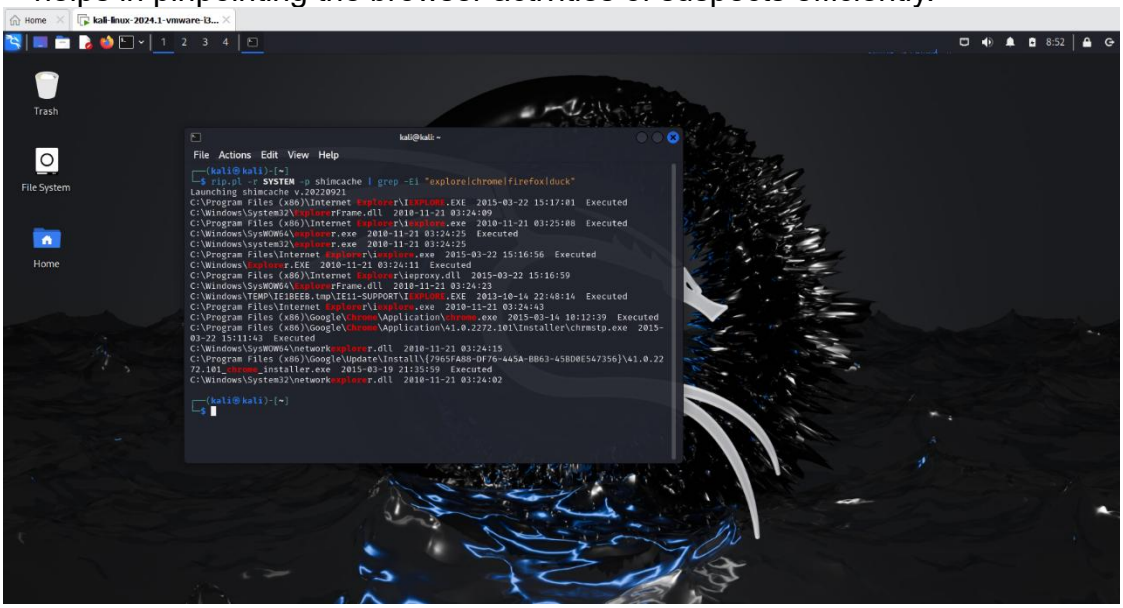
ITS60904

COMPUTER CRIME AND DIGITAL EVIDENCE

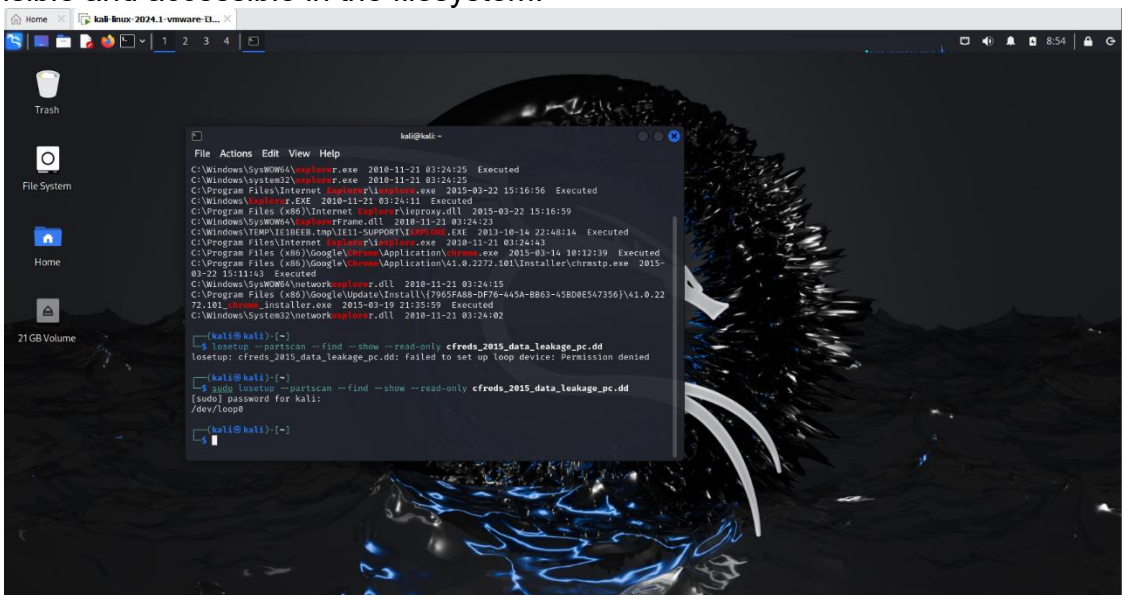
PRACTICAL 3 LAB REPORT

1. What web browsers were used?

- Find all possible browsers used by suspects including only those related to popular browsers like Chrome, Firefox, Safari, Opera, and Edge. This approach helps in pinpointing the browser activities of suspects efficiently.

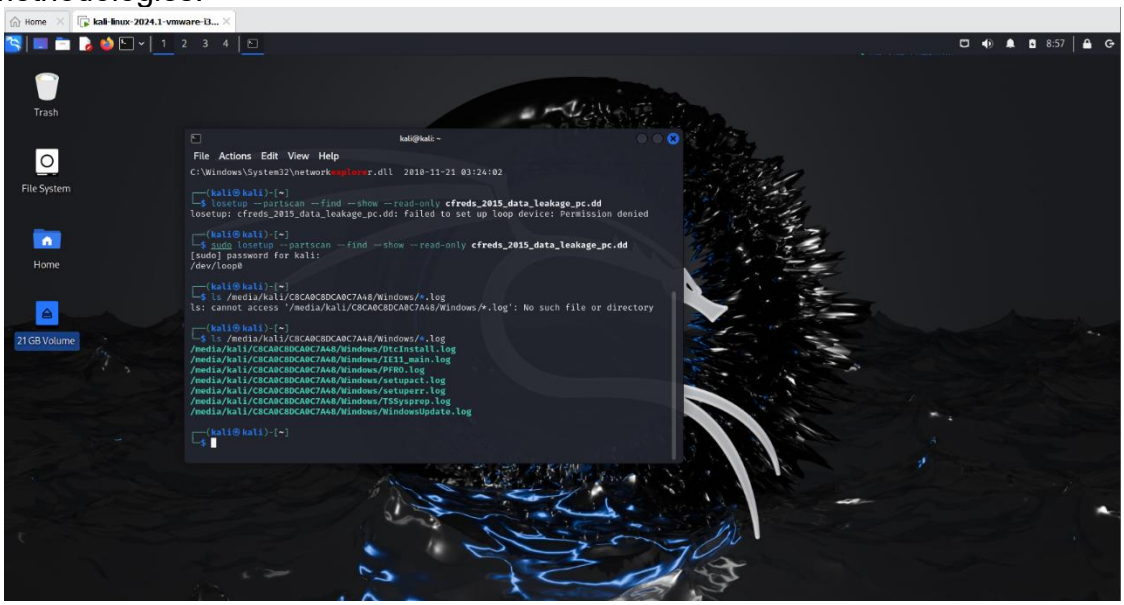


- To set up a loop device, create a file to use as the virtual disk. Then, use `losetup` to associate this file with a loop device, making it accessible as a block device. There must be `sudo` as this command allows a permitted user to execute a command as the superuser or another user, providing elevated permissions temporarily. Finally, mount the loop device to make its contents visible and accessible in the filesystem.

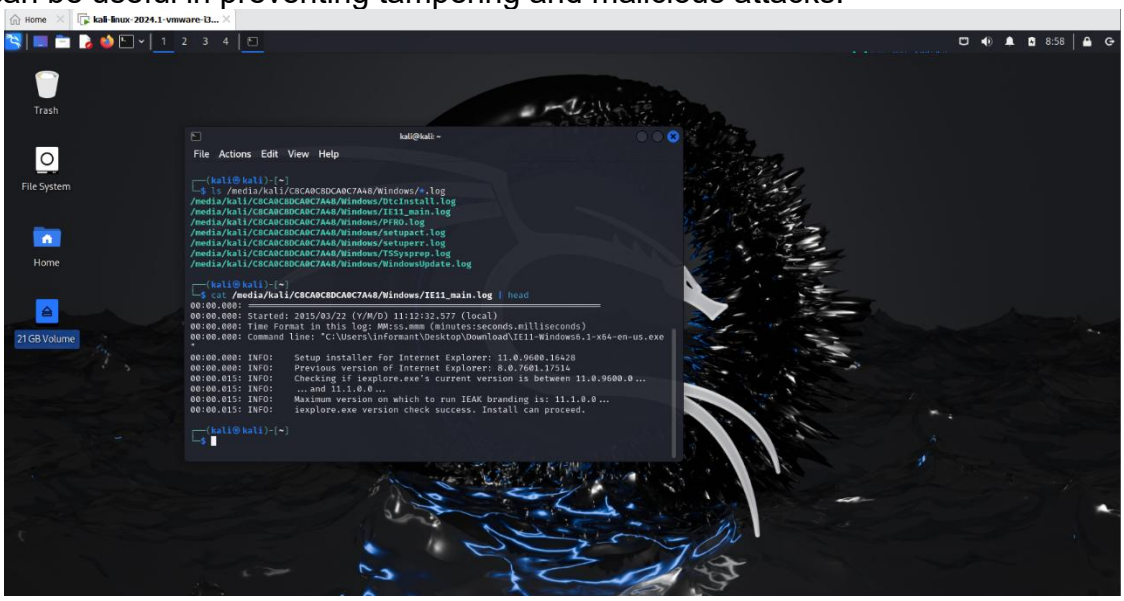


- Monitoring log files of all versions of Internet Explorer aid in identifying potential

security threat, compatibility problems, and use frequency of this browser. It is essential for maintaining the systems and security, checking compatibility of the new software version with the old one, and also for investigating forensic methodologies.



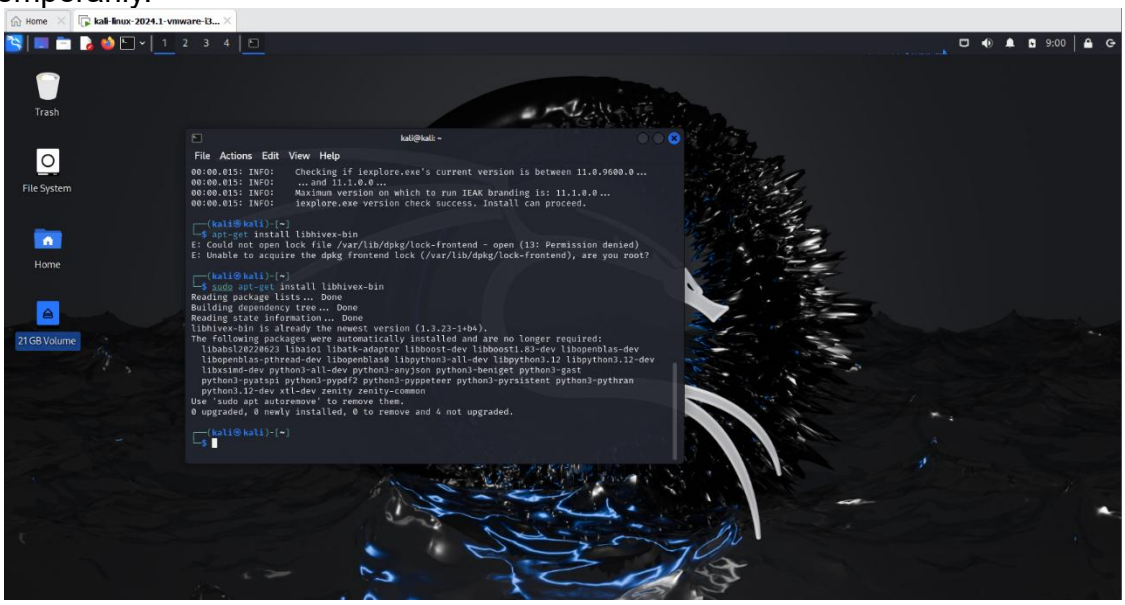
- It is vital to analyze the logs of Internet Explorer because the logs contain information about how people interact with websites, suspicious activities, and difficulties users have with browsers. It gives information on browser history, possible malicious activity of malware, and alterations in system settings, which can be useful in preventing tampering and malicious attacks.



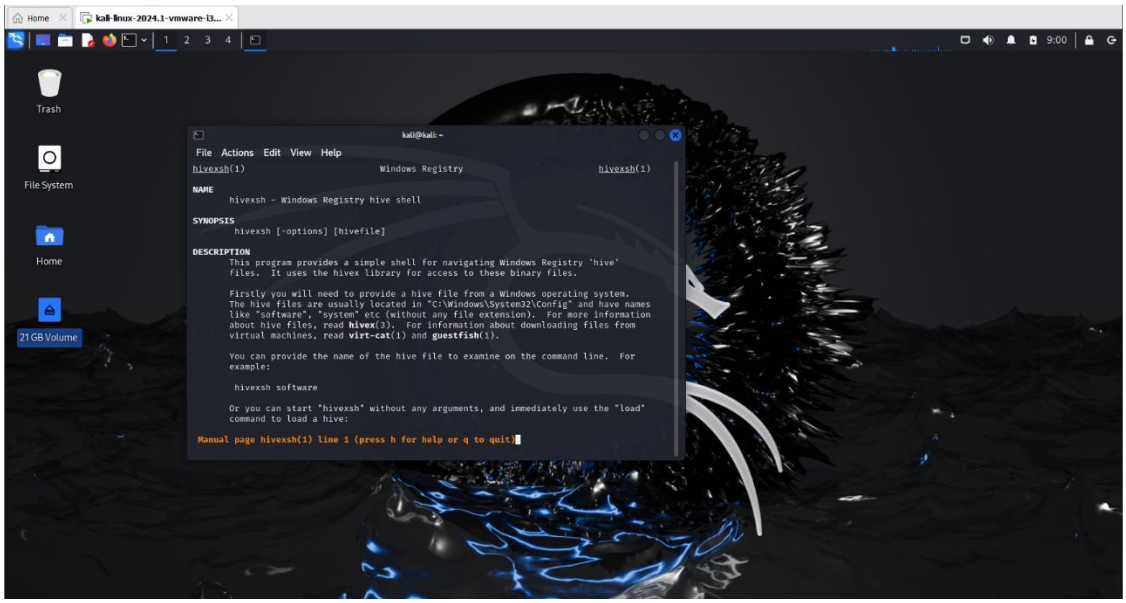
2. Can you find the version number?

- Install hivexsh

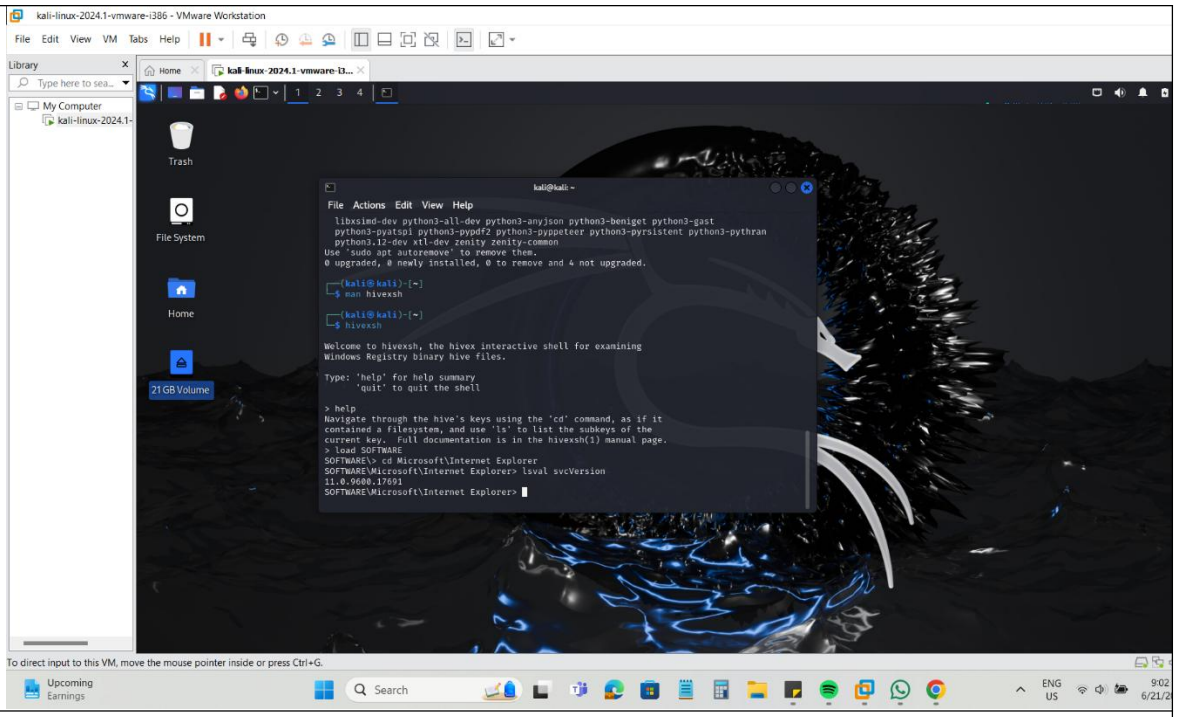
There must be `sudo` as this command allows a permitted user to execute a command as the superuser or another user, providing elevated permissions temporarily.



- Show hivexsh manual.

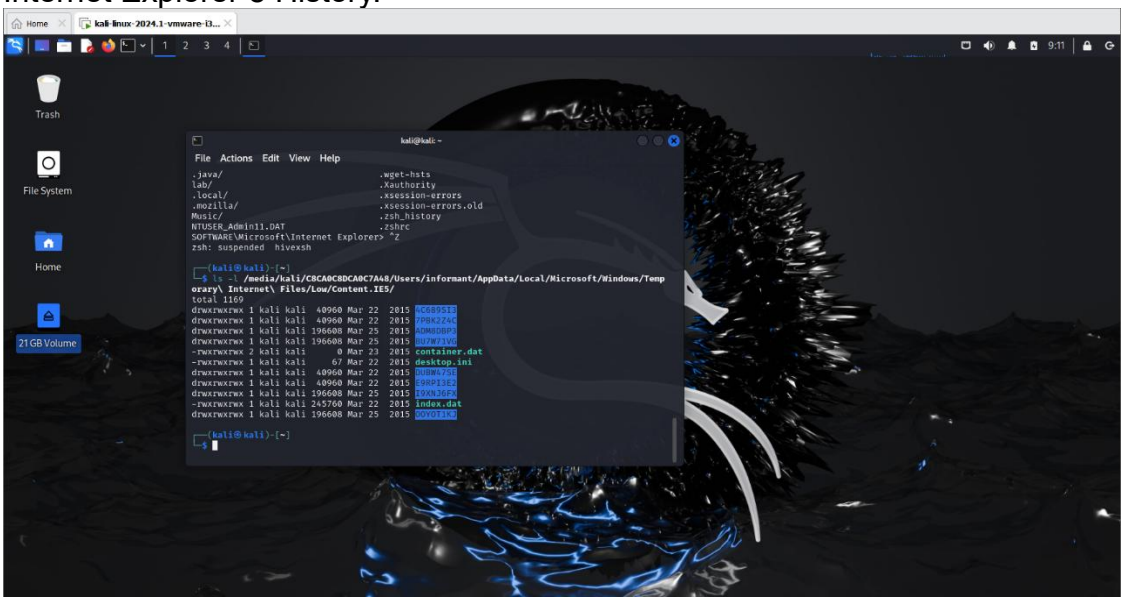


- Exam the version of IE using hivexsh
  This method is to analyze the version of Internet Explorer using `hivexsh` that would help to know specifically the type of vulnerability and whether it implements the standards of the web or not. This step is helpful in the evaluation of the security vulnerability of the system because the various IE versions come with different levels of risks and susceptibility to threats and attacks.

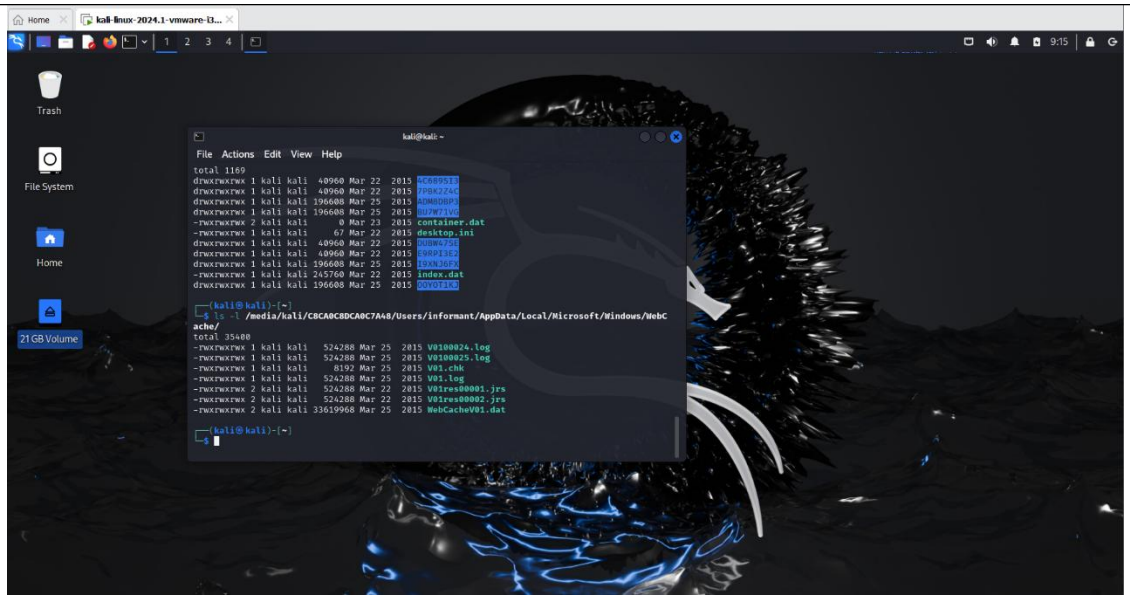


3. Identify directory/file paths related to the web browser history.

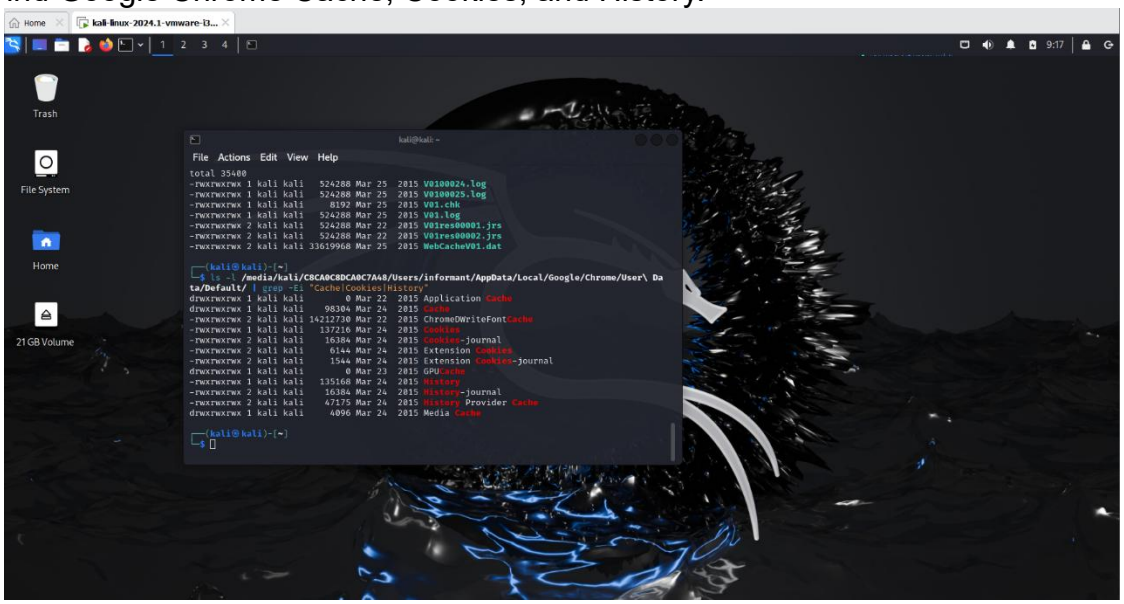
- Internet Explorer 8 History.



- Internet Explorer 11 History.

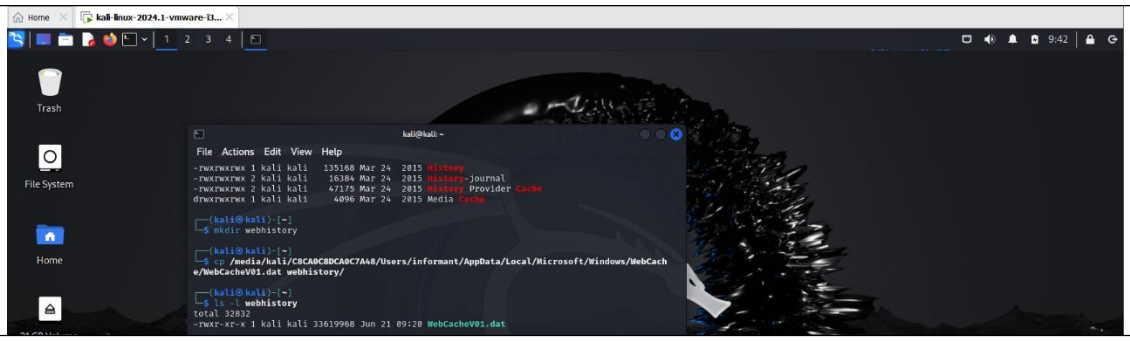


- Find Google Chrome Cache, Cookies, and History.

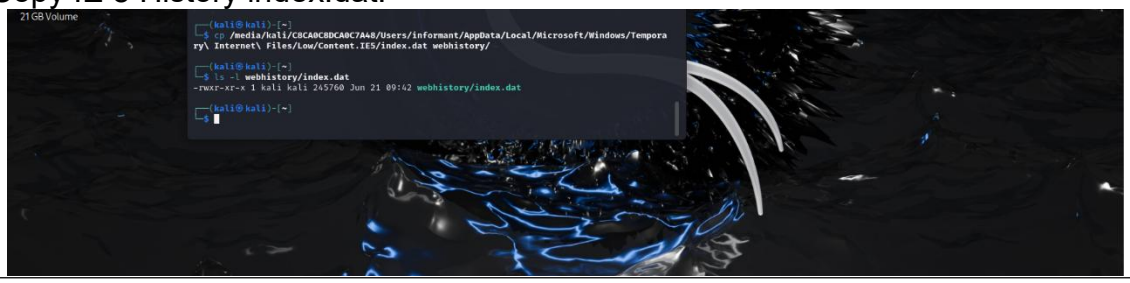


4. What websites were the suspect accessing? (Timestamp, URL...)

- Copy IE 11 History WebCacheV01.dat.



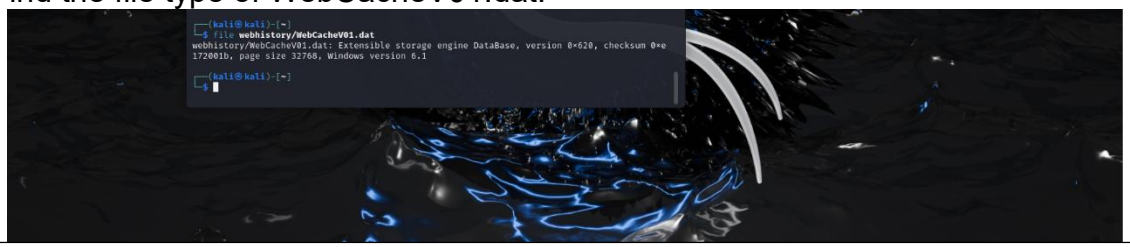
- Copy IE 8 History index.dat.



- Copy Chrome History History.

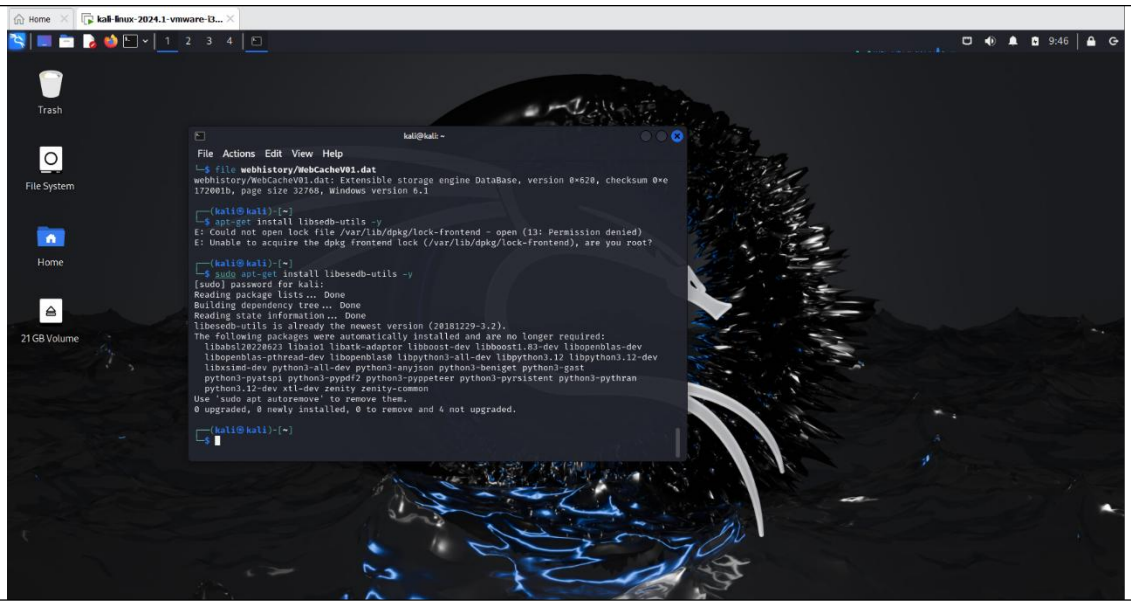
5. View IE 11 History Using libesedb.

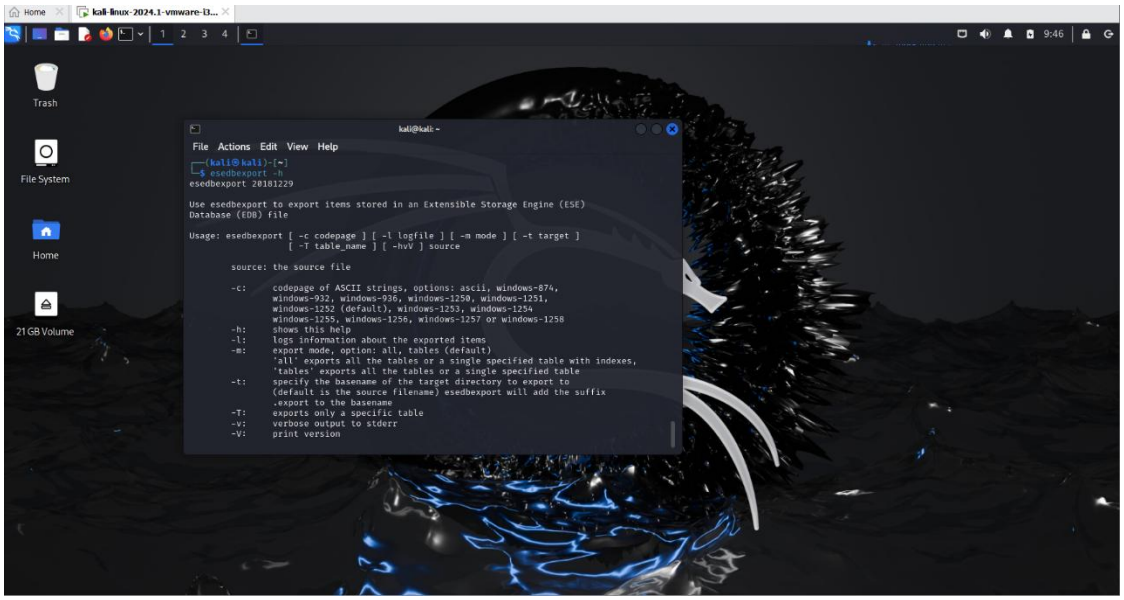
- Find the file type of WebCacheV01.dat.



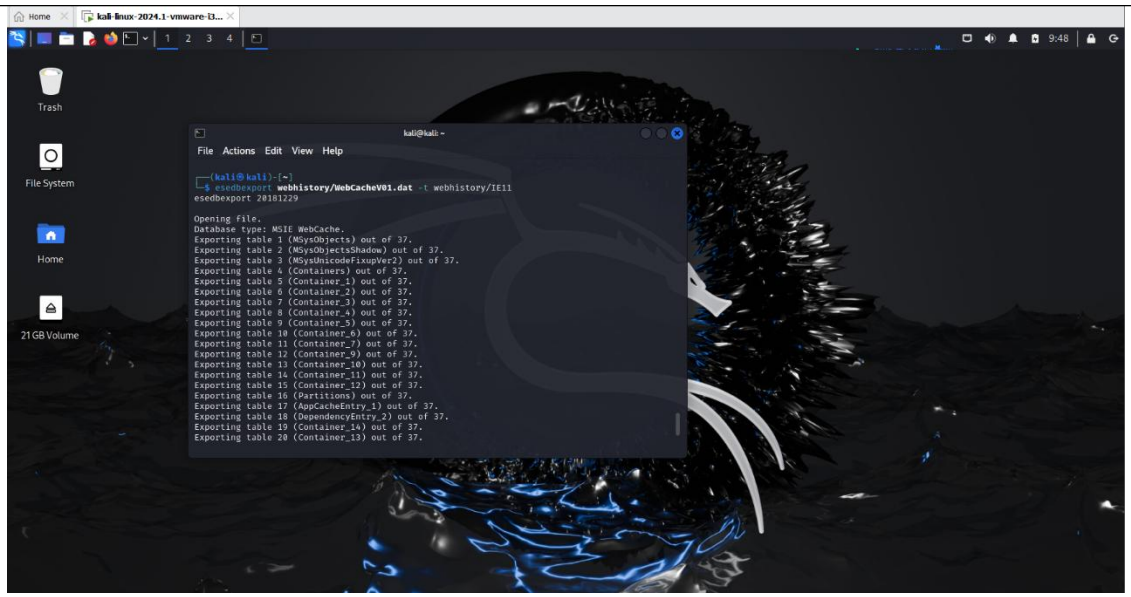
- Install libesedb

  There must be `sudo` as this command allows a permitted user to execute a command as the superuser or another user, providing elevated permissions temporarily. The utilization of libesedb is helpful to gain access to the ESE Database File (.edb) format is great for getting data out of applications running on the Windows platform such as Windows Search, Windows Mail, Exchange, and Active Directory. This step is critical for data investigations, forensic and diagnostic logs, and information about a particular application's data and its activity.

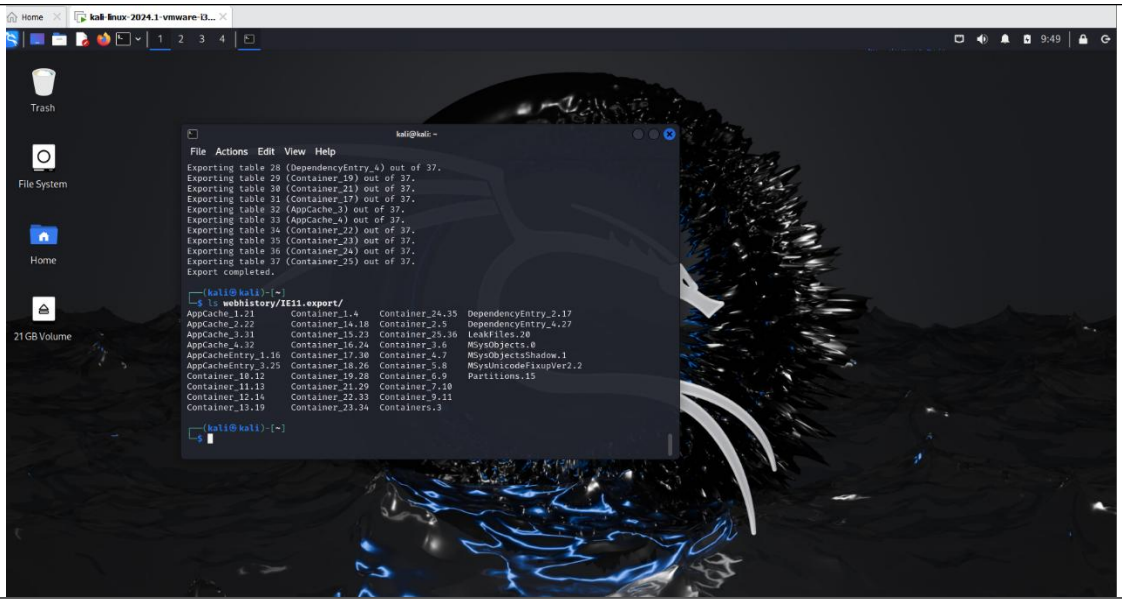




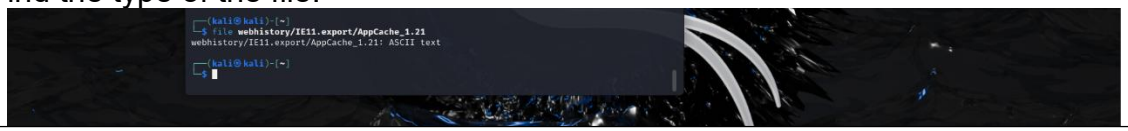
- Export WebCacheV01.dat to the folder webhistory/IE11.



- Verify the file the folder.



- Find the type of the file.



- Create three lines with three attributes. The `-e` option is used to enable interpretation of backslash escapes since we might wish to include any special character in the output. The `\n` option is to make a new line, thus enhancing the organization and legibility of the output to be generated. This step helps in producing formatted text to either scripts or command-line outputs for better arrangement of predicted structures.

- Select lines with the key word “manager”.
- Select attributes 1 and 3.
- The practical operation that concerns selection is `awk` which works by using the following syntax: `/selection_criteria/ {action }` input-file > output-file The above operation is crucial when it comes to refining large text documents. This step creates the opportunity for selective extraction and even selective alteration of the information with the help of criteria set to make automation of analysis and reporting possible.

- Show Row Number.

- Calculate sum.

- Show field names. There must be `_` for it to be able to work.

- Separate fields with tab ‘\t’ and show ModifiedTime and URL. Fields must be separated by the tab \t. The necessity of displaying ModifiedTime and URL arises due to the further correct display of data. This step is useful in simplification the comparison of large numbers both in the timestamps and URLs which is useful in such tasks as monitoring of changes, web activity, and in forensic analysis.

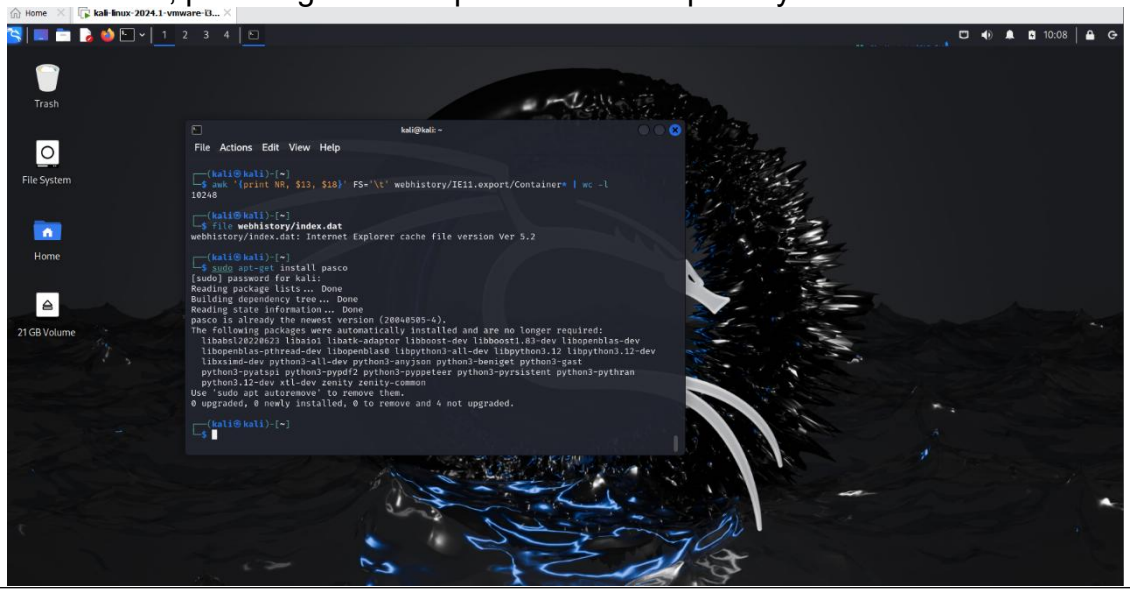
- Count the number records in the file.

- Count the number records in all files start with the string “Container”.

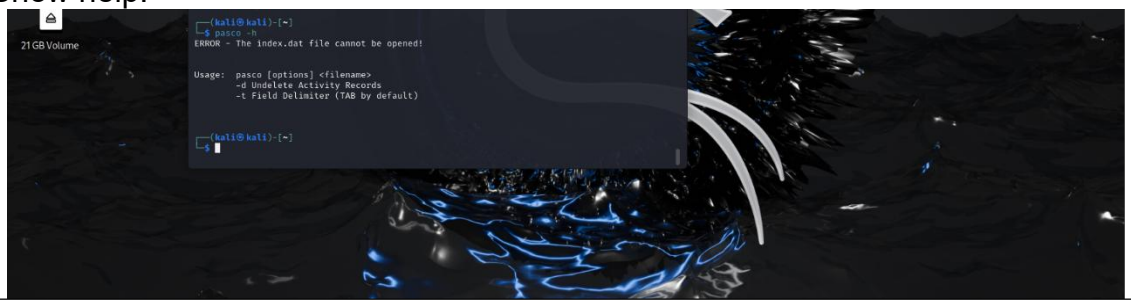
6. View IE 8 History using pasco.

- Exam the file type.

- Install pasco.
- pasco - tool to extract information from index.dat. There must be `sudo` as this command allows a permitted user to execute a command as the superuser or another user, providing elevated permissions temporarily.

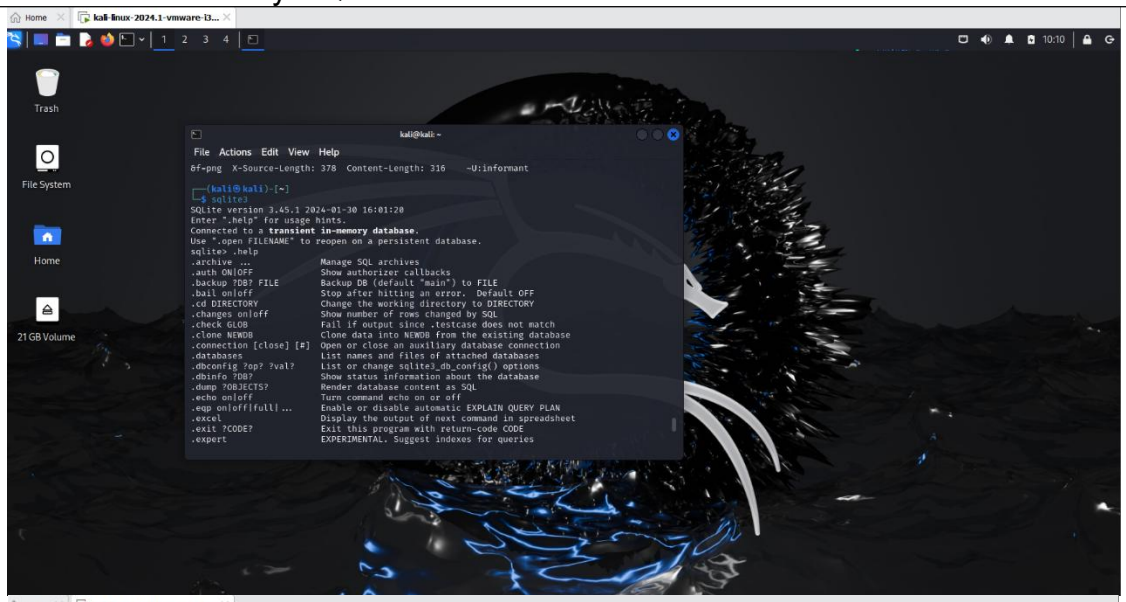


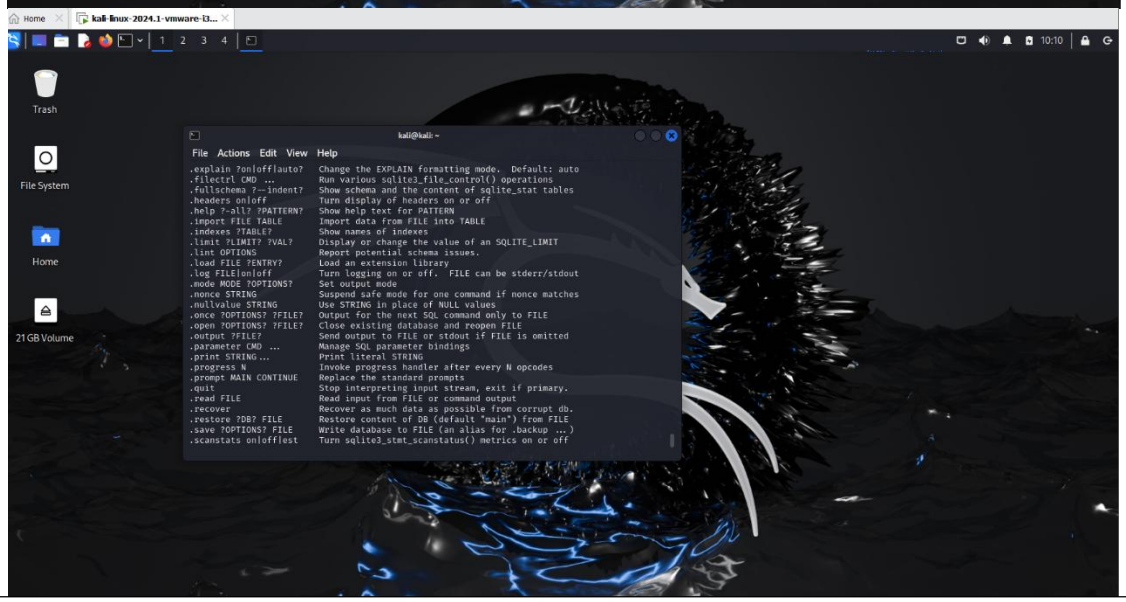
- Show help.

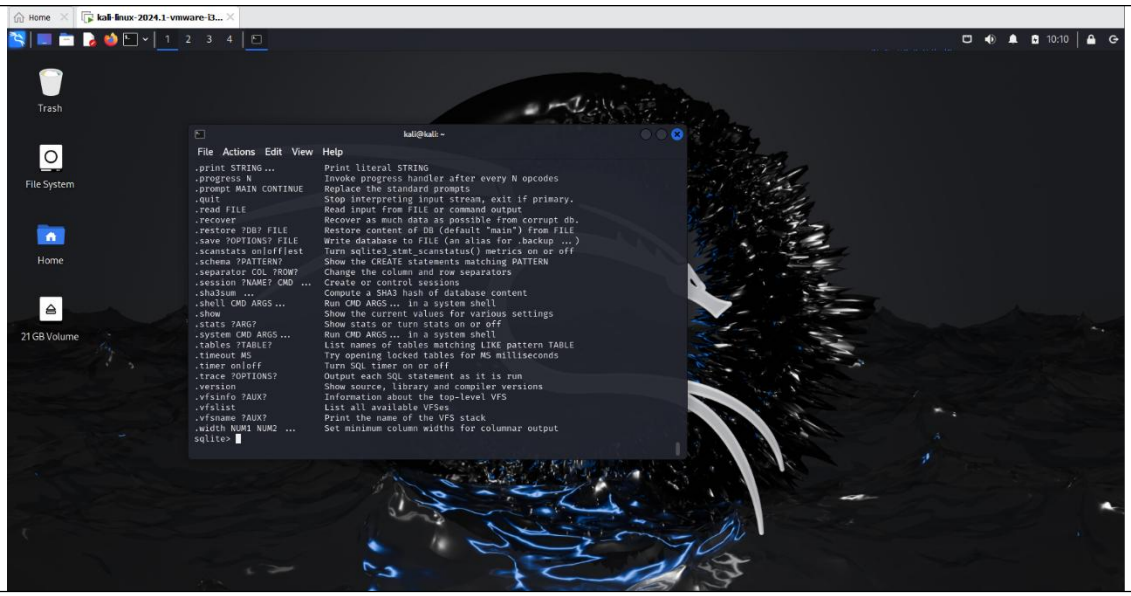


- Exam index.dat.

7. View Chrome History SQLite.





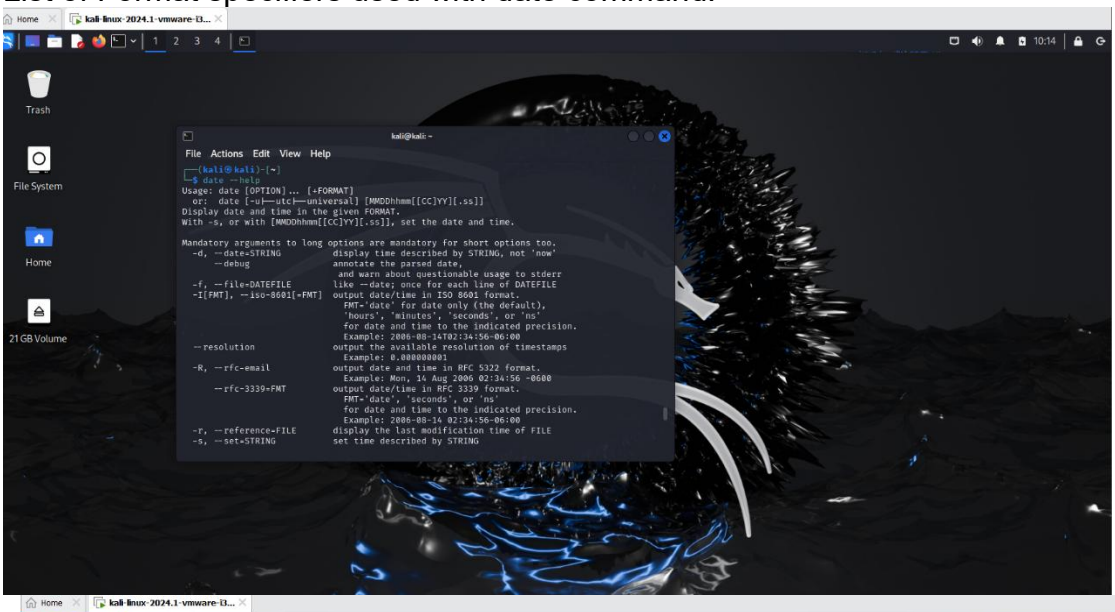


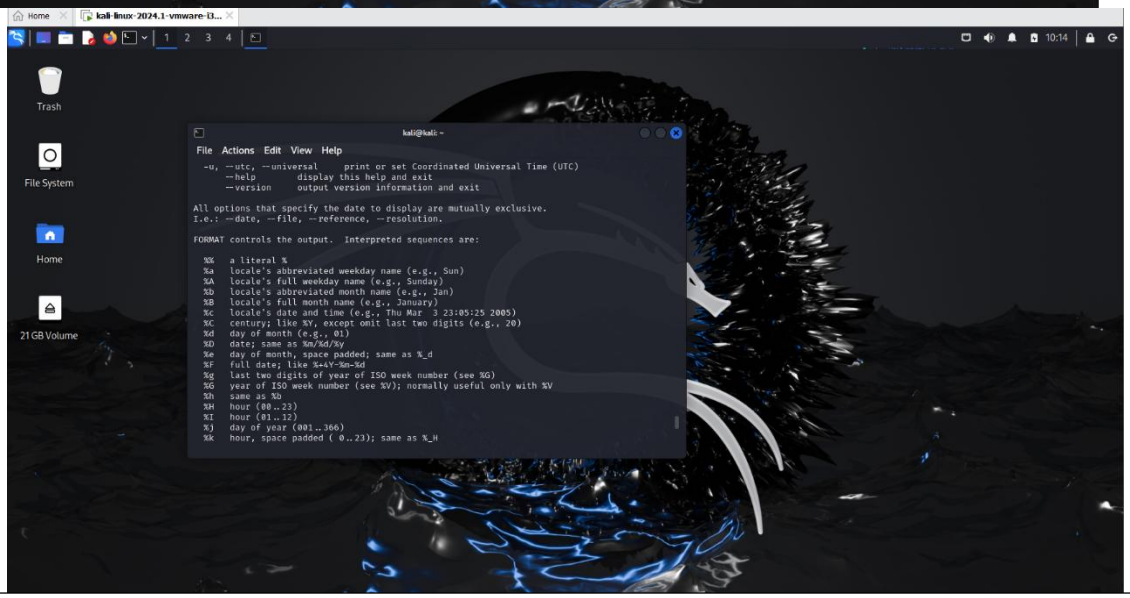
- Open Chrome history.

- This format of timestamp `13071510650000000` is implemented in Apple Safari (WebKit), Google Chrome, and Opera browsers (Chromium/Blink) and is hugely beneficial in timing and synchronizing web activity over a while. The time is accurately represented by 64 bits of microsecond since the year 1601-Jan-01 to facilitate logging (audit trails) which is help for debugging or to solve any crime cases.

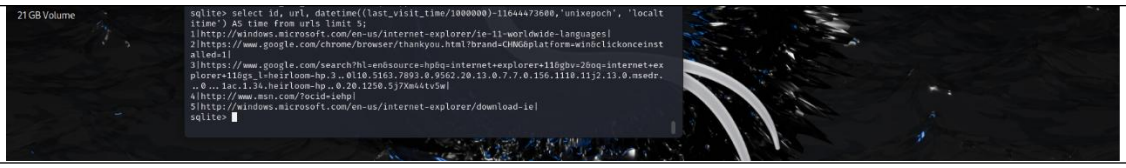
- The number of seconds elapsed since 01/01/1970 00:00:00. %s: seconds since 1970-01-01 00:00:00 UTC.

- List of Format specifiers used with date command.



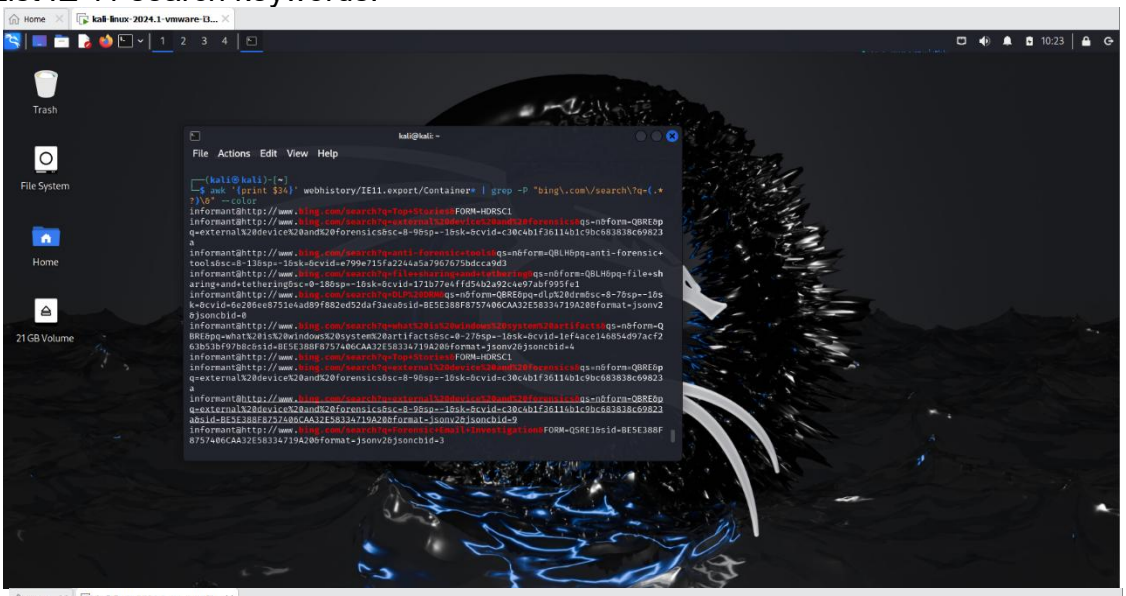


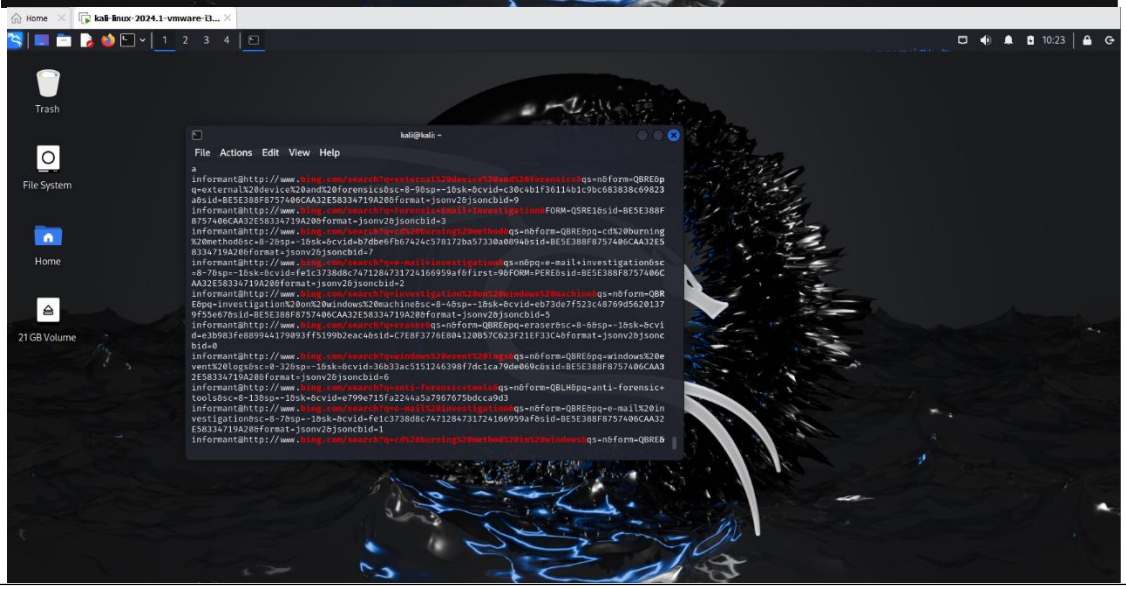
- Datetime function to convert webkit time to Unix epoch.

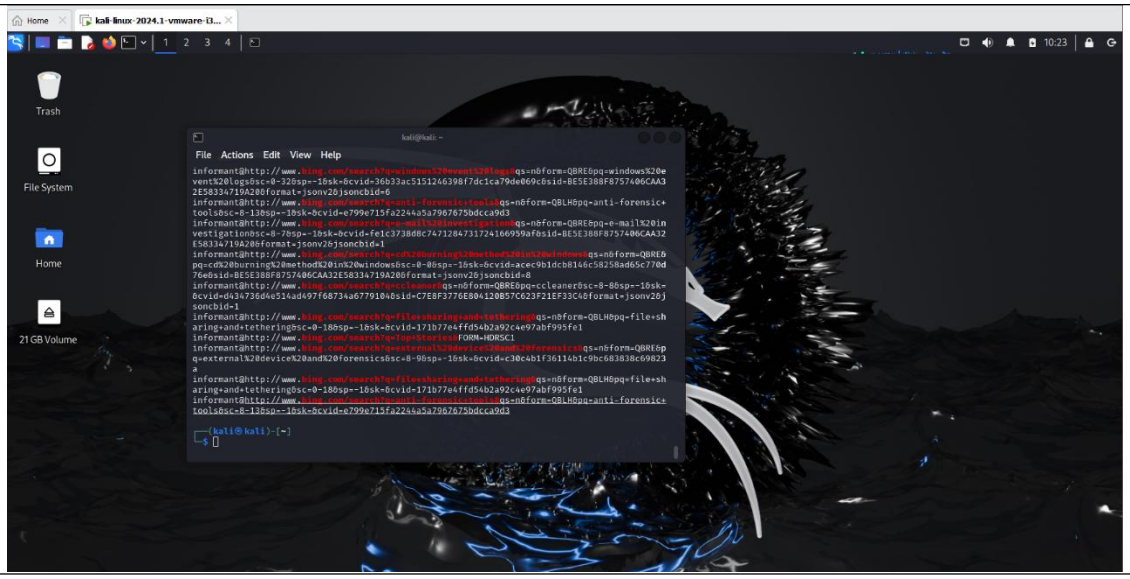


8. List all search keywords using web browsers. (Timestamp, URL, keyword...)

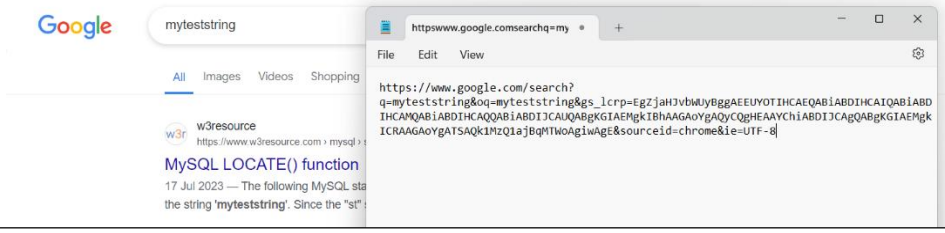
- List IE 11 search keywords.



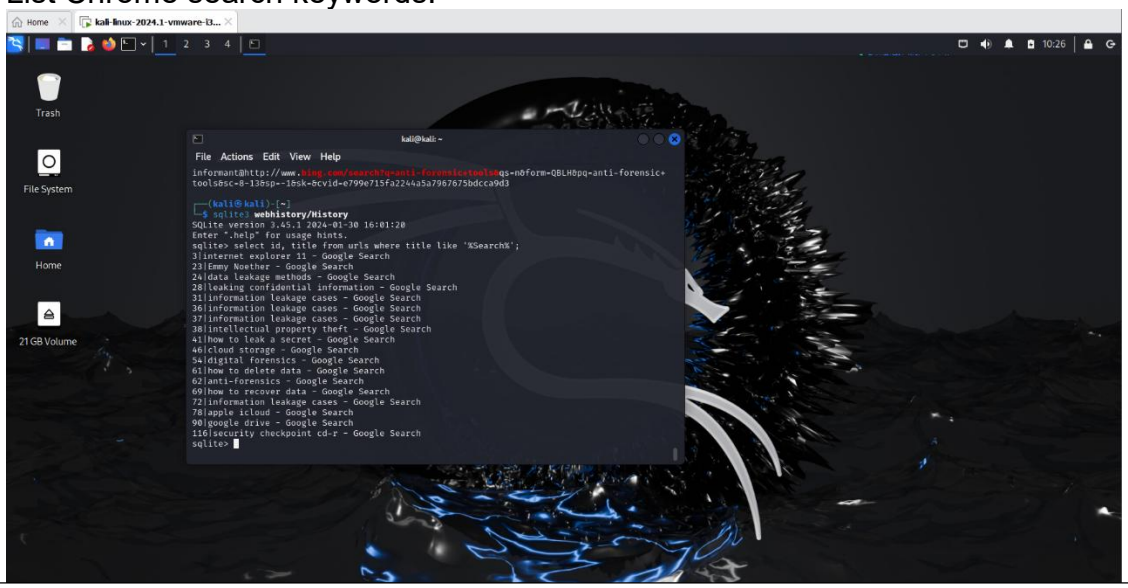




- Chrome browser.



- List Chrome search keywords.



9. List all user keywords at the search bar in Windows Explorer. (Timestamp, Keyword)

- rip.pl on NTUSER.DAT file with wordwheelquery plugin. Running `rip. pl` on an `NTUSER. A '.DAT' file, particularly generated by the `wordwheelquery` plugin, is relevant for the identification of recent search terms entered by a user on a system running on Windows. This step is of utmost importance in the digital forensic investigation, allows germinating insights toward users' details, search

history, and possibly evidence related with the case being investigated.