Forensic Analysis Notes:

Case Information:

Case: Analyze HTTP request (GET /images/NASA-logosmall.gif HTTP/1.0)

Analyst: Julius Niyonzima

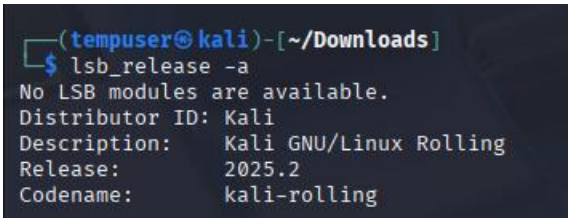
Professor: Dr. Chris Lamb

Email: jnbfg@umkc.edu

Id	File name	Hash(None)	Notes
1	NASA_access_log_Aug95	Verified and found to be human-readable text using file command(NASA_access_log_Aug95: ASCII text)	HTTP request logs

Tools and Environment

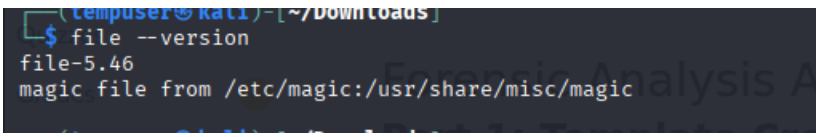
Kali Linux v2025.2



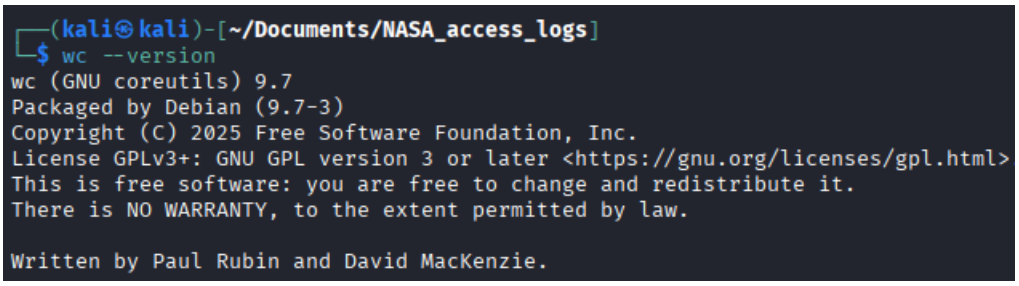
Grep v13.11

Chosen because it allows precise text pattern searching and line counting in large log files.

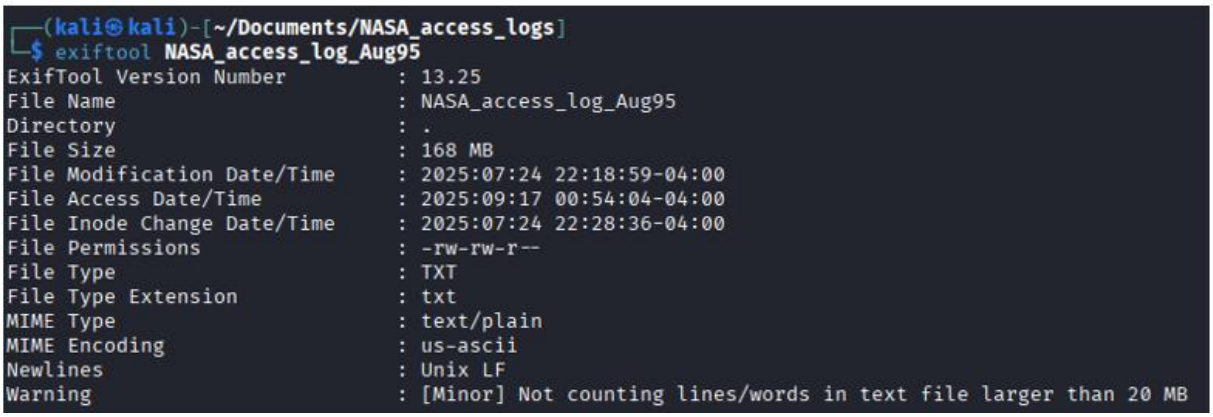
File v5.46 was chosen because it checks the type of the file



WC –9.7 was chosen because it gives the number of words, lines, and bytes in the file.



Exiftool v13.25 was chosen because it gives data information about data of the file

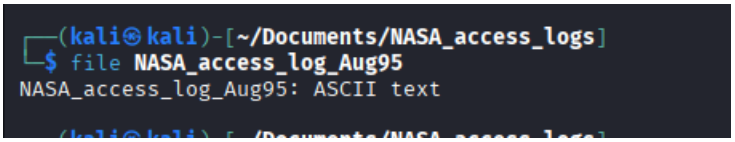


Analysis Steps :

Step1: Verified file type using the file command

Command: File NASA_access_log_Aug95

Result: the file was found to human human-readable text



Status: Worked

Step 2: Check the metadata with exfitool

Command: exiftool NASA_access_log_Aug95

Result: The file was confirmed to contain a human-readable text, which can be searched through using commands like grep, wc, and Wc

```
┌──(kali㉿kali)-[~/Documents/NASA_access_logs]
└─$ exiftool NASA_access_log_Aug95
ExifTool Version Number         : 13.25
File Name                       : NASA_access_log_Aug95
Directory                       : .
File Size                       : 168 MB
File Modification Date/Time     : 2025:07:24 22:18:59-04:00
File Access Date/Time           : 2025:09:17 00:54:04-04:00
File Inode Change Date/Time     : 2025:07:24 22:28:36-04:00
File Permissions                : -rw-rw-r--
File Type                       : TXT
File Type Extension             : txt
MIME Type                       : text/plain
MIME Encoding                   : us-ascii
Newlines                        : Unix LF
Warning                         : [Minor] Not counting lines/words in text file larger than 20 MB
```

Status: Worked

Step 3: Using WC to finding the number of lines, words, and bytes in NASA_access_log_Aug95

Command: wc NASA_access_log_Aug95

Result: Extract the number of lines, words, and bytes in the file.

```
┌──(kali㉿kali)-[~/Documents/NASA_access_logs]
└─$ wc NASA_access_log_Aug95
  1569898  15697986 167813770 NASA_access_log_Aug95
```

Status: Worked

Step 4: Search for the HTTP request in the NASA_access_log_Aug95

Command: grep "GET /images/NASA-logosmall.gif HTTP/1.0" NASA_access_log_Aug95

Result: I failed to extract the number of lines containing GET /images/NASA-logosmall.gif HTTP/1.0 from the logs; however, the link was found to exist in the log file.

```
└─$ grep "GET /images/NASA-logosmall.gif HTTP/1.0"  NASA_access_log_Aug95
uplherc.upl.com - - [01/Aug/1995:00:00:14 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 304 0
kgtyk4.kj.yamagata-u.ac.jp - - [01/Aug/1995:00:00:21 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 304
piweba4y.prodigy.com - - [01/Aug/1995:00:00:32 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 200 786
www-d3.proxy.aol.com - - [01/Aug/1995:00:01:28 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 200 786
205.163.36.61 - - [01/Aug/1995:00:02:01 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 304 0
rpgopher.aist.go.jp - - [01/Aug/1995:00:02:02 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 304 0
piweba1y.prodigy.com - - [01/Aug/1995:00:02:50 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 304 0
piweba1y.prodigy.com - - [01/Aug/1995:00:03:41 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 304 0
haraway.ucet.ufl.edu - - [01/Aug/1995:00:04:30 -0400] "GET /images/NASA-logosmall.gif HTTP/1.0" 200 786
```

Status: Did not work

Step 4: Find the number of times the request was made.

Command: grep -c “GET /images/NASA-logosmall.gif HTTP/1.0” NASA_access_log_Aug95

Result: Finding the number of times the HTTP request occurs in the log did not match the actual number (96841) because the command returns anything that matches the request, even if there’s a slight difference.

```
┌──(kali㉿kali)-[~/Documents/NASA_access_logs]
└─$ grep -c "GET /images/NASA-logosmall.gif HTTP/1.0"  NASA_access_log_Aug95
96849
```

Status: Did not work

Step5: Finding the number of occurrences of the request using grep and wc -l

Command: grep “GET /images/NASA-logosmall.gif HTTP/1.0” NASA_access_log_Aug95 | wc -l

Result. Finding the number of times the HTTP request occurs in the log did not match the actual number (96841) because the command returns anything that matches the request, even if there’s a slight difference. This suggests the search was too long.

```
┌──(kali㉿kali)-[~/Documents/NASA_access_logs]
└─$ grep  "GET /images/NASA-logosmall.gif HTTP/1.0"  NASA_access_log_Aug95 | wc -l
96849
```

Status: Did not work

Step 6: Refined the search for the web request pattern using grep -c by embedding the web request link in double “” nested in single ‘’ to eliminate overcounting.

Command: grep -c ‘ “GET /images/NASA-logosmall.gif HTTP/1.0” ‘ NASA_access_log_Aug95

```
┌──(kali㉿kali)-[~/Documents/NASA_access_logs]
└─$ grep -c '"GET /images/NASA-logosmall.gif HTTP/1.0"'  NASA_access_log_Aug95
96841
```

Result: The number of occurrences of the web request where found to be exactly 96841

This approach ensures only lines containing the exact request GET /images/NASA-logosmall.gif HTTP/1.0 are counted.

Status: Worked

Findings:

After running various commands, the resource /images/NASA-logosmall.gif was requested **96,841 times** during August 1995.

The difference of 8 requests between my search attempts and the correct number of occurrences provided demonstrates the importance of **precise pattern matching** in forensic analysis. Incorrect search patterns can introduce false positives, leading to inaccurate reporting.

Conclusion.

Through careful refinement of the search command, the exact number of requests was determined. This explains the reason why we need to validate our commands with various resources to make sure they are giving us accurate information in digital investigations.