys

- **/home/(username)/.ssh/** and **/root/.ssh/** contain default SSH key locations.
- known_hosts helps identify lateral movement.
- authorized_keys shows evidence of backdoor access.

History files to investigate

.bash_history	commands issued in the Bash shell. Other shells may store history elsewhere and the actual location of this file is stored in the $HISTFILE variable
.lesshst	record of any searches or shell commands issued while running less. this can maintain a record of users or attackers searching through files for specific strings or, in the case of restricted shells, attempting shell escapes.
.viminfo	This file contains the command line, search string and input-line history from any vi or vim invocations. It also contains references to file locations, buffer lists and key variables.
.mysql_history	Any commands line MySql activity is stored in this file.

Other Potential History Files

- .python_history
- .gdb_history

- .wget-hsts
- .local/share/nano/search_history

Alternative Shells and History Files

Zsh History: **Kali and Parrot**

Stored in ~/.zsh_history

fc -lf	Lists the most recent commands from the history
fc -li 100	Lists the history starting from the 100th command
history	search your command history in Linux

Use Grep to get search for particular commands example:

Search for sudo commands: *(history | grep sudo)*

Networking Data Collection in IR

Key Networking Files

/etc/hosts	Contains local IP resolution data. Attackers may modify this file to reroute hostnames or disguise C2 IP addresses.
/etc/resolv.conf and **/etc/systemd/resolved.conf**	Check the DNS resolution configurations for suspicious changes, especially invalid nameservers.

Useful Networking Commands

lsof -Pni	(Live response only) Files with network connections
netstat -nap	(Live response only) displays network connection data.
route	Live response only) displays the kernel routing table.
arp -a	(Live response only) returns the arp table on the system.

Running Processes

ps -auxww	command to list processes
/proc directory	more details on running processes

Persistence Techniques:

1. **Services:**

System V Configurations (Older Systems)

/etc/inittab	manage startup processes
/etc/init.d/ and /etc/rc.d/	store startup scripts that run services when the system boots.

Systemd Configurations

/etc/systemd/system/	directory holds system-wide configuration files for services
/usr/lib/systemd/user/ & /usr/lib/systemd/system/	store service files

2. **Cron Jobs:**

/etc/cron.d/
/etc/crontab
/etc/cron.hourly/
/etc/cron.daily/
/etc/cron.weekly/
/etc/cron.monthly/

3. **Start-Up Scripts**

/etc/init.d/
/etc/rc(x).d/
/etc/systemd/system/
/usr/lib/systemd/user/
/usr/lib/systemd/system/

Useful commands:

- systemctl list-unit-files: Default on CentOS & Ubuntu.
- chkconfig –list: For System V systems.

Hidden Files

Hidden files are another method attackers use to conceal backdoors. Files with a leading **. in their name**, such as .evil, are hidden from default views

Command to search for hidden directories:

```
find / -type d -iname '.*' -exec ls -alht {} \; 2>/dev/null
```

Validating SSH Access

/var/log/auth.log or /var/log/secure	Investigate SSH logs for failed login attempts followed by successful logins,
/etc/ssh/sshd_config	unusual modifications that might have been made to weaken security

File Modifications

find / -type f -size +1G	Look for large files (often staged for exfiltration)
find /dev -type f	/dev folder should only contain device files or symbolic links.
find / -type f -newermt YYYY-MM-DD ! -newermt YYYY-MM-DD	looks for files modified in given time

Log Data Collection

Primary Logs to Examine:

Apache/httpd Logs	Look for unusual requests, especially ones that may indicate scanning or exploitation attempts
Audit Logs	These capture all system-level events, and you can check for unusual file accesses, command executions, or authentication failures.
/var/log/secure	Focus on **sudo** usage, SSH authentications, and any failed login attempts
/var/log/messages	Check for system errors, warnings, and notifications that may indicate misconfigurations or exploits.
/var/log/auth.log	Focus on user authentication attempts, including both failed and successful ones.

Quick Wins (Log-Based Indicators):

Sudo Use and Command Execution	grep 'sudo' /var/log/secure.
User Authentication:	grep 'Failed password' /var/log/auth.log.
Unusual Notifications or Warnings:	grep 'warning' /var/log/messages.
Audit Logs for Commands Issued:	ausearch -m execve.

Additional Logs to Consider:

Mail Logs	var/log/maillog or /var/log/mail.log	identify if malicious actors are sending spam or phishing emails.
Firewalld Logs	/var/log/firewalld	Look for changes or violations in firewall rules
IPTables Logs	/var/log/syslog	unexpected firewall rule modifications.
UFW Logs (Uncomplicated Firewall on Ubuntu)	/var/log/ufw	sudden allow/deny actions that are unusual for the environment.
Samba Logs	/usr/local/samba/var/smbd.log or /var/log/samba/smbd.log	Useful if you're in a mixed Windows/Linux environment, especially for tracking lateral movement via file shares.