CBS322 Digital Forensics

FINAL PROJECT

Group 2

Sudipto Das 2022BCY0007

Imtiaz 2022BCY0006

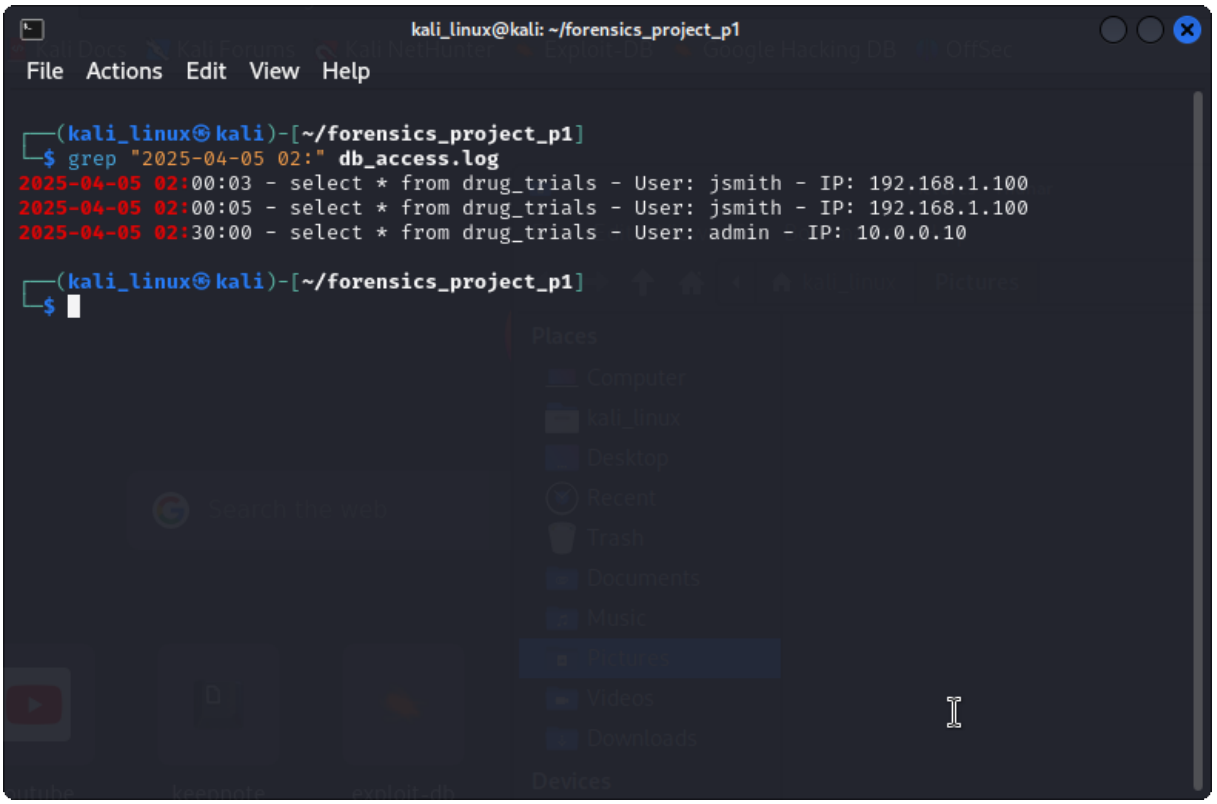
Mokshith 2022BCY0004

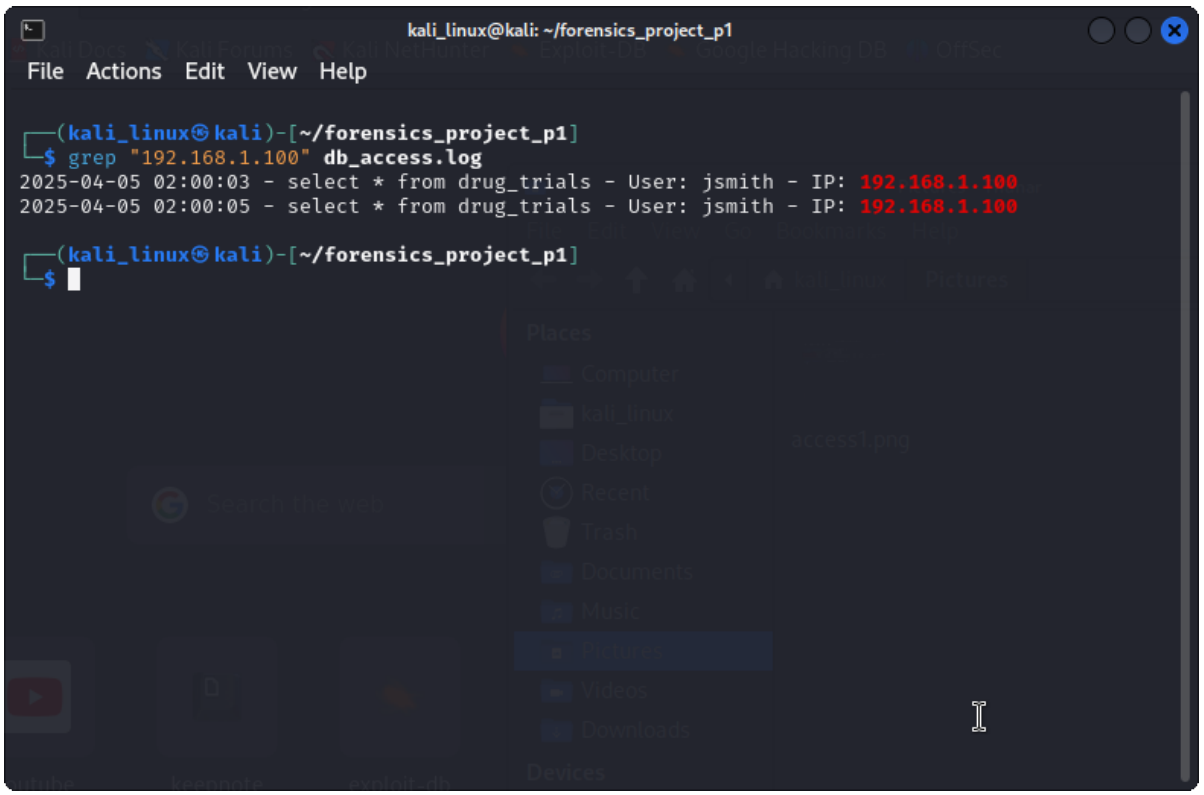
Problem Statement: A major pharmaceutical company is on the verge of releasing a groundbreaking drug, but sensitive research data is stolen from their servers and leaked to a competitor. The company hires a digital forensics expert to investigate the breach, recover the stolen data, and identify the culprit. The expert uncovers evidence of an insider threat—a disgruntled employee who used a combination of phishing attacks and privilege escalation to exfiltrate the data.

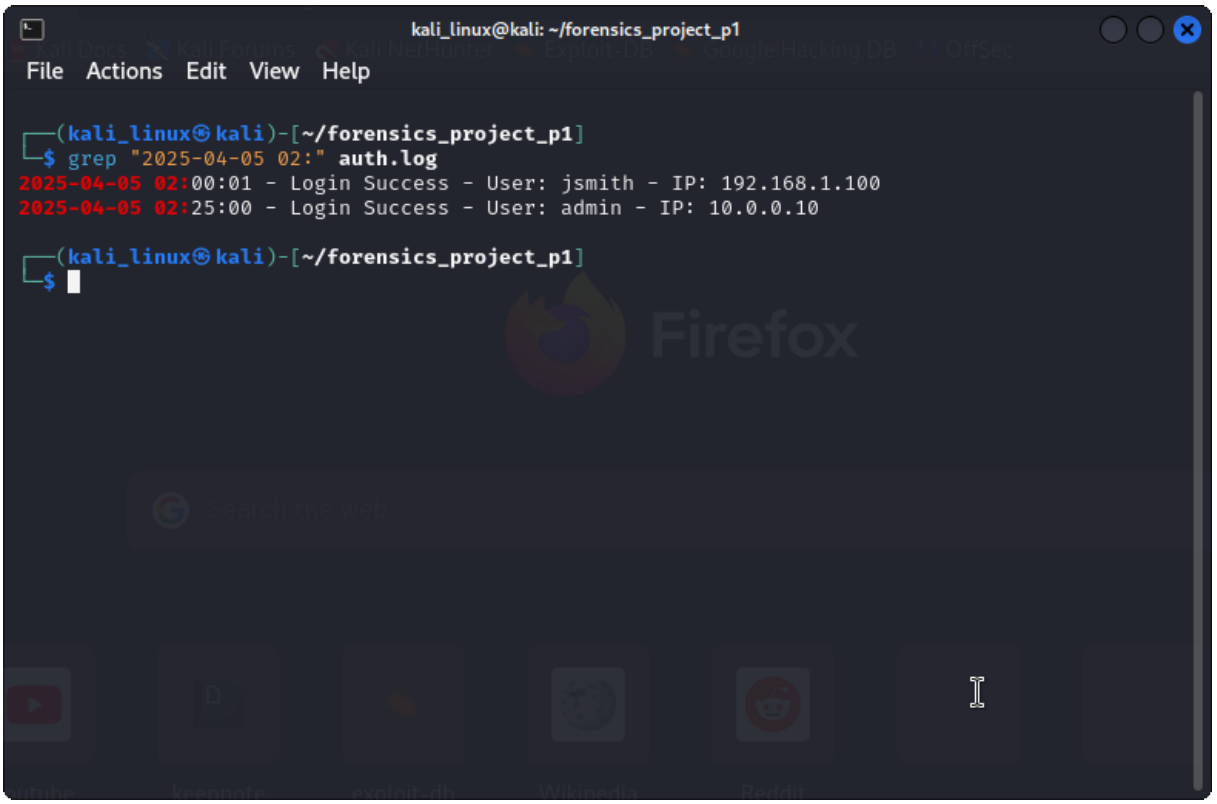
Phase 1: Initial Discovery of the Breach

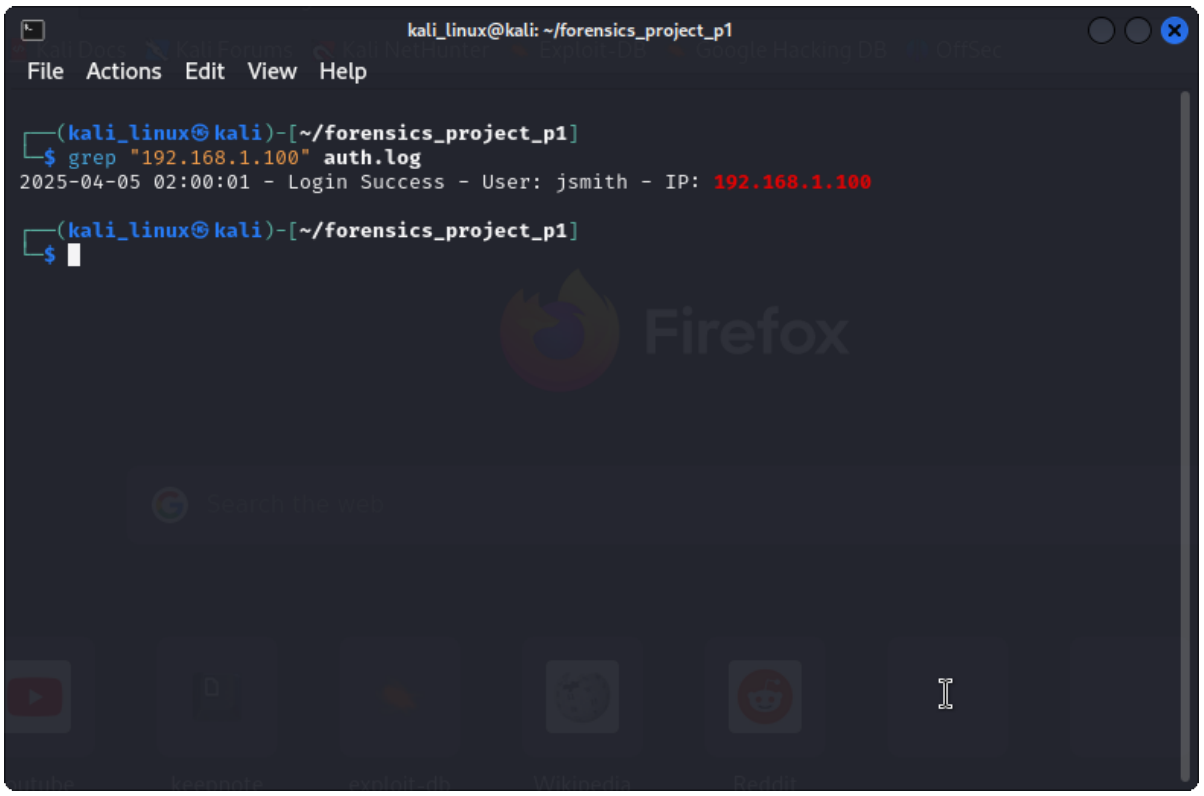
Plot Point: The pharmaceutical company discovers the data breach when a competitor announces a suspiciously similar drug. The digital forensics expert is hired to investigate.

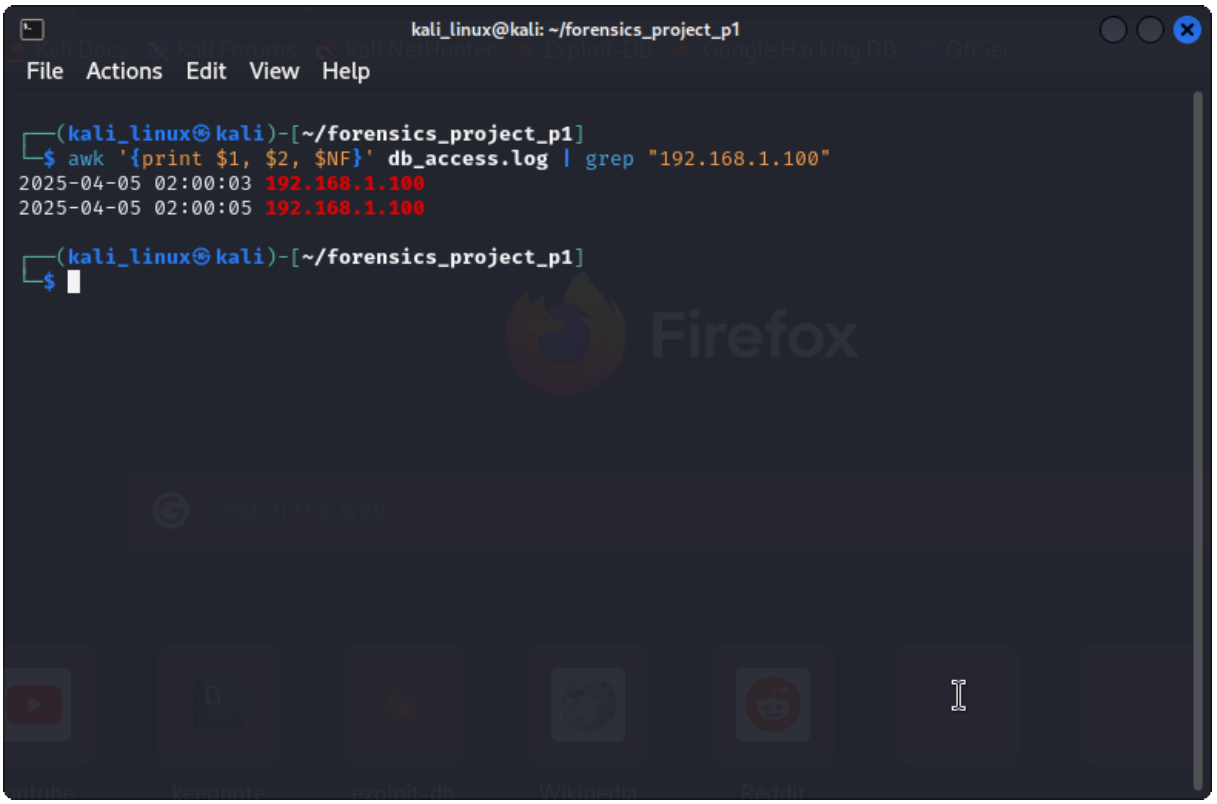
The investigator sat in the server room, the glow of the monitor casting shadows across the racks of humming machines. Opening Splunk, they filtered the database access logs by timestamp, narrowing the search to the night of the suspected breach. There it was—a series of queries executed at 2:03 AM, pulling every record from the drug trials database. Cross-referencing the authentication logs, they found the login: jsmith—an employee account. But the source IP address, 192.168.1.100, didn't match any company device. "This wasn't remote access," the investigator muttered. "Someone was inside the network."

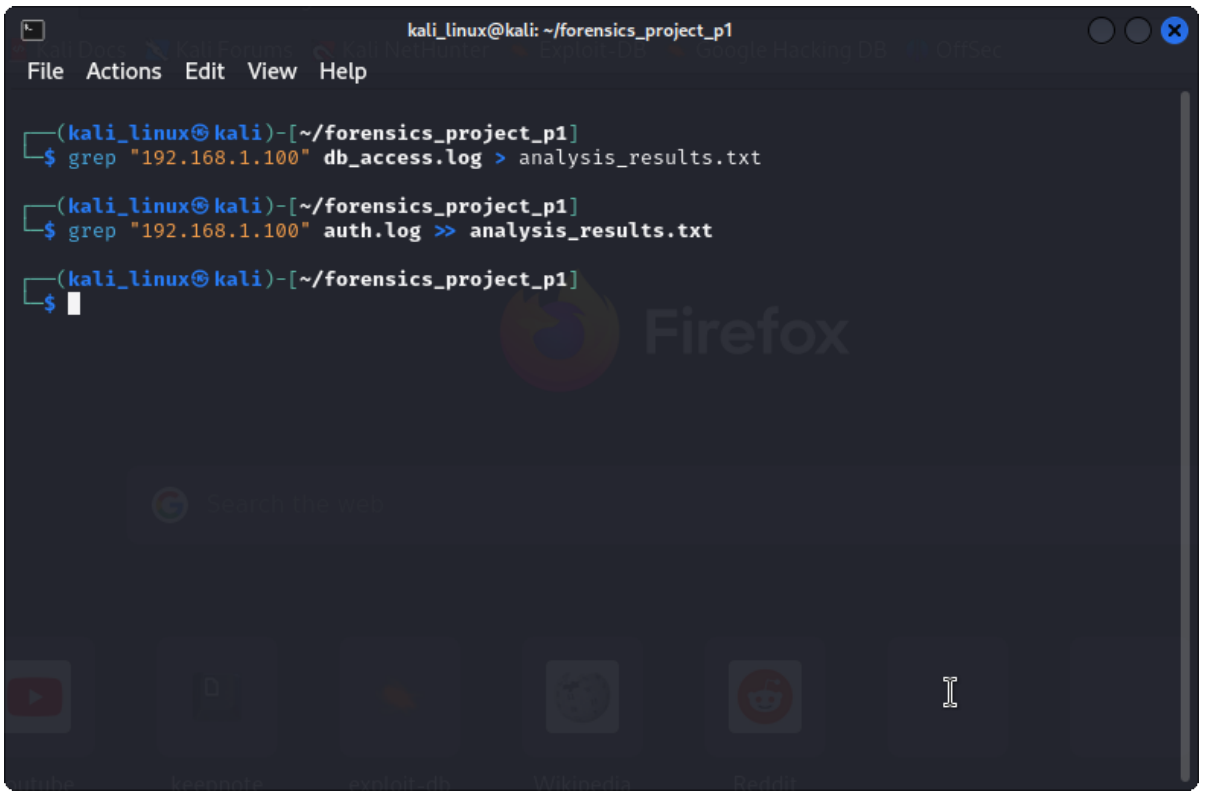

kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ grep "2025-04-05 02:" db_access.log
2025-04-05 02:00:03 - select * from drug_trials - User: jsmith - IP: 192.168.1.100
2025-04-05 02:00:05 - select * from drug_trials - User: jsmith - IP: 192.168.1.100
2025-04-05 02:30:00 - select * from drug_trials - User: admin - IP: 10.0.0.10
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$

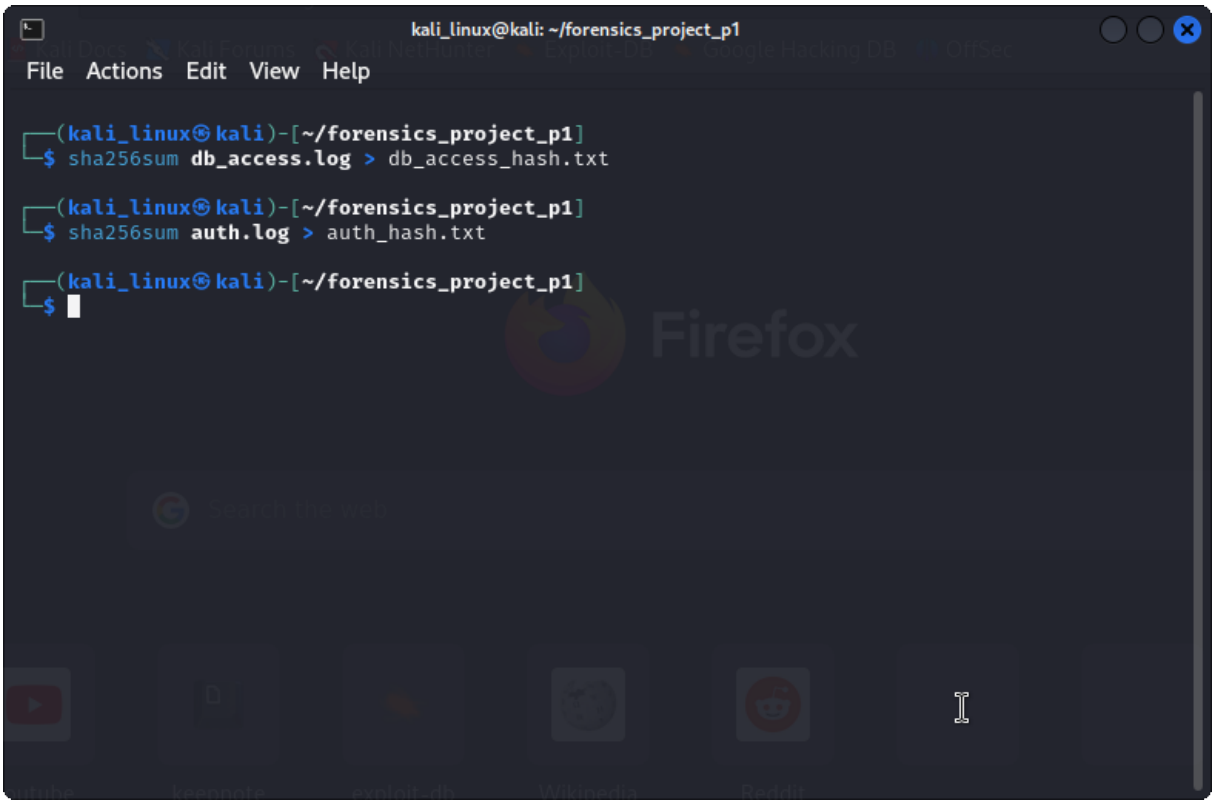

kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ grep "192.168.1.100" db_access.log
2025-04-05 02:00:03 - select * from drug_trials - User: jsmith - IP: 192.168.1.100
2025-04-05 02:00:05 - select * from drug_trials - User: jsmith - IP: 192.168.1.100
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$

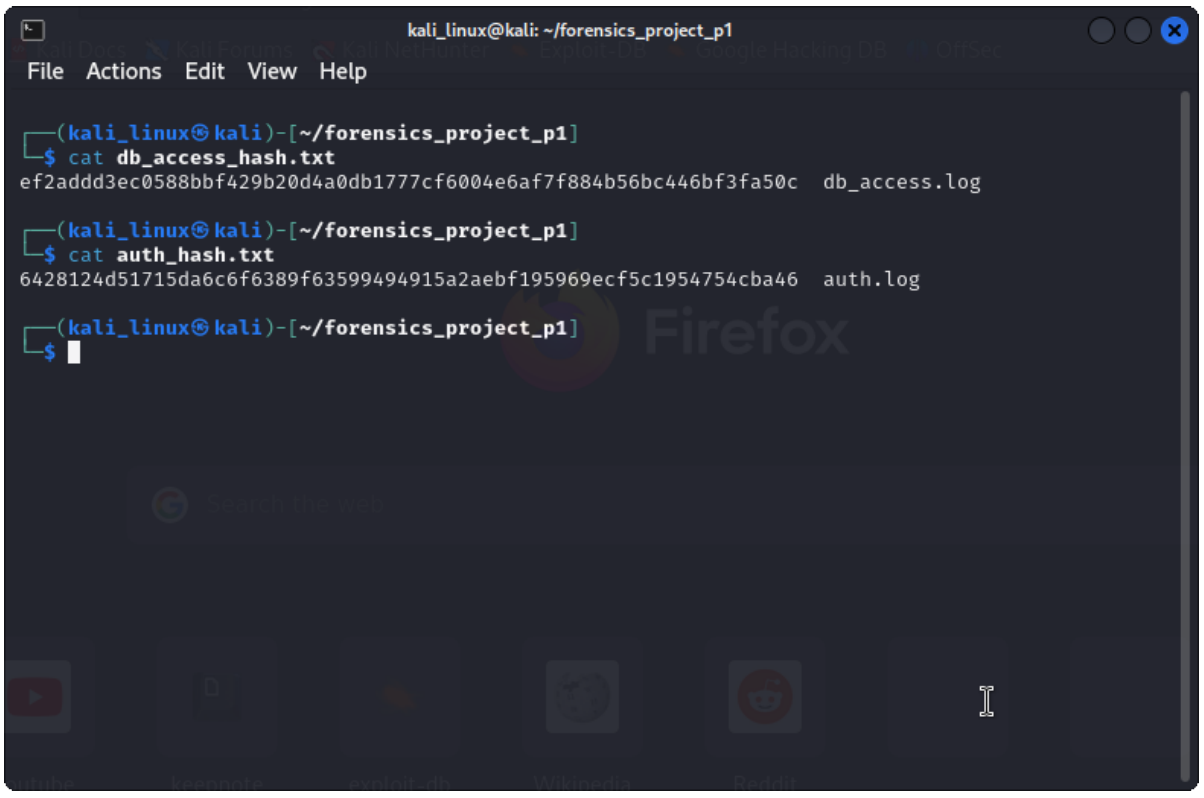

kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ grep "2025-04-05 02:" auth.log
2025-04-05 02:00:01 - Login Success - User: jsmith - IP: 192.168.1.100
2025-04-05 02:25:00 - Login Success - User: admin - IP: 10.0.0.10
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$

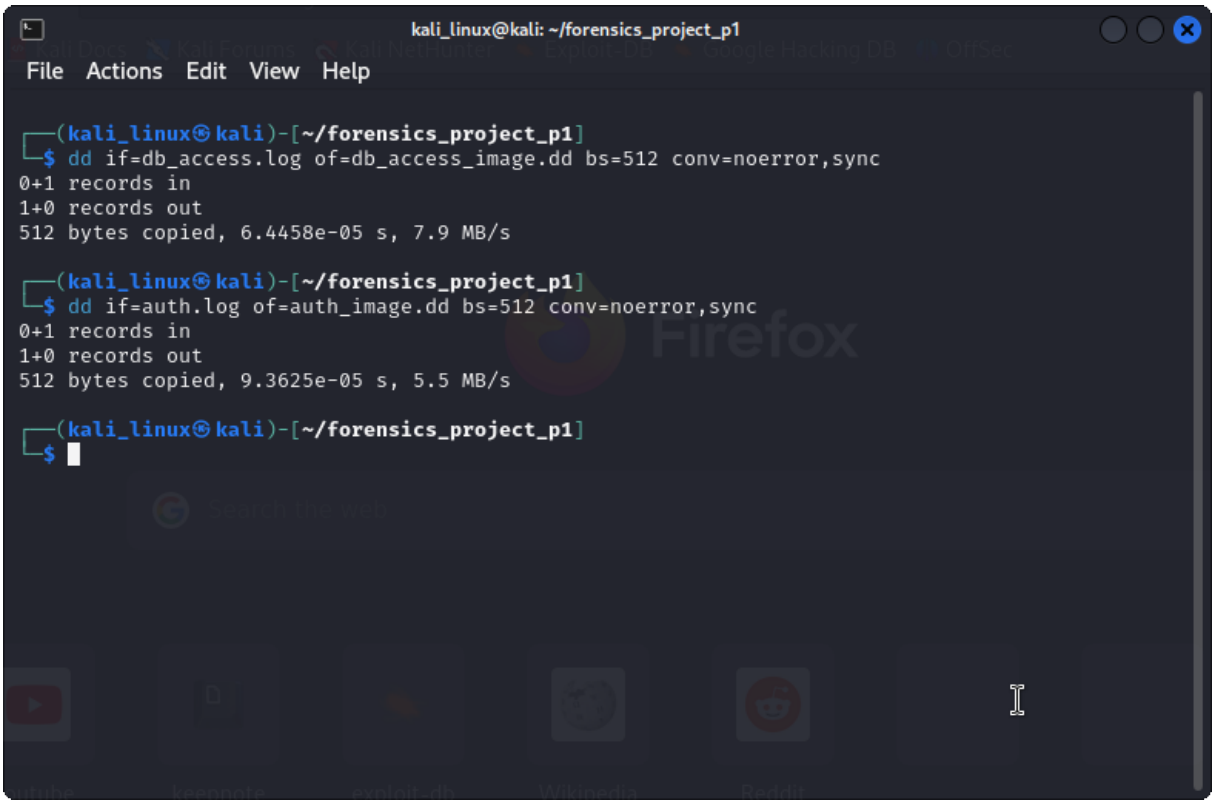

kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ grep "192.168.1.100" auth.log
2025-04-05 02:00:01 - Login Success - User: jsmith - IP: 192.168.1.100
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$

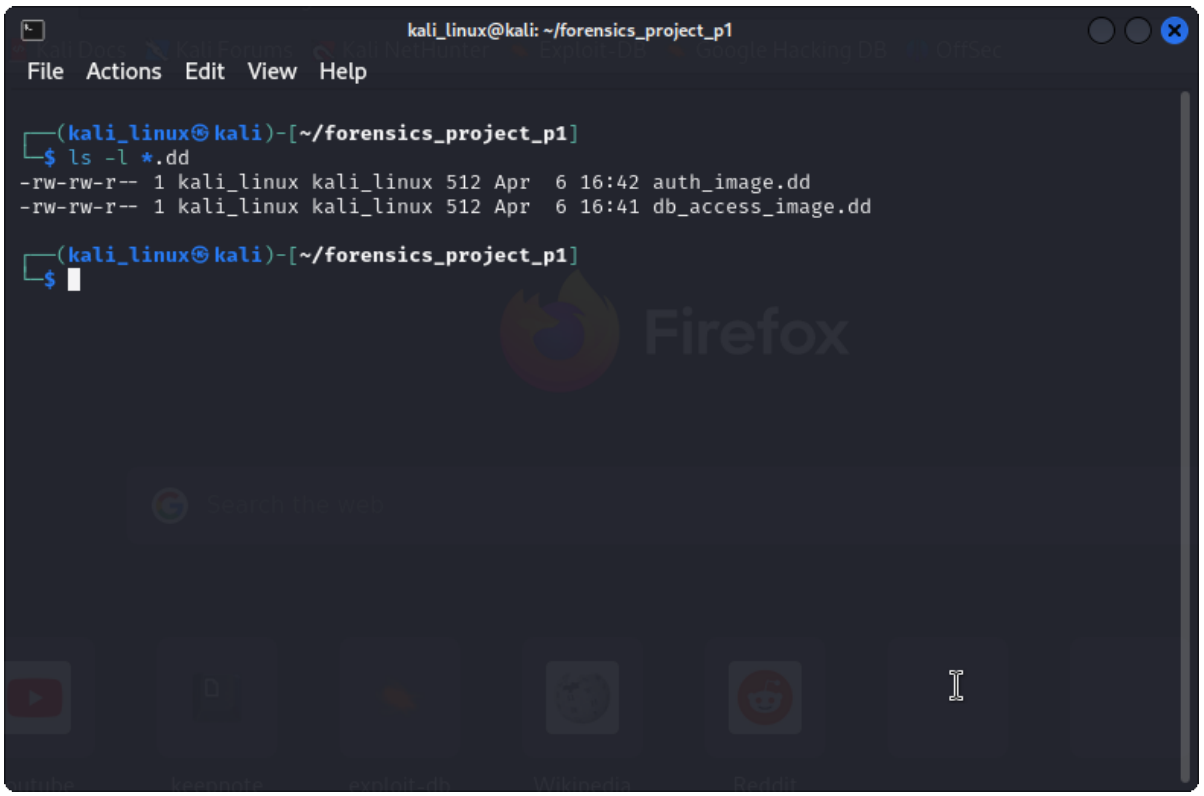

kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ awk '{print $1, $2, $NF}' db_access.log | grep "192.168.1.100"
2025-04-05 02:00:03 192.168.1.100
2025-04-05 02:00:05 192.168.1.100
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$

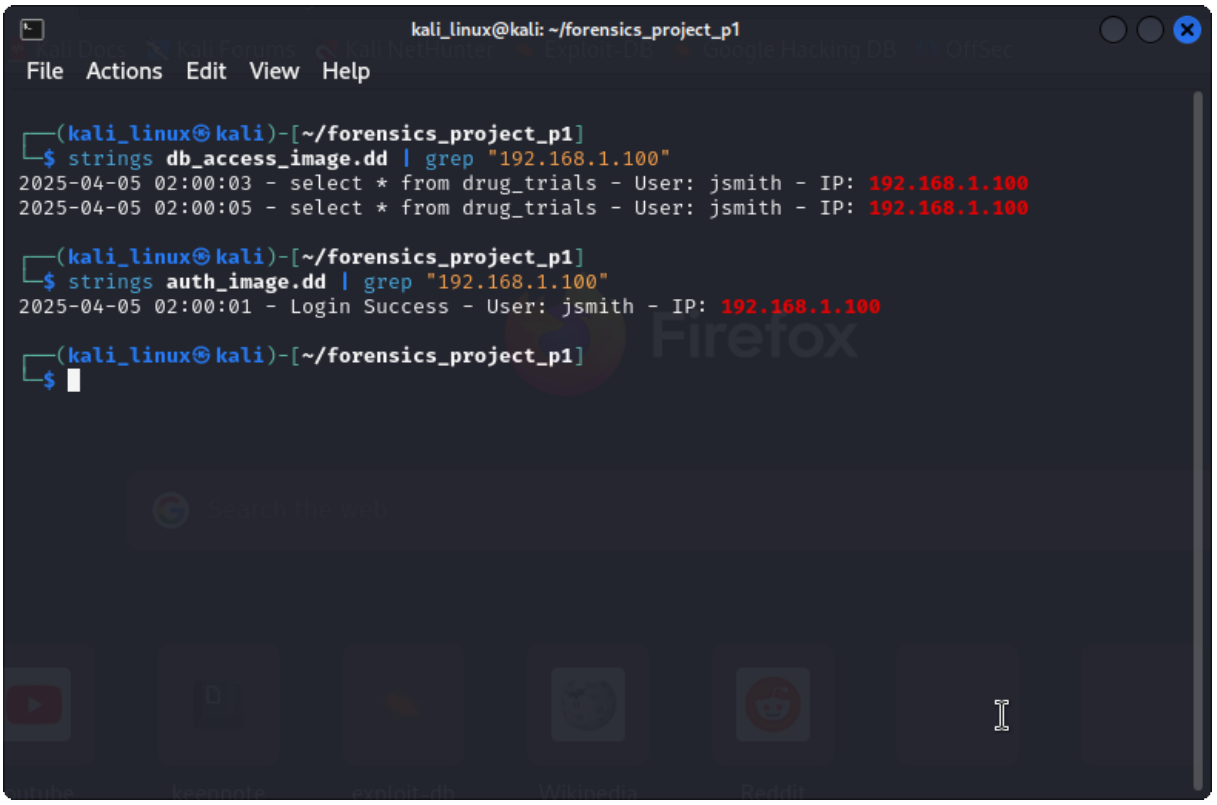

kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ grep "192.168.1.100" db_access.log > analysis_results.txt
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ grep "192.168.1.100" auth.log >> analysis_results.txt
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$

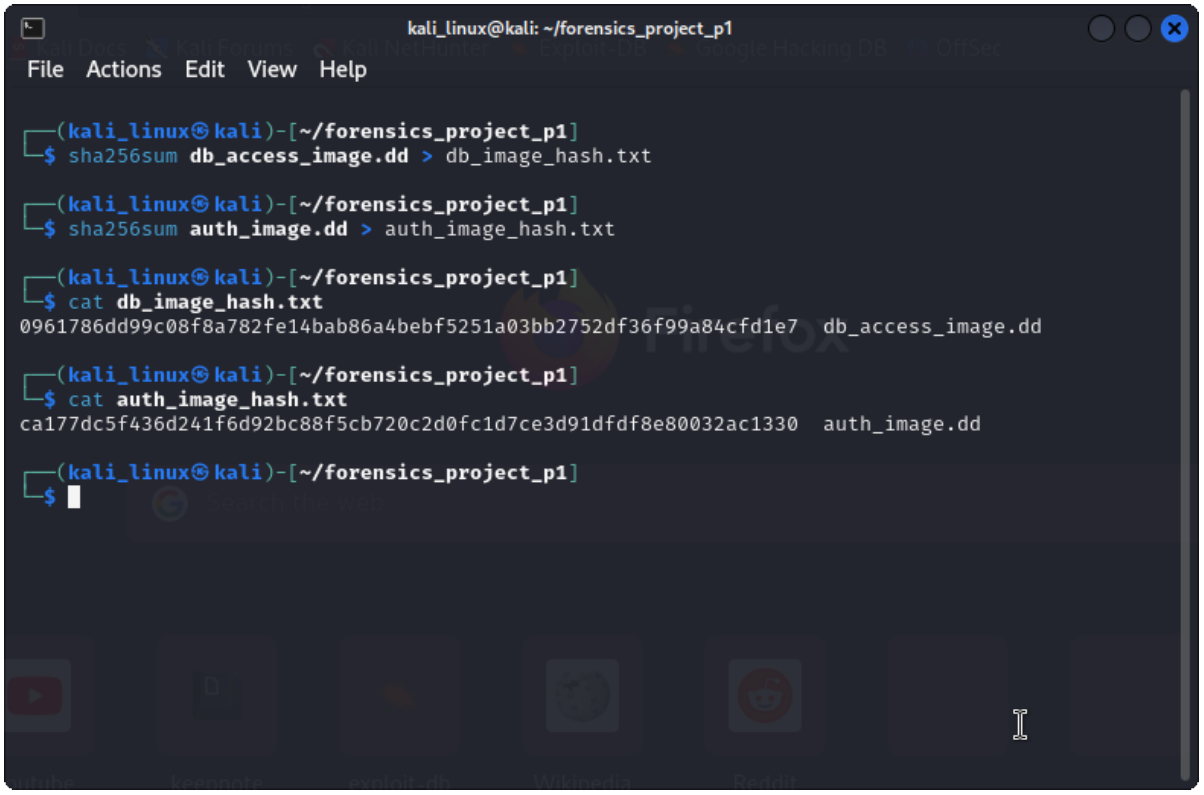

kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ sha256sum db_access.log > db_access_hash.txt
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ sha256sum auth.log > auth_hash.txt
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$

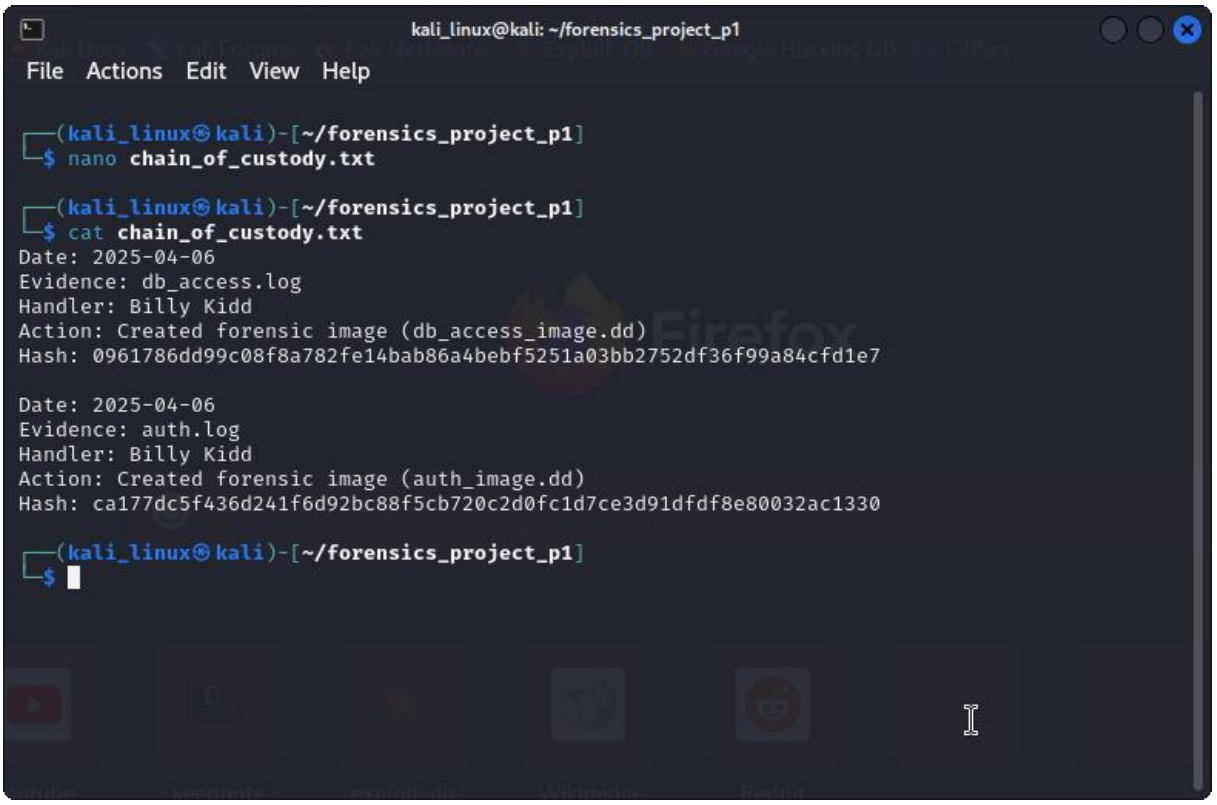

kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ cat db_access_hash.txt
ef2addd3ec0588bbf429b20d4a0db1777cf6004e6af7f884b56bc446bf3fa50c db_access.log
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ cat auth_hash.txt
6428124d51715da6c6f6389f63599494915a2aebf195969ecf5c1954754cba46 auth.log
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$


kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ dd if=db_access.log of=db_access_image.dd bs=512 conv=noerror,sync
0+1 records in
1+0 records out
512 bytes copied, 6.4458e-05 s, 7.9 MB/s
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ dd if=auth.log of=auth_image.dd bs=512 conv=noerror,sync
0+1 records in
1+0 records out
512 bytes copied, 9.3625e-05 s, 5.5 MB/s
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$


kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ ls -l *.dd
-rw-rw-r-- 1 kali_linux kali_linux 512 Apr 6 16:42 auth_image.dd
-rw-rw-r-- 1 kali_linux kali_linux 512 Apr 6 16:41 db_access_image.dd
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$


kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ strings db_access_image.dd | grep "192.168.1.100"
2025-04-05 02:00:03 - select * from drug_trials - User: jsmith - IP: 192.168.1.100
2025-04-05 02:00:05 - select * from drug_trials - User: jsmith - IP: 192.168.1.100
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ strings auth_image.dd | grep "192.168.1.100"
2025-04-05 02:00:01 - Login Success - User: jsmith - IP: 192.168.1.100
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$


kali_linux@kali: ~/forensics_project_p1
File Actions Edit View Help
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ sha256sum db_access_image.dd > db_image_hash.txt
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ sha256sum auth_image.dd > auth_image_hash.txt
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ cat db_image_hash.txt
0961786dd99c08f8a782fe14bab86a4bebf5251a03bb2752df36f99a84cfd1e7 db_access_image.dd
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$ cat auth_image_hash.txt
ca177dc5f436d241f6d92bc88f5cb720c2d0fc1d7ce3d91dfdf8e80032ac1330 auth_image.dd
┌──(kali_linux㉿kali)-[~/forensics_project_p1]
└─$



Phase 2: Tracing the Insider Threat

Plot Point: The investigator suspects an insider threat and shifts focus to the employee's workstation to uncover evidence of phishing and privilege escalation.

The investigator loaded the forensic image of John Smith's workstation into Autopsy, scanning for deleted files. A recovered .zip file caught their eye—drug_trials_data.zip, deleted but still lingering in unallocated space. The file's metadata showed it was created the day before the database queries. Digging deeper, they parsed the Windows Registry with RegRipper, finding a key under RunOnce that executed a PowerShell script: elevate_privileges.ps1. "Clever," the investigator thought. "He used a phishing email to get in, then escalated his access to steal the data." Opening the Outlook PST file, they found the smoking gun—a phishing email with a malicious Word document, timestamped just hours before the script ran.