

IOC Extraction Case Report

Date: [2025-08-10]

▼ Dataset

- Analyst: **Jynx**
- Source: Apache Access Logs from compromised web server simulated under controlled environments.

▼ Files:

```
└──(jynx㉿kali)-[~/Desktop/linux/august10]
    └──$ ls -lh
        total 52K
        -rw-r--r-- 1 jynx jynx 5.2K Aug 10 17:47 access_log_1.log
        -rw-r--r-- 1 jynx jynx 5.0K Aug 10 17:47 access_log_2.log
        -rw-r--r-- 1 jynx jynx 5.1K Aug 10 17:47 access_log_3.log
        -rw-rw-r-- 1 jynx jynx 3.1K Aug 10 13:48 compromised_logs.zip
        -rw-rw-r-- 1 jynx jynx 1.1K Aug 10 17:35 domainFinder.py
        -rw-rw-r-- 1 jynx jynx 983 Aug 10 17:42 DomainsFound.txt
        -rw-rw-r-- 1 jynx jynx 1.5K Aug 10 19:05 hashesFinder.py
        -rw-rw-r-- 1 jynx jynx 1.1K Aug 10 19:06 HashesFound.txt
        -rw-rw-r-- 1 jynx jynx 965 Aug 10 16:58 ipFinder.py
        -rw-rw-r-- 1 jynx jynx 972 Aug 10 17:02 IPsFound.txt

└──(jynx㉿kali)-[~/Desktop/linux/august10]
    └──$ █
```

▼ access_log_1.log

```
(jynx㉿kali)-[~/Desktop/linux/august10]
└─$ cat access_log.1.log
8.8.8.8 - [07/Aug/2025:18:59:05 +0000] "GET http://malicious-site.ru/download?hash=4d88612fea8af36de82e1278abb02f HTTP/1.1" 200 512
142.250.182.4 - [01/Aug/2025:11:23:33:04 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
8.8.8.8 - [10/Aug/2025:22:07:00 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
13.107.21.200 - [10/Aug/2025:12:23:17 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
142.250.182.4 - [04/Aug/2025:22:23:23 +0000] "GET http://example.com/about HTTP/1.1" 200 512
8.8.8.8 - [04/Aug/2025:21:07:00 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
45.77.23.12 - [02/Aug/2025:05:07:55 +0000] "GET http://data-stealer.net/wp-content/plugins/vuln.php HTTP/1.1" 200 512
8.8.8.8 - [10/Aug/2025:10:07:00 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
142.250.182.4 - [08/Aug/2025:10:07:00 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
13.107.21.200 - [07/Aug/2025:07:58:56 +0000] "GET http://wikimedia.org/contact HTTP/1.1" 200 512
103.45.67.89 - [09/Aug/2025:00:25:08 +0000] "GET http://h4or.biz/admin/login.php HTTP/1.1" 200 512
142.250.182.4 - [08/Aug/2025:03:11:48 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
192.168.56.23 - [07/Aug/2025:01:20:15 +0000] "GET http://h4or.biz/wp-content/plugins/vuln.php HTTP/1.1" 200 512
103.45.67.89 - [01/Aug/2025:01:45:28 +0000] "GET http://data-stealer.net/download?hash=9074c9897bc770ffcc029102a200c5de80dbd3f3f6a7f5f90b7e3aee8a8a6f6 HTTP/1.1" 200 512
142.250.182.4 - [03/Aug/2025:10:07:00 +0000] "GET http://wikimedia.org/index.html HTTP/1.1" 200 512
13.107.21.200 - [07/Aug/2025:09:56:32 +0000] "GET http://wikimedia.org/contact HTTP/1.1" 200 512
142.250.182.4 - [04/Aug/2025:10:07:00 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
66.102.12.54 - [02/Aug/2025:17:45:30 +0000] "GET http://h4or.biz/wp-content/plugins/vuln.php HTTP/1.1" 200 512
13.107.21.200 - [10/Aug/2025:01:40:56 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
8.8.8.8 - [05/Aug/2025:00:27:39 +0000] "GET http://openai.com/contact HTTP/1.1" 200 512
103.45.67.89 - [01/Aug/2025:00:43:42 +0000] "GET http://h4or.biz/download?hash=5d4192abc4b2a76b9719d911017c592 HTTP/1.1" 200 512
142.250.182.4 - [03/Aug/2025:10:07:00 +0000] "GET http://wikimedia.org/index.html HTTP/1.1" 200 512
142.250.182.4 - [05/Aug/2025:23:42:57 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
8.8.8.8 - [10/Aug/2025:15:16:34 +0000] "GET http://wikimedia.org/contact HTTP/1.1" 200 512
192.168.56.23 - [10/Aug/2025:10:03:33:47 +0000] "GET http://malicious-site.ru/uploadfile=webshell.php HTTP/1.1" 200 512
192.168.56.23 - [08/Aug/2025:10:03:44:17 +0000] "GET http://h4or.biz/download?hash=d7fcfe471194aa8b5b6e47267f03d4a0e2bd7db66d962f5a7bdee6f8a7e0 HTTP/1.1" 200 512
13.107.21.200 - [01/Aug/2025:19:35:42 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
13.107.21.200 - [01/Aug/2025:19:35:42 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
13.107.21.200 - [01/Aug/2025:19:35:42 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
13.107.21.200 - [09/Aug/2025:07:59:00 +0000] "GET http://h4or.biz/contact HTTP/1.1" 200 512
192.168.56.23 - [02/Aug/2025:12:16:45 +0000] "GET http://data-stealer.net/uploadfile=webshell.php HTTP/1.1" 200 512
8.8.8.8 - [01/Aug/2025:23:09:56 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
13.107.21.200 - [07/Aug/2025:18:26:28 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
8.8.8.8 - [06/Aug/2025:19:28:20 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
8.8.8.8 - [02/Aug/2025:20:02:37 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
13.107.21.200 - [06/Aug/2025:20:23:33 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
13.107.21.200 - [04/Aug/2025:20:23:33 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
142.250.182.4 - [01/Aug/2025:09:57:20 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
8.8.8.8 - [06/Aug/2025:12:05:17 +0000] "GET http://wikimedia.org/index.html HTTP/1.1" 200 512
66.102.12.54 - [03/Aug/2025:20:23:33 +0000] "GET http://malicious-site.ru/wp-content/plugins/vuln.php HTTP/1.1" 200 512
45.77.23.12 - [03/Aug/2025:21:19 +0000] "GET http://h4or.biz/wp-content/plugins/vuln.php HTTP/1.1" 200 512
8.8.8.8 - [04/Aug/2025:21:35:30 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
192.168.56.23 - [06/Aug/2025:08:15:13 +0000] "GET http://h4or.biz/uploadfile=webshell.php HTTP/1.1" 200 512
103.45.67.89 - [04/Aug/2025:08:15:13 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
66.102.12.54 - [08/Aug/2025:04:56:06 +0000] "GET http://data-stealer.net/download?hash=9074c9897bc770ffcc029102a200c5de80dbd3f3f6a7f5f90b7e3aee8a8a6f6 HTTP/1.1" 200 512
142.250.182.4 - [05/Aug/2025:06:09:17 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
13.107.21.200 - [06/Aug/2025:12:03:49 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
13.107.21.200 - [10/Aug/2025:03:42:35 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
8.8.8.8 - [05/Aug/2025:12:41:35 +0000] "GET http://example.com/about HTTP/1.1" 200 512
```

▼ access_log_2.log

```
(jynx㉿kali)-[~/Desktop/linux/august10]
└─$ cat access_log.2.log
8.8.8.8 - [07/Aug/2025:02:21:21 +0000] "GET http://example.com/about HTTP/1.1" 200 512
13.107.21.200 - [02/Aug/2025:03:26:54 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
192.168.56.23 - [09/Aug/2025:15:41:18 +0000] "GET http://evil-domain.com/wp-content/plugins/vuln.php HTTP/1.1" 200 512
142.250.182.4 - [04/Aug/2025:17:33:15 +0000] "GET http://example.com/about HTTP/1.1" 200 512
142.250.182.4 - [10/Aug/2025:01:22:15 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
8.8.8.8 - [02/Aug/2025:10:47:10 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
8.8.8.8 - [10/Aug/2025:15:08:47 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
8.8.8.8 - [10/Aug/2025:00:41:43 +0000] "GET http://example.com/about HTTP/1.1" 200 512
8.8.8.8 - [04/Aug/2025:22:59:00 +0000] "GET http://example.com/about HTTP/1.1" 200 512
8.8.8.8 - [07/Aug/2025:15:24:25 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
142.250.182.4 - [01/Aug/2025:21:31:55 +0000] "GET http://wikimedia.org/contact HTTP/1.1" 200 512
142.250.182.4 - [01/Aug/2025:10:19:57 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
13.107.21.200 - [04/Aug/2025:03:58:31 +0000] "GET http://wikimedia.org/contact HTTP/1.1" 200 512
142.250.182.4 - [03/Aug/2025:02:36:00 +0000] "GET http://example.com/about HTTP/1.1" 200 512
13.107.21.200 - [10/Aug/2025:03:44:37 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
13.107.21.200 - [10/Aug/2025:02:36:37 +0000] "GET http://openai.com/contact HTTP/1.1" 200 512
13.107.21.200 - [05/Aug/2025:00:52:18 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
13.107.21.200 - [09/Aug/2025:19:44:30 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
8.8.8.8 - [06/Aug/2025:17:59:31 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
8.8.8.8 - [04/Aug/2025:14:14:01 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
103.45.67.89 - [07/Aug/2025:00:25:37 +0000] "GET http://malicious-site.ru/download?hash=4d88612fea8af36de82e1278abb02f HTTP/1.1" 200 512
66.102.12.54 - [09/Aug/2025:11:52:34 +0000] "GET http://data-stealer.net/admin/login.php HTTP/1.1" 200 512
192.168.56.23 - [01/Aug/2025:18:23 +0000] "GET http://h4or.biz/download?hash=4d88612fea8af36de82e1278abb02f HTTP/1.1" 200 512
13.107.21.200 - [08/Aug/2025:14:58:13 +0000] "GET http://wikimedia.org/contact HTTP/1.1" 200 512
13.107.21.200 - [10/Aug/2025:03:51:15 +0000] "GET http://wikimedia.org/contact HTTP/1.1" 200 512
142.250.182.4 - [01/Aug/2025:08:58:47 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
13.107.21.200 - [06/Aug/2025:02:24:49 +0000] "GET http://openai.com/contact HTTP/1.1" 200 512
8.8.8.8 - [09/Aug/2025:18:51:50 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
142.250.182.4 - [08/Aug/2025:12:23:54 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
142.250.182.4 - [01/Aug/2025:00:54:33 +0000] "GET http://openai.com/contact HTTP/1.1" 200 512
45.77.23.12 - [08/Aug/2025:22:39:42 +0000] "GET http://data-stealer.net/wp-content/plugins/vuln.php HTTP/1.1" 200 512
8.8.8.8 - [05/Aug/2025:11:15:51 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
142.250.182.4 - [08/Aug/2025:22:24:00 +0000] "GET http://wikimedia.org/about HTTP/1.1" 200 512
192.168.56.23 - [10/Aug/2025:13:21:24 +0000] "GET http://data-stealer.net/uploadfile=webshell.php HTTP/1.1" 200 512
103.45.67.89 - [07/Aug/2025:15:19:33 +0000] "GET http://evil-domain.com/admin/login.php HTTP/1.1" 200 512
66.102.12.54 - [05/Aug/2025:16:05:07 +0000] "GET http://evil-domain.com/download?hash=4d88612fea8af36de82e1278abb02f HTTP/1.1" 200 512
13.107.21.200 - [07/Aug/2025:22:03:31 +0000] "GET http://example.com/about HTTP/1.1" 200 512
8.8.8.8 - [01/Aug/2025:12:12:46 +0000] "GET http://wikimedia.org/index.html HTTP/1.1" 200 512
13.107.21.200 - [10/Aug/2025:11:00:23 +0000] "GET http://openai.com/contact HTTP/1.1" 200 512
142.250.182.4 - [01/Aug/2025:11:35:55 +0000] "GET http://example.com/about HTTP/1.1" 200 512
45.77.23.12 - [07/Aug/2025:19:09:42 +0000] "GET http://malicious-site.ru/uploadfile=webshell.php HTTP/1.1" 200 512
13.107.21.200 - [07/Aug/2025:14:52:54 +0000] "GET http://wikimedia.org/contact HTTP/1.1" 200 512
8.8.8.8 - [08/Aug/2025:12:13:12 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
142.250.182.4 - [06/Aug/2025:17:06:57 +0000] "GET http://wikimedia.org/index.html HTTP/1.1" 200 512
8.8.8.8 - [01/Aug/2025:15:46:00 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
45.77.23.12 - [06/Aug/2025:13:34:18 +0000] "GET http://malicious-site.ru/admin/login.php HTTP/1.1" 200 512
8.8.8.8 - [05/Aug/2025:06:20:52 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
13.107.21.200 - [05/Aug/2025:17:16:38 +0000] "GET http://wikimedia.org/contact HTTP/1.1" 200 512
8.8.8.8 - [10/Aug/2025:01:45:50 +0000] "GET http://wikimedia.org/index.html HTTP/1.1" 200 512
8.8.8.8 - [05/Aug/2025:10:49:01 +0000] "GET http://example.com/about HTTP/1.1" 200 512
```

▼ access_log_3.log

```
(jynx@kali)-[~/Desktop/Linux/august10]
└─$ cat access_log.3.log
8.8.8.8 - - [01/Aug/2025:11:53:01 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
13.107.21.200 - - [03/Aug/2025:09:23:52 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
142.256.182.4 - - [09/Aug/2025:11:14:54 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
142.256.182.4 - - [03/Aug/2025:11:23:42:58 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
142.256.182.4 - - [03/Aug/2025:09:47:37 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
8.8.8.8 - - [01/Aug/2025:16:44:26 +0000] "GET http://wikipedia.org/index.html HTTP/1.1" 200 512
8.8.8.8 - - [07/Aug/2025:03:10:28 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
142.256.182.4 - - [04/Aug/2025:03:10:14 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
142.256.182.4 - - [06/Aug/2025:11:14:22 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
13.107.21.200 - - [03/Aug/2025:19:38:42 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
8.8.8.8 - - [06/Aug/2025:01:21:31 +0000] "GET http://example.com/about HTTP/1.1" 200 512
8.8.8.8 - - [04/Aug/2025:16:26:35 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
13.107.21.200 - - [03/Aug/2025:17:41:59 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
13.107.21.200 - - [02/Aug/2025:15:23:27 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
8.8.8.8 - - [04/Aug/2025:03:25:28 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
8.8.8.8 - - [09/Aug/2025:16:14:41 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
8.8.8.8 - - [04/Aug/2025:16:50:37 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
45.77.23.12 - - [04/Aug/2025:01:40:10 +0000] "GET http://malicious-site.ru/w0-content/plugins/vuln.php HTTP/1.1" 200 512
142.256.182.4 - - [01/Aug/2025:22:13:33 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
142.256.182.4 - - [08/Aug/2025:09:24:07 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
8.8.8.8 - - [08/Aug/2025:18:59:24 +0000] "GET http://openi.com/contact HTTP/1.1" 200 512
142.256.182.4 - - [03/Aug/2025:17:41:59 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
13.107.21.200 - - [03/Aug/2025:06:17:23 +0000] "GET http://example.com/about HTTP/1.1" 200 512
8.8.8.8 - - [03/Aug/2025:18:07:44 +0000] "GET http://wikipedia.org/index.html HTTP/1.1" 200 512
45.77.23.12 - - [06/Aug/2025:15:17:55 +0000] "GET http://data-stealer.net/upload?file=webshell.php HTTP/1.1" 200 512
13.107.21.200 - - [03/Aug/2025:05:32:51 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
13.107.21.200 - - [01/Aug/2025:05:36:55 +0000] "GET http://wikipedia.org/index.html HTTP/1.1" 200 512
45.77.23.12 - - [06/Aug/2025:20:44:30 +0000] "GET http://data-stealer.net/upload?file=webshell.php HTTP/1.1" 200 512
142.256.182.4 - - [01/Aug/2025:11:27:54 +0000] "GET http://data-stealer.net/upload?file=webshell.php HTTP/1.1" 200 512
8.8.8.8 - - [08/Aug/2025:03:05:01 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
103.45.67.89 - - [08/Aug/2025:03:24:05 +0000] "GET http://data-stealer.net/admin/login.php HTTP/1.1" 200 512
45.77.23.12 - - [05/Aug/2025:15:33:41 +0000] "GET http://malicious-site.ru/upload?file=webshell.php HTTP/1.1" 200 512
13.107.21.200 - - [10/Aug/2025:11:01:56 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
13.107.21.200 - - [03/Aug/2025:14:06:45 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
142.256.182.4 - - [02/Aug/2025:06:18:43 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
60.6.10.10 - - [04/Aug/2025:11:27:44 +0000] "GET http://data-stealer.net/upload?file=webshell.php HTTP/1.1" 200 512
142.256.182.4 - - [08/Aug/2025:11:27:04 +0000] "GET http://wikipedia.org/index.html HTTP/1.1" 200 512
8.8.8.8 - - [05/Aug/2025:13:32:43 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
8.8.8.8 - - [08/Aug/2025:07:49:44 +0000] "GET http://wikipedia.org/index.html HTTP/1.1" 200 512
103.45.67.89 - - [08/Aug/2025:07:49:44 +0000] "GET http://malicious-site.ru/download?hash=d7fc9e471194aa8b5b6e47267f03d4a0e2b7db66d962f5a7bdee6f8a7e0 HTTP/1.1" 200 512
142.256.182.4 - - [08/Aug/2025:12:56:25 +0000] "GET http://openai.com/contact HTTP/1.1" 200 512
192.168.56.23 - - [04/Aug/2025:08:58:57 +0000] "GET http://evil-domain.com/upload?file=webshell.php HTTP/1.1" 200 512
13.107.21.200 - - [03/Aug/2025:11:14:22 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
66.102.12.50 - - [03/Aug/2025:00:53:20 +0000] "GET http://evil-domain.com/download?hash=c4088613fea8a8f3de82e1278abb02f HTTP/1.1" 200 512
103.45.67.89 - - [09/Aug/2025:03:08:59 +0000] "GET http://malicious-site.ru/download?hash=44d88612fe8a8af3de82e1278abb02f HTTP/1.1" 200 512
192.168.56.23 - - [03/Aug/2025:12:44:53 +0000] "GET http://hx40.biz/admin/login.php HTTP/1.1" 200 512
8.8.8.8 - - [10/Aug/2025:08:38:36 +0000] "GET http://example.com/index.html HTTP/1.1" 200 512
142.256.182.4 - - [06/Aug/2025:18:16:56 +0000] "GET http://wikipedia.org/index.html HTTP/1.1" 200 512
103.45.67.89 - - [10/Aug/2025:00:17:39 +0000] "GET http://hx40.biz/download?hash=6d7fce9fe471194aa8b5b6e47267f03d4a0e2b7db66d962f5a7bdee6f8a7e0 HTTP/1.1" 200 512
```

▼ Objective(s)

- Extract Unique IP Addresses into .txt file from the log files.**
- Extract Unique Domain Names into .txt file from the log files.**
- Extract MD5 and SHA256 hashed texts.**

▼ Detection Methodology

IOC Type	Regex Pattern Used	Notes
IPv4	r"\b(?:\d{1,3}\.){3}\d{1,3}\b"	Matches all dotted IPv4 addresses
Domain	r"https?:\/\/([\w\.-]+)", re.IGNORECASE	Matches clean & malicious domains
MD5	r"\b[a-fA-F0-9]{32}\b"	Detects MD5 hashes
SHA256	r"\b[a-fA-F0-9]{64}\b"	Detects SHA256 hashes

▼ Scripts & Findings

Language: **Python 3.13.3**

▼ 1. IP Address Extraction

▼ Execution Script:

```

jynx@kali: ~/Desktop/linux/august10
File Actions Edit View Help
GNU nano 8.4
import re
from datetime import datetime
filename = input("Enter your FILE name (.log): ")
ipPattern = re.compile(r"\b(?:\d{1,3}\.){3}\d{1,3}\b")
with open(filename, "r", errors="ignore") as f:
    text = f.read()
IPs = ipPattern.findall(text)
UniqueIPs = sorted(set(IPs)) # set data-types removes duplicates
if IPs:
    print(f"\nTotal {len(IPs)} IP addresses in {filename} found.")
    print(f"\nTotal Unique {len(UniqueIPs)} IP addresses in {filename} found:")
    for ip in UniqueIPs:
        print(" ", ip)
with open("IPsFound.txt", "a") as out:
    out.write("\n" + "="*50 + "\n")
    out.write(f"Results from file: {filename}(Scanned: {datetime.now().strftime('%Y-%m-%d %H:%M:%S')})\n")
    out.write(f"Total {len(IPs)} IP addresses Found.\n")
    out.write(f"Total Unique IP addresses found - {len(UniqueIPs)}:\n")
    for ip in UniqueIPs:
        out.write(ip+"\n")
    out.write("*"*50 + "\n\n")
print("\nResults saved to IPsFound.txt")
else:
    print(f"NO IP address found in {filename}.")

```

Python Script [code]

```

import re
from datetime import datetime

filename = input("Enter your FILE name (.log): ")

ipPattern = re.compile(r"\b(?:\d{1,3}\.){3}\d{1,3}\b")

with open(filename, "r", errors="ignore") as f:
    text = f.read()

IPs = ipPattern.findall(text)
UniqueIPs = sorted(set(IPs)) # set data-types removes duplicates

if IPs:
    print(f"\nTotal {len(IPs)} IP addresses in {filename} found.")
    print(f"\nTotal Unique {len(UniqueIPs)} IP addresses in {filename} found:")
    for ip in UniqueIPs:
        print(" ", ip)

with open("IPsFound.txt", "a") as out:
    out.write("\n" + "="*50 + "\n")
    out.write(f"Results from file: {filename}(Scanned: {datetime.now().strftime('%Y-%m-%d %H:%M:%S')})\n")
    out.write(f"Total {len(IPs)} IP addresses Found.\n")
    out.write(f"Total Unique IP addresses found - {len(UniqueIPs)}:\n")
    for ip in UniqueIPs:
        out.write(ip+"\n")
    out.write("*"*50 + "\n\n")
print("\nResults saved to IPsFound.txt")
else:
    print(f"NO IP address found in {filename}.")

```

```
        out.write(f"Results from file: {filename}(Scanned: {dateime.now().strftime('%Y-%m-%d %H:%M:%S')})\n")
        out.write(f"Total {len(IPs)} IP addresses Found.\n")
        out.write(f"Total Unique IP addresses found - {len(UniqueIPs)}:\n")
        for ip in UniqueIPs:
            out.write(ip+"\n")
            out.write("*50 + "\n\n")
        print("\nResults saved to IPsFound.txt")
else:
    print(f"NO IP address found in {filename}.")
```

▼  **Findings:**

```

[jynx㉿kali)-[~/Desktop/linux/august10]GET http://example.com/index
$ python3 ipFinder.py
Enter your FILE name (.log): access_log_1.log
103.45.67.89 -- [09/Aug/2025:00:25:08 +0000] "GET http://h4x0r.biz/ad
Total 50 IP addresses in access_log_1.log found.
192.168.56.23 -- [07/Aug/2025:12:20:15 +0000] "GET http://h4x0r.biz/w
Total Unique 50 IP addresses in access_log_1.log found://data-stealer
103.45.67.893f6a7f5f90b7e3aee8a8a6f6 HTTP/1.1" 200 512
13.107.21.200 -- [10/Aug/2025:19:30:11 +0000] "GET http://wikipedia.o
142.250.182.4 -- [04/Aug/2025:13:48:53 +0000] "GET http://example.com
192.168.56.23 -- [07/Aug/2025:03:56:32 +0000] "GET http://wikipedia.o
45.77.23.12 -- [04/Aug/2025:19:51:59 +0000] "GET http://openai.com/
66.102.12.54 -- [02/Aug/2025:17:45:39 +0000] "GET http://h4x0r.biz/wp
8.8.8.8.200 -- [10/Aug/2025:01:40:56 +0000] "GET http://wikipedia.o
8.8.8.8 -- [05/Aug/2025:00:27:39 +0000] "GET http://openai.com/contact
Results saved to IPsFound.txt:03:42:24 +0000] "GET http://h4x0r.biz/do
HTTP/1.1" 200 512
[jynx㉿kali)-[~/Desktop/linux/august10]000] "GET http://example.com
$ python3 ipFinder.py
Enter your FILE name (.log): access_log_2.log http://wikipedia.org/con
192.168.56.23 -- [10/Aug/2025:10:33:47 +0000] "GET http://malicious-s
Total 50 IP addresses in access_log_2.log found.
192.168.56.23 -- [08/Aug/2025:03:44:17 +0000] "GET http://h4x0r.biz/d
Total Unique 50 IP addresses in access_log_2.log found:
103.45.67.89 -- [01/Aug/2025:19:35:42 +0000] "GET http://wikipedia.o
13.107.21.200 -- [02/Aug/2025:12:33:49 +0000] "GET http://wikipedia.o
142.250.182.4 [09/Aug/2025:07:49:08 +0000] "GET http://data-stealer.
192.168.56.23
45.77.23.12 -- [03/Aug/2025:12:16:45 +0000] "GET http://data-steale
66.102.12.54
8.8.8.8 -- [01/Aug/2025:23:09:56 +0000] "GET http://wikipedia.org/con
13.107.21.200 -- [07/Aug/2025:18:26:28 +0000] "GET http://example.com
Results saved to IPsFound.txt:20 +0000] "GET http://wikipedia.org/about
8.8.8.8 -- [02/Aug/2025:20:02:37 +0000] "GET http://openai.com/index.
[jynx㉿kali)-[~/Desktop/linux/august10]000] "GET http://example.com
$ python3 ipFinder.py
Enter your FILE name (.log): access_log_3.log
8.8.8.8 -- [06/Aug/2025:12:05:17 +0000] "GET http://wikipedia.org/ind
Total 50 IP addresses in access_log_3.log found.
192.168.56.23 -- [01/Aug/2025:13:38:08 +0000] "GET http://example.com
Total Unique 50 IP addresses in access_log_3.log found://h4x0r.biz/wp-
103.45.67.894/Aug/2025:21:35:30 +0000] "GET http://openai.com/index.
13.107.21.200 -- [06/Aug/2025:08:15:13 +0000] "GET http://h4x0r.biz/u
142.250.182.4 -- [09/Aug/2025:09:25:38 +0000] "GET http://h4x0r.biz/wp
192.168.56.23 -- [08/Aug/2025:04:54:06 +0000] "GET http://data-stealer
45.77.23.12 3f6a7f5f90b7e3aee8a8a6f6 HTTP/1.1" 200 512
66.102.12.54 -- [05/Aug/2025:06:09:17 +0000] "GET http://wikipedia.o
8.8.8.8.200 -- [06/Aug/2025:12:03:49 +0000] "GET http://openai.com/
13.107.21.200 -- [04/Aug/2025:14:15:20 +0000] "GET http://wikipedia.o
Results saved to IPsFound.txt:03:42:35 +0000] "GET http://example.com

```

Extracted IPs:

```

(jynx㉿kali)-[~/Desktop/linux/august10] $ cat IPsFound.txt
$ cat IPsFound.txt
142.250.182.4 - - [04/Aug/2025:13:48:53 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
142.250.182.4 - - [04/Aug/2025:13:48:53 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
142.250.182.4 - - [04/Aug/2025:13:48:53 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
Results from file: access_log_1.log(Scanned: 2025-08-10 16:58:30).com/about
Total 50 IP addresses Found.
Total Unique IP addresses found - 7:56 +0000] "GET http://h4x0r.biz/wp-content/themes/h4x0r/ 200 512
103.45.67.89 [05/Aug/2025:00:27:39 +0000] "GET http://openai.com/contact HTTP/1.1" 200 512
13.107.21.200 - - [07/Aug/2025:03:42:24 +0000] "GET http://h4x0r.biz/download/ 200 512
142.250.182.4 512
192.168.56.23 - - [03/Aug/2025:07:10:53 +0000] "GET http://example.com/index.html" 200 512
45.77.23.12.4 - - [05/Aug/2025:23:02:57 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
66.102.12.54 [10/Aug/2025:15:16:34 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
8.8.8.8 56.23 - - [10/Aug/2025:10:33:47 +0000] "GET http://malicious-site.com/index.php" 200 512
192.168.56.23 - - [08/Aug/2025:03:44:17 +0000] "GET http://h4x0r.biz/download/d430e7fb/db66d962f5a7bdee6f8a7e0 HTTP/1.1" 200 512
Results from file: access_log_2.log(Scanned: 2025-08-10 16:58:45).com/about
Total 50 IP addresses Found.
Total Unique IP addresses found - 7:
103.45.67.89 - - [03/Aug/2025:12:16:45 +0000] "GET http://data-stealer.net/index.html" 200 512
13.107.21.200
142.250.182.4 [1/Aug/2025:23:09:56 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
192.168.56.23 - - [07/Aug/2025:18:26:28 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
45.77.23.12 [06/Aug/2025:19:28:20 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
66.102.12.54 [02/Aug/2025:20:02:37 +0000] "GET http://openai.com/index.htm 200 512
8.8.8.8 1.200 - - [06/Aug/2025:23:03:11 +0000] "GET http://example.com/index.php" 200 512
Results from file: access_log_3.log(Scanned: 2025-08-10 16:58:53)
Total 50 IP addresses Found.
Total Unique IP addresses found - 7:000
103.45.67.89 - - [06/Aug/2025:08:15:13 +0000] "GET http://h4x0r.biz/upload/ 200 512
13.107.21.200 - - [09/Aug/2025:09:25:38 +0000] "GET http://h4x0r.biz/wp-content/themes/h4x0r/ 200 512
142.250.182.4 - - [08/Aug/2025:04:54:06 +0000] "GET http://data-stealer.net/index.html" 200 512
192.168.56.23 3f6a7f5f90b7e3aee8a8a6f6 HTTP/1.1" 200 512
45.77.23.12.4 - - [05/Aug/2025:06:09:17 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
66.102.12.54 - - [06/Aug/2025:12:03:49 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
8.8.8.8 1.200 - - [04/Aug/2025:14:15:20 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512

```

▼ 2. Domain Name Extraction

▼ Execution Script:

```

jynx@kali: ~/Desktop/linux/august10
File Actions Edit View Help
GNU nano 8.4
import re
from datetime import datetime

filename = input("Enter your FILE name (.log): ")
domainPattern = re.compile(r"https?://([\w\.-]+)", re.IGNORECASE)
with open(filename, "r", errors="ignore") as f:
    text = f.read()
domains = domainPattern.findall(text)
unique_domains = sorted(set(domains))
if domains:
    print(f"\nTotal {len(domains)} domains in {filename} found.")
    print(f"\nTotal Unique {len(unique_domains)} domains in {filename} found:")
    for domain in unique_domains:
        print(" ", domain)
with open("DomainsFound.txt", "a") as out:
    out.write("\n" + "="*50 + "\n")
    out.write(f"Domain Results from file: {filename} (Scanned: {datetime.now().strftime('%Y-%m-%d %H:%M:%S')})\n")
    out.write(f"Total {len(domains)} domains found.\n")
    out.write(f"Total Unique domains found - {len(unique_domains)}:\n")
    for domain in unique_domains:
        out.write(domain + "\n")
print("\nDomain results appended to DomainsFound.txt")
else:
    print(f"NO domains found in {filename}.")

```

Python Script:

```

import re
from datetime import datetime

filename = input("Enter your FILE name (.log): ")

domainPattern = re.compile(r"https?://([\w\.-]+)", re.IGNORECASE)

with open(filename, "r", errors="ignore") as f:
    text = f.read()

domains = domainPattern.findall(text)
unique_domains = sorted(set(domains))

if domains:
    print(f"\nTotal {len(domains)} domains in {filename} found.")
    print(f"\nTotal Unique {len(unique_domains)} domains in {filename} found:")
    for domain in unique_domains:
        print(" ", domain)
with open("DomainsFound.txt", "a") as out:
    out.write("\n" + "="*50 + "\n")
    out.write(f"Domain Results from file: {filename} (Scanned: {datetime.now().strftime('%Y-%m-%d %H:%M:%S')})\n")
    out.write(f"Total {len(domains)} domains found.\n")
    out.write(f"Total Unique domains found - {len(unique_domains)}:\n")
    for domain in unique_domains:
        out.write(domain + "\n")
print("\nDomain results appended to DomainsFound.txt")
else:
    print(f"NO domains found in {filename}.")

```

```
{datetime.now().strftime('%Y-%m-%d %H:%M:%S'))}\n")  
    out.write(f"Total {len(domains)} domains found.\n")  
    out.write(f"Total Unique domains found - {len(unique_domains)}:\n")  
    for domain in unique_domains:  
        out.write(domain + "\n")  
    out.write("=*50 + "\n\n")  
  
    print("\nDomain results appended to DomainsFound.txt")  
  
else:  
    print(f"NO domains found in {filename}.")
```

▼  **Findings:**

```
[jynx㉿kali)-[~/Desktop/linux/august10]$ python3 domainFinder.py
Enter your FILE name (.log): access_log_1.log
Total 50 domains in access_log_1.log found.
Total Unique 6 domains in access_log_1.log found:
data-stealer.net [07/Aug/2025:12:20:15 +0000] "GET http://h4x0r.biz
example.com - - [01/Aug/2025:01:45:28 +0000] "GET http://data-stealer.net
h4x0r.biz [f33F6a7f5F90b7e3aee8a8a6f6 HTTP/1.1" 200 512
malicious-site.ru [0/Aug/2025:19:30:11 +0000] "GET http://wikipedia.org
openai.com - - [04/Aug/2025:13:48:53 +0000] "GET http://example.com
wikipedia.org - [07/Aug/2025:03:56:32 +0000] "GET http://h4x0r.biz
142.250.182.4 - - [04/Aug/2025:19:51:59 +0000] "GET http://openai.com
Domain results appended to DomainsFound.txt
[jynx㉿kali)-[~/Desktop/linux/august10]$ python3 domainFinder.py
Enter your FILE name (.log): access_log_2.log
Total 50 domains in access_log_2.log found.
Total Unique 7 domains in access_log_2.log found:
data-stealer.net [08/Aug/2025:03:44:17 +0000] "GET http://evil-domain.com
example.com [d962f5a7bdee6f8a7e0 HTTP/1.1" 200 512
h4x0r.biz [0 - - [01/Aug/2025:19:35:42 +0000] "GET http://wikipedia.org
malicious-site.ru [02/Aug/2025:12:33:49 +0000] "GET http://openai.com
openai.com - [09/Aug/2025:07:49:08 +0000] "GET http://data-stealer.net
wikipedia.org
192.168.56.23 - - [03/Aug/2025:12:16:45 +0000] "GET http://data-stealer.net
Domain results appended to DomainsFound.txt
[jynx㉿kali)-[~/Desktop/linux/august10]$ python3 domainFinder.py
Enter your FILE name (.log): access_log_3.log
Total 50 domains in access_log_3.log found.
Total Unique 7 domains in access_log_3.log found:
data-stealer.net [03/Aug/2025:20:23:36 +0000] "GET http://evil-domain.com
example.com - [03/Aug/2025:13:21:19 +0000] "GET http://h4x0r.biz
h4x0r.biz [04/Aug/2025:21:35:30 +0000] "GET http://openai.com
malicious-site.ru [06/Aug/2025:08:15:13 +0000] "GET http://wikipedia.org
openai.com - - [09/Aug/2025:09:25:38 +0000] "GET http://h4x0r.biz
wikipedia.org - [08/Aug/2025:04:54:06 +0000] "GET http://data-stealer.net
Domain results appended to DomainsFound.txt
```

Extracted Domain(s):

```
(jynx㉿kali)-[~/Desktop/linux/august10]000] "GET http://wikipedia.org/index.html
$ cat DomainsFound.txt
[07/Aug/2025:03:48:53 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
[07/Aug/2025:03:56:32 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
[07/Aug/2025:03:42:24 +0000] "GET http://h4x0r.biz/download?hash=d4a0e22b7db66d962f5a7bdee6f8a7e0" HTTP/1.1" 200 512
[07/Aug/2025:03:10:53 +0000] "GET http://example.com/index.html" HTTP/1.1" 200 512
[05/Aug/2025:23:02:57 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
[10/Aug/2025:15:16:34 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
[10/Aug/2025:10:33:47 +0000] "GET http://malicious-site.ru/upload" HTTP/1.1" 200 512
[08/Aug/2025:03:44:17 +0000] "GET http://h4x0r.biz/download?hash=d4a0e22b7db66d962f5a7bdee6f8a7e0" HTTP/1.1" 200 512
[07/Aug/2025:12:16:45 +0000] "GET http://data-stealer.net/upload" HTTP/1.1" 200 512
[01/Aug/2025:23:09:56 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
[07/Aug/2025:18:26:28 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
[05/Aug/2025:19:28:20 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
[02/Aug/2025:20:02:37 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
[06/Aug/2025:23:03:11 +0000] "GET http://example.com/index.html" HTTP/1.1" 200 512
[01/Aug/2025:09:52:20 +0000] "GET http://example.com/about HTTP/1.1" 200 512
[06/Aug/2025:12:05:17 +0000] "GET http://wikipedia.org/index.html" HTTP/1.1" 200 512
[06/Aug/2025:09:15:38 +0000] "GET http://h4x0r.biz/wp-content/plugins" HTTP/1.1" 200 512
[06/Aug/2025:08:15:13 +0000] "GET http://openai.com/index.html" HTTP/1.1" 200 512
[09/Aug/2025:09:15:38 +0000] "GET http://h4x0r.biz/upload?file=sd3f33f6a7f5f90b7e3aee8a8a6f6" HTTP/1.1" 200 512
[08/Aug/2025:04:54:06 +0000] "GET http://data-stealer.net/download" HTTP/1.1" 200 512
[05/Aug/2025:06:09:17 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
[06/Aug/2025:12:03:49 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
[04/Aug/2025:14:15:20 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
[04/Aug/2025:14:15:20 +0000] "GET http://example.com/index.html" HTTP/1.1" 200 512

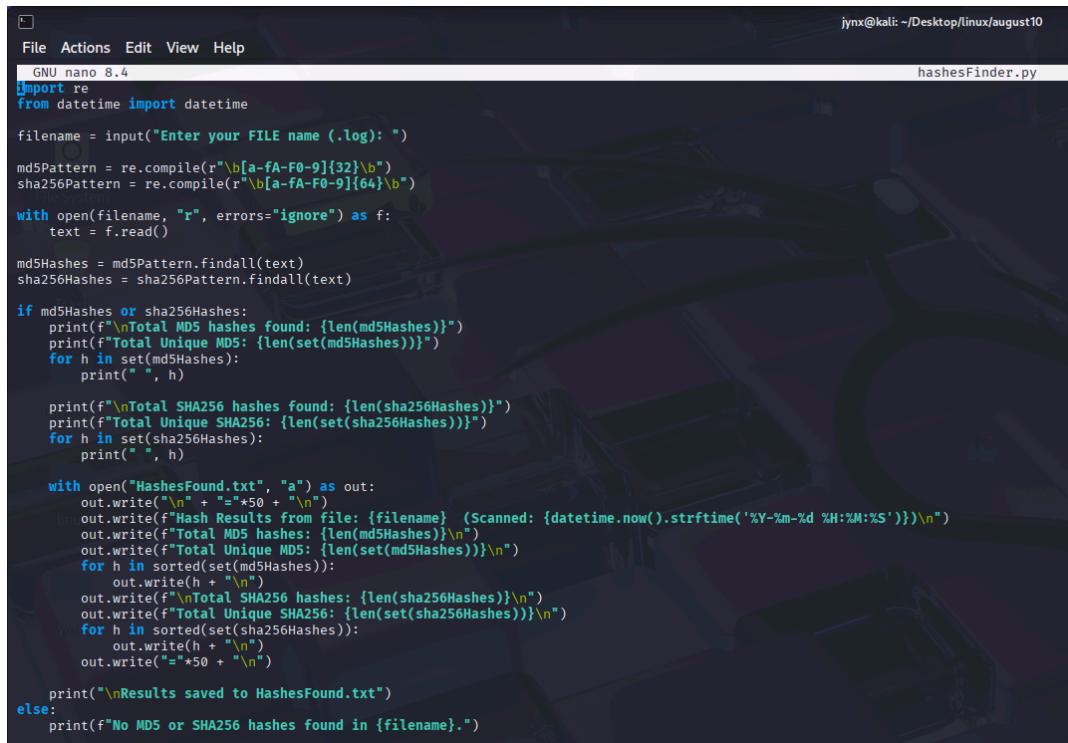
Domain Results from file: access_log_1.log (Scanned: 2025-08-10 17:42:14)
Total 50 domains found.
Total Unique domains found - 26:
data-stealer.net [07/Aug/2025:03:42:24 +0000] "GET http://h4x0r.biz/download?hash=d4a0e22b7db66d962f5a7bdee6f8a7e0" HTTP/1.1" 200 512
example.com [0 512]
h4x0r.biz [2.4 -- [03/Aug/2025:07:10:53 +0000] "GET http://example.com/index.html" HTTP/1.1" 200 512
malicious-site.ru [05/Aug/2025:23:02:57 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
openai.com [10/Aug/2025:15:16:34 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
wikipedia.org -- [10/Aug/2025:10:33:47 +0000] "GET http://malicious-site.ru/upload" HTTP/1.1" 200 512
[192.168.56.23 -- [08/Aug/2025:03:44:17 +0000] "GET http://h4x0r.biz/download?hash=d4a0e22b7db66d962f5a7bdee6f8a7e0" HTTP/1.1" 200 512
[07/Aug/2025:07:49:08 +0000] "GET http://data-stealer.net/wp-content" HTTP/1.1" 200 512
[03/Aug/2025:12:16:45 +0000] "GET http://data-stealer.net/upload" HTTP/1.1" 200 512
[01/Aug/2025:23:09:56 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
[07/Aug/2025:18:26:28 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
[05/Aug/2025:19:28:20 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
[02/Aug/2025:20:02:37 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
[06/Aug/2025:23:03:11 +0000] "GET http://example.com/index.html" HTTP/1.1" 200 512
[01/Aug/2025:09:52:20 +0000] "GET http://example.com/about HTTP/1.1" 200 512
[06/Aug/2025:12:05:17 +0000] "GET http://wikipedia.org/index.html" HTTP/1.1" 200 512
[06/Aug/2025:09:15:38 +0000] "GET http://h4x0r.biz/wp-content/plugins" HTTP/1.1" 200 512
[06/Aug/2025:08:15:13 +0000] "GET http://openai.com/index.html" HTTP/1.1" 200 512
[09/Aug/2025:09:15:38 +0000] "GET http://h4x0r.biz/upload?file=sd3f33f6a7f5f90b7e3aee8a8a6f6" HTTP/1.1" 200 512
[08/Aug/2025:04:54:06 +0000] "GET http://data-stealer.net/download" HTTP/1.1" 200 512
[05/Aug/2025:06:09:17 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
[06/Aug/2025:12:03:49 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
[04/Aug/2025:14:15:20 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
[04/Aug/2025:14:15:20 +0000] "GET http://example.com/index.html" HTTP/1.1" 200 512

Domain Results from file: access_log_2.log (Scanned: 2025-08-10 17:42:22)
Total 50 domains found.
Total Unique domains found - 7:
data-stealer.net -- [03/Aug/2025:12:16:45 +0000] "GET http://data-stealer.net/upload" HTTP/1.1" 200 512
evil-domain.com
example.com [01/Aug/2025:23:09:56 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
h4x0r.biz [200 -- [07/Aug/2025:18:26:28 +0000] "GET http://example.com/contact HTTP/1.1" 200 512
malicious-site.ru [05/Aug/2025:19:28:20 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
openai.com [02/Aug/2025:20:02:37 +0000] "GET http://openai.com/index.html HTTP/1.1" 200 512
wikipedia.org -- [06/Aug/2025:23:03:11 +0000] "GET http://example.com/index.html" HTTP/1.1" 200 512
[01/Aug/2025:09:52:20 +0000] "GET http://example.com/about HTTP/1.1" 200 512
[06/Aug/2025:12:05:17 +0000] "GET http://wikipedia.org/index.html" HTTP/1.1" 200 512
[06/Aug/2025:09:15:38 +0000] "GET http://h4x0r.biz/wp-content/plugins" HTTP/1.1" 200 512
[06/Aug/2025:08:15:13 +0000] "GET http://openai.com/index.html" HTTP/1.1" 200 512
[09/Aug/2025:09:15:38 +0000] "GET http://h4x0r.biz/upload?file=sd3f33f6a7f5f90b7e3aee8a8a6f6" HTTP/1.1" 200 512
[08/Aug/2025:04:54:06 +0000] "GET http://data-stealer.net/download" HTTP/1.1" 200 512
[05/Aug/2025:06:09:17 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
[06/Aug/2025:12:03:49 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
[04/Aug/2025:14:15:20 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
[04/Aug/2025:14:15:20 +0000] "GET http://example.com/index.html" HTTP/1.1" 200 512

Domain Results from file: access_log_3.log (Scanned: 2025-08-10 17:42:37)
Total 50 domains found.
Total Unique domains found - 7:
data-stealer.net [06/Aug/2025:08:15:13 +0000] "GET http://openai.com/index.html" HTTP/1.1" 200 512
evil-domain.com [09/Aug/2025:09:15:38 +0000] "GET http://h4x0r.biz/wp-content/plugins" HTTP/1.1" 200 512
example.com -- [08/Aug/2025:04:54:06 +0000] "GET http://data-stealer.net/download" HTTP/1.1" 200 512
h4x0r.biz [sd3f33f6a7f5f90b7e3aee8a8a6f6 HTTP/1.1" 200 512
malicious-site.ru [05/Aug/2025:06:09:17 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
openai.com [00 -- [06/Aug/2025:12:03:49 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
wikipedia.org -- [04/Aug/2025:14:15:20 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
[01/Aug/2025:09:52:20 +0000] "GET http://example.com/about HTTP/1.1" 200 512
[06/Aug/2025:12:05:17 +0000] "GET http://wikipedia.org/index.html" HTTP/1.1" 200 512
[06/Aug/2025:09:15:38 +0000] "GET http://h4x0r.biz/wp-content/plugins" HTTP/1.1" 200 512
[06/Aug/2025:08:15:13 +0000] "GET http://openai.com/index.html" HTTP/1.1" 200 512
[09/Aug/2025:09:15:38 +0000] "GET http://h4x0r.biz/upload?file=sd3f33f6a7f5f90b7e3aee8a8a6f6" HTTP/1.1" 200 512
[08/Aug/2025:04:54:06 +0000] "GET http://data-stealer.net/download" HTTP/1.1" 200 512
[05/Aug/2025:06:09:17 +0000] "GET http://wikipedia.org/about HTTP/1.1" 200 512
[06/Aug/2025:12:03:49 +0000] "GET http://openai.com/about HTTP/1.1" 200 512
[04/Aug/2025:14:15:20 +0000] "GET http://wikipedia.org/contact HTTP/1.1" 200 512
[04/Aug/2025:14:15:20 +0000] "GET http://example.com/index.html" HTTP/1.1" 200 512
```

▼ 3. MD5 and SHA256 Extraction

▼ Execution Script:



```

File Actions Edit View Help
GNU nano 8.4
jynx@kali: ~/Desktop/linux/august10
hashesFinder.py

import re
from datetime import datetime

filename = input("Enter your FILE name (.log): ")

md5Pattern = re.compile(r"\b[a-fA-F0-9]{32}\b")
sha256Pattern = re.compile(r"\b[a-fA-F0-9]{64}\b")

with open(filename, "r", errors="ignore") as f:
    text = f.read()

md5Hashes = md5Pattern.findall(text)
sha256Hashes = sha256Pattern.findall(text)

if md5Hashes or sha256Hashes:
    print(f"\nTotal MD5 hashes found: {len(md5Hashes)}")
    print(f"Total Unique MD5: {len(set(md5Hashes))}")
    for h in set(md5Hashes):
        print(" ", h)

    print(f"\nTotal SHA256 hashes found: {len(sha256Hashes)}")
    print(f"Total Unique SHA256: {len(set(sha256Hashes))}")
    for h in set(sha256Hashes):
        print(" ", h)

    with open("HashesFound.txt", "a") as out:
        out.write("\n" + "="*50 + "\n")
        out.write(f"Hashes found from file: {filename} (Scanned: {datetime.now().strftime('%Y-%m-%d %H:%M:%S')})\n")
        out.write(f"Total MD5 hashes: {len(md5Hashes)}\n")
        out.write(f"Total Unique MD5: {len(set(md5Hashes))}\n")
        for h in sorted(set(md5Hashes)):
            out.write(h + "\n")
        out.write(f"\nTotal SHA256 hashes: {len(sha256Hashes)}\n")
        out.write(f"Total Unique SHA256: {len(set(sha256Hashes))}\n")
        for h in sorted(set(sha256Hashes)):
            out.write(h + "\n")
        out.write("=".join(["="]*50))

    print("\nResults saved to HashesFound.txt")
else:
    print(f"No MD5 or SHA256 hashes found in {filename}.")

```

Python Script:

```

import re
from datetime import datetime

filename = input("Enter your FILE name (.log): ")

md5Pattern = re.compile(r"\b[a-fA-F0-9]{32}\b")
sha256Pattern = re.compile(r"\b[a-fA-F0-9]{64}\b")

with open(filename, "r", errors="ignore") as f:
    text = f.read()

md5Hashes = md5Pattern.findall(text)
sha256Hashes = sha256Pattern.findall(text)

if md5Hashes or sha256Hashes:
    print(f"\nTotal MD5 hashes found: {len(md5Hashes)}")
    print(f"Total Unique MD5: {len(set(md5Hashes))}")
    for h in set(md5Hashes):
        print(" ", h)

    print(f"\nTotal SHA256 hashes found: {len(sha256Hashes)}")
    print(f"Total Unique SHA256: {len(set(sha256Hashes))}")
    for h in set(sha256Hashes):
        print(" ", h)

else:
    print(f"No MD5 or SHA256 hashes found in {filename}.")

```

```
print(f"\nTotal SHA256 hashes found: {len(sha256Hashes)}")
print(f"Total Unique SHA256: {len(set(sha256Hashes))}")
for h in set(sha256Hashes):
    print(" ", h)

with open("HashesFound.txt", "a") as out:
    out.write("\n" + "="*50 + "\n")
    out.write(f"Hash Results from file: {filename} (Scanned: {datetime.now().strftime('%Y-%m-%d %H:%M:%S')})\n")
    out.write(f"Total MD5 hashes: {len(md5Hashes)}\n")
    out.write(f"Total Unique MD5: {len(set(md5Hashes))}\n")
    for h in sorted(set(md5Hashes)):
        out.write(h + "\n")
    out.write(f"\nTotal SHA256 hashes: {len(sha256Hashes)}\n")
    out.write(f"Total Unique SHA256: {len(set(sha256Hashes))}\n")
    for h in sorted(set(sha256Hashes)):
        out.write(h + "\n")
    out.write("=".join(["="]*50) + "\n")

print("\nResults saved to HashesFound.txt")
else:
    print(f"No MD5 or SHA256 hashes found in {filename}.")
```

▼ Findings:

```
(jynx㉿kali)-[~/Desktop/linux/august10]
└─$ python3 hashesFinder.py
Enter your FILE name (.log): access_log_1.log

Total MD5 hashes found: 2
Total Unique MD5: 2
    5d41402abc4b2a76b9719d911017c592
    44d88612fea8a8f36de82e1278abb02f

Total SHA256 hashes found: 3
Total Unique SHA256: 2
    6d7fce9fee471194aa8b5b6e47267f03d4a0e22b7db66d962f5a7bdee6f8a7e0
    9b74c9897bac770ffc029102a200c5de80dbd3f33f6a7f5f90b7e3aee8a8a6f6

Results saved to HashesFound.txt

(jynx㉿kali)-[~/Desktop/linux/august10]
└─$ python3 hashesFinder.py
Enter your FILE name (.log): access_log_2.log

Total MD5 hashes found: 3
Total Unique MD5: 1
    44d88612fea8a8f36de82e1278abb02f

Total SHA256 hashes found: 0
Total Unique SHA256: 0

Results saved to HashesFound.txt

(jynx㉿kali)-[~/Desktop/linux/august10]
└─$ python3 hashesFinder.py
Enter your FILE name (.log): access_log_3.log

Total MD5 hashes found: 2
Total Unique MD5: 1
    44d88612fea8a8f36de82e1278abb02f

Total SHA256 hashes found: 2
Total Unique SHA256: 1
    6d7fce9fee471194aa8b5b6e47267f03d4a0e22b7db66d962f5a7bdee6f8a7e0

Results saved to HashesFound.txt
```

Extracted MD5 and SHA256 Hashes:

```
(jynx㉿kali)-[~/Desktop/linux/august10]
$ cat HashesFound.txt

=====
Hash Results from file: access_log_1.log (Scanned: 2025-08-10 19:05:30)
Total MD5 hashes: 2
Total Unique MD5: 2
44d88612fea8a8f36de82e1278abb02f
5d41402abc4b2a76b9719d911017c592

Total SHA256 hashes: 3
Total Unique SHA256: 2
6d7fce9fee471194aa8b5b6e47267f03d4a0e22b7db66d962f5a7bdee6f8a7e0
9b74c9897bac770ffc029102a200c5de80dbd3f33f6a7f5f90b7e3aee8a8a6f6
=====

=====

Hash Results from file: access_log_2.log (Scanned: 2025-08-10 19:05:52)
Total MD5 hashes: 3
Total Unique MD5: 1
44d88612fea8a8f36de82e1278abb02f

Total SHA256 hashes: 0
Total Unique SHA256: 0
=====

=====

Hash Results from file: access_log_3.log (Scanned: 2025-08-10 19:06:02)
Total MD5 hashes: 2
Total Unique MD5: 1
44d88612fea8a8f36de82e1278abb02f

Total SHA256 hashes: 2
Total Unique SHA256: 1
6d7fce9fee471194aa8b5b6e47267f03d4a0e22b7db66d962f5a7bdee6f8a7e0
=====
```