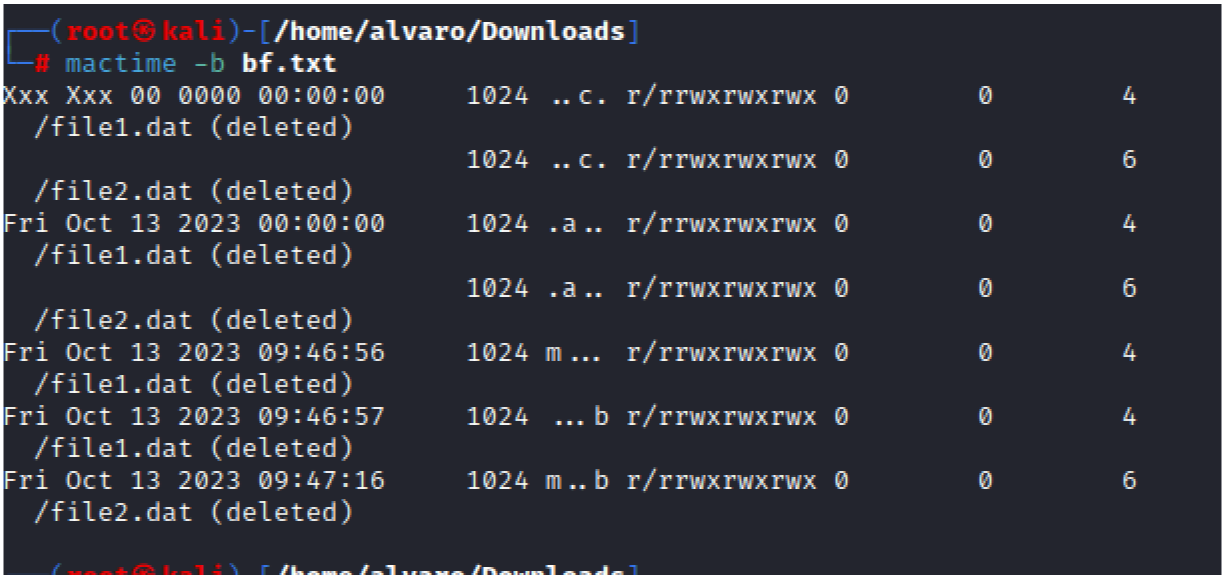
Dikerjakan oleh: Alvaro Austin (2106752180)

Tugas Individu

1. **Exercise 12.5.2**



```
┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# mactime -b bf.txt
Xxx Xxx 00 0000 00:00:00     1024 ..c. r/rrwxrwxrwx 0        0        4
  /file1.dat (deleted)
                             1024 ..c. r/rrwxrwxrwx 0        0        6
  /file2.dat (deleted)
Fri Oct 13 2023 00:00:00     1024 .a.. r/rrwxrwxrwx 0        0        4
  /file1.dat (deleted)
                             1024 .a.. r/rrwxrwxrwx 0        0        6
  /file2.dat (deleted)
Fri Oct 13 2023 09:46:56     1024 m... r/rrwxrwxrwx 0        0        4
  /file1.dat (deleted)
Fri Oct 13 2023 09:46:57     1024 ...b r/rrwxrwxrwx 0        0        4
  /file1.dat (deleted)
Fri Oct 13 2023 09:47:16     1024 m..b r/rrwxrwxrwx 0        0        6
  /file2.dat (deleted)

┌──(root㉿kali)-[/home/alvaro/Downloads]
```

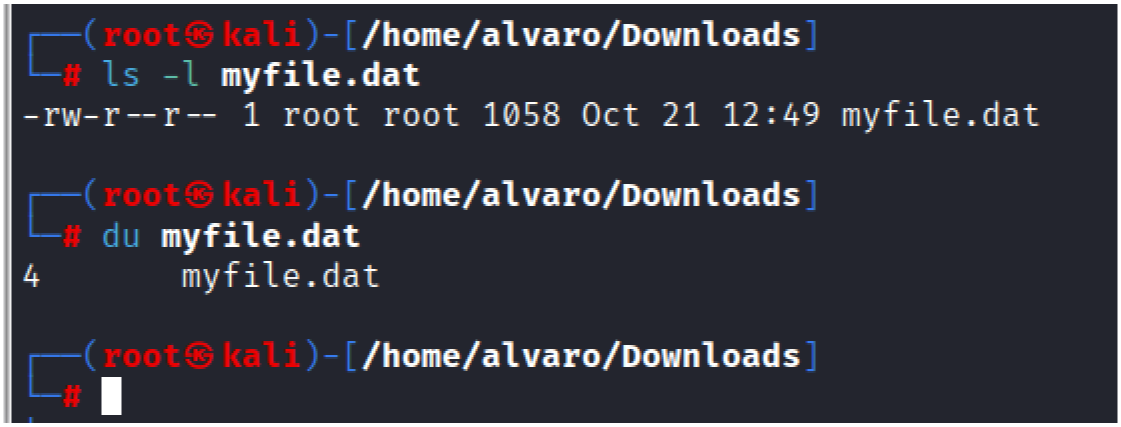
Q1. How many files are found in the image? **2 Files**

Q2. Which file is created first, “file 1.dat” or “file 2.dat”? file 1.dat **was created first** (2023-10-13 09:46:57 (+08)) than file 2.dat (2023-10-13 09:47:16 (+08))

Q3. What is the exact date and time when “file 1.dat” is created?

file 1.dat was created on Friday Oct 13 2023 with a timestamp of 09:46:57 (+08).

2. **Exercise 12.5.2**



```
┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# ls -l myfile.dat
-rw-r--r-- 1 root root 1058 Oct 21 12:49 myfile.dat

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# du myfile.dat
4       myfile.dat

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# 
```

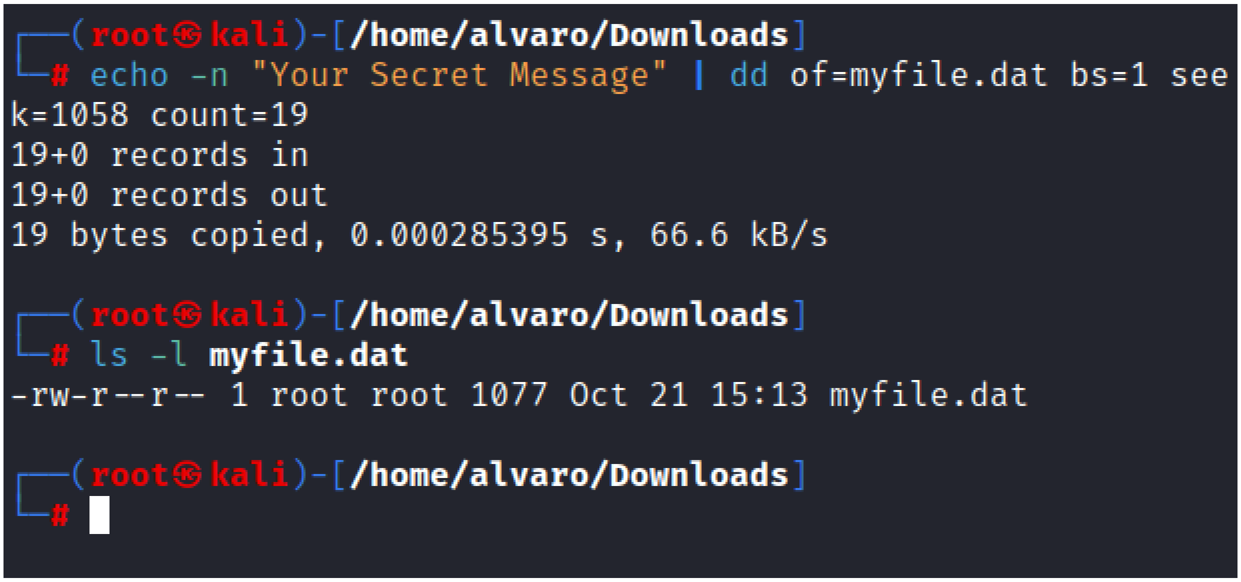
Q1. What is the file size of “myfile.dat"? (in bytes) 1058 bytes

Q2. What is the size of the disk space used by the file “myfile.dat”? (in bytes) 4096 bytes.

Q3. What is the size of slack space for the file? (in bytes) 3038 bytes.

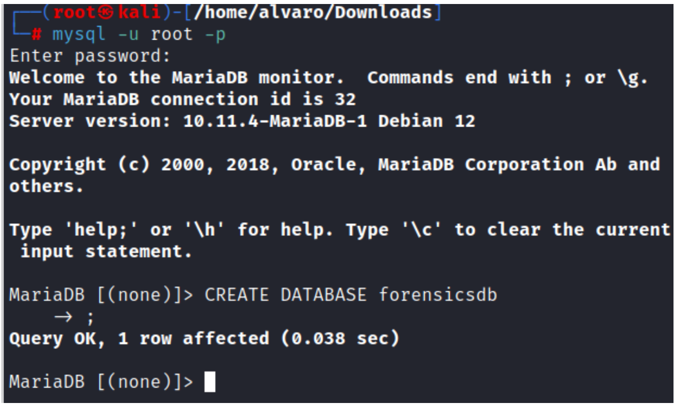
Karena saya tidak berhasil melakukan proses “make” pada bmap (sepertinya datanya corrupt), akhirnya saya menggunakan alternatif lain namun sama outputnya dengan menggunakan bantuan bmap.

Dikerjakan oleh: Alvaro Austin (2106752180)

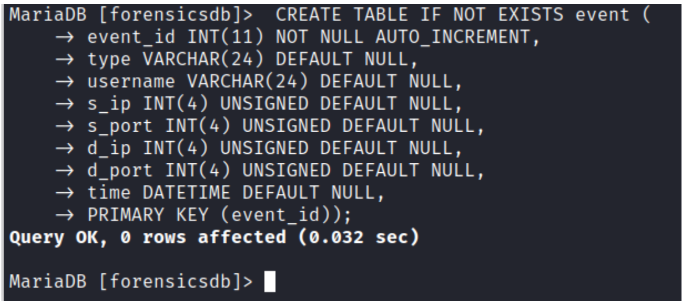


```
┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# echo -n "Your Secret Message" | dd of=myfile.dat bs=1 see
k=1058 count=19
19+0 records in
19+0 records out
19 bytes copied, 0.000285395 s, 66.6 kB/s

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# ls -l myfile.dat
-rw-r--r-- 1 root root 1077 Oct 21 15:13 myfile.dat

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# 
```

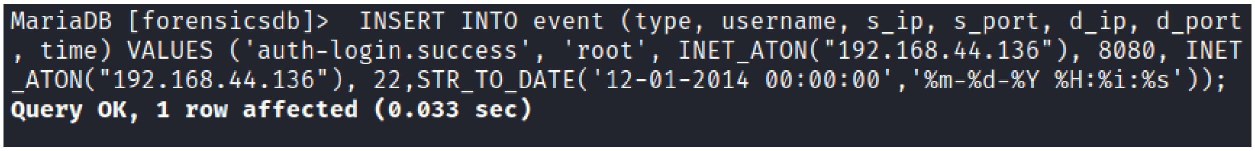
3. **Exercise 14.4.2**



```
┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.11.4-MariaDB-1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and
others.

Type 'help;' or '\h' for help. Type '\c' to clear the current
 input statement.

MariaDB [(none)]> CREATE DATABASE forensicsdb
    → ;
Query OK, 1 row affected (0.038 sec)

MariaDB [(none)]> 
```

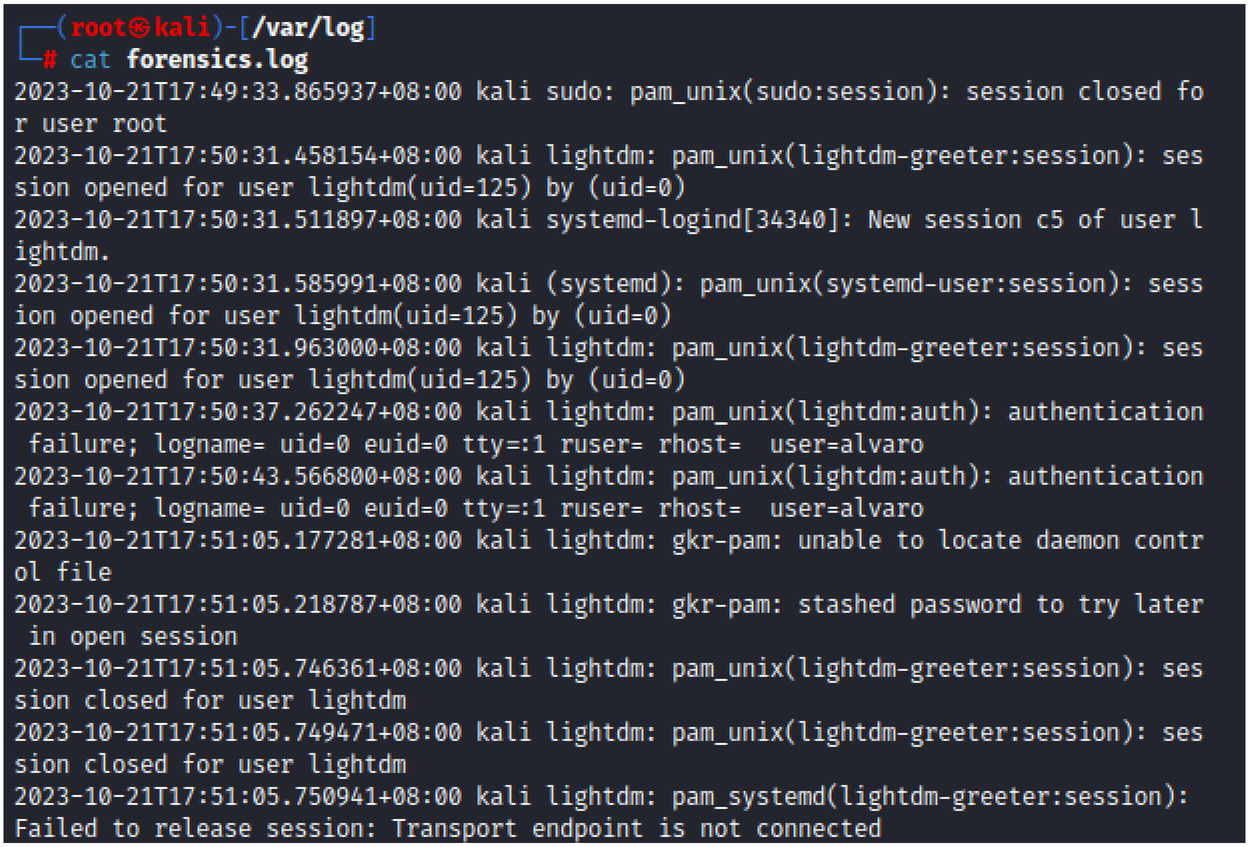


```
MariaDB [forensicsdb]>  CREATE TABLE IF NOT EXISTS event (
    → event_id INT(11) NOT NULL AUTO_INCREMENT,
    → type VARCHAR(24) DEFAULT NULL,
    → username VARCHAR(24) DEFAULT NULL,
    → s_ip INT(4) UNSIGNED DEFAULT NULL,
    → s_port INT(4) UNSIGNED DEFAULT NULL,
    → d_ip INT(4) UNSIGNED DEFAULT NULL,
    → d_port INT(4) UNSIGNED DEFAULT NULL,
    → time DATETIME DEFAULT NULL,
    → PRIMARY KEY (event_id));
Query OK, 0 rows affected (0.032 sec)

MariaDB [forensicsdb]> 
```



```
MariaDB [forensicsdb]>  INSERT INTO event (type, username, s_ip, s_port, d_ip, d_port
, time) VALUES ('auth-login.success', 'root', INET_ATON("192.168.44.136"), 8080, INET
_ATON("192.168.44.136"), 22,STR_TO_DATE('12-01-2014 00:00:00','%m-%d-%Y %H:%i:%s'));
Query OK, 1 row affected (0.033 sec)
```

Dikerjakan oleh: Alvaro Austin (2106752180)

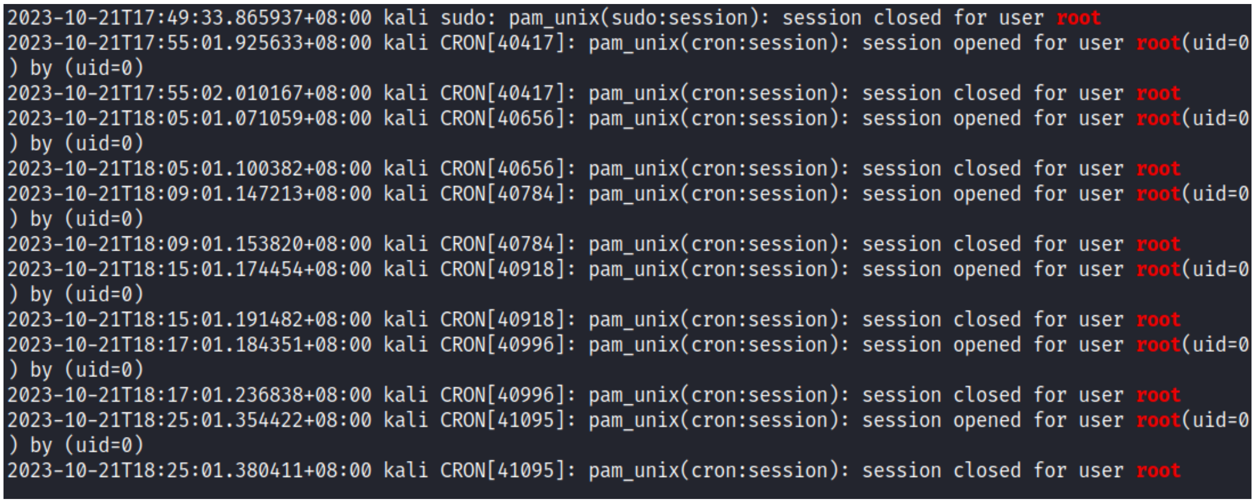


```
┌──(root㉿kali)-[/var/log]
└─# cat forensics.log
2023-10-21T17:49:33.865937+08:00 kali sudo: pam_unix(sudo:session): session closed fo
r user root
2023-10-21T17:50:31.458154+08:00 kali lightdm: pam_unix(lightdm-greeter:session): ses
sion opened for user lightdm(uid=125) by (uid=0)
2023-10-21T17:50:31.511897+08:00 kali systemd-logind[34340]: New session c5 of user l
ightdm.
2023-10-21T17:50:31.585991+08:00 kali (systemd): pam_unix(systemd-user:session): sess
ion opened for user lightdm(uid=125) by (uid=0)
2023-10-21T17:50:31.963000+08:00 kali lightdm: pam_unix(lightdm-greeter:session): ses
sion opened for user lightdm(uid=125) by (uid=0)
2023-10-21T17:50:37.262247+08:00 kali lightdm: pam_unix(lightdm:auth): authentication
 failure; logname= uid=0 euid=0 tty=:1 ruser= rhost=  user=alvaro
2023-10-21T17:50:43.566800+08:00 kali lightdm: pam_unix(lightdm:auth): authentication
 failure; logname= uid=0 euid=0 tty=:1 ruser= rhost=  user=alvaro
2023-10-21T17:51:05.177281+08:00 kali lightdm: gkr-pam: unable to locate daemon contr
ol file
2023-10-21T17:51:05.218787+08:00 kali lightdm: gkr-pam: stashed password to try later
 in open session
2023-10-21T17:51:05.746361+08:00 kali lightdm: pam_unix(lightdm-greeter:session): ses
sion closed for user lightdm
2023-10-21T17:51:05.749471+08:00 kali lightdm: pam_unix(lightdm-greeter:session): ses
sion closed for user lightdm
2023-10-21T17:51:05.750941+08:00 kali lightdm: pam_systemd(lightdm-greeter:session):
Failed to release session: Transport endpoint is not connected
```

In this part of the exercises, you are required to develop SQL search queries to answer the following questions

Q1. Who logged into Forensics Workstation last night between 9pm and 11pm? **None, because i have not used my forensics workstation between those hours**

Q2. How many failed login attempts since the last successful login of user root? **None**



```
2023-10-21T17:49:33.865937+08:00 kali sudo: pam_unix(sudo:session): session closed for user root
2023-10-21T17:55:01.925633+08:00 kali CRON[40417]: pam_unix(cron:session): session opened for user root(uid=0
) by (uid=0)
2023-10-21T17:55:02.010167+08:00 kali CRON[40417]: pam_unix(cron:session): session closed for user root
2023-10-21T18:05:01.071059+08:00 kali CRON[40656]: pam_unix(cron:session): session opened for user root(uid=0
) by (uid=0)
2023-10-21T18:05:01.100382+08:00 kali CRON[40656]: pam_unix(cron:session): session closed for user root
2023-10-21T18:09:01.147213+08:00 kali CRON[40784]: pam_unix(cron:session): session opened for user root(uid=0
) by (uid=0)
2023-10-21T18:09:01.153820+08:00 kali CRON[40784]: pam_unix(cron:session): session closed for user root
2023-10-21T18:15:01.174454+08:00 kali CRON[40918]: pam_unix(cron:session): session opened for user root(uid=0
) by (uid=0)
2023-10-21T18:15:01.191482+08:00 kali CRON[40918]: pam_unix(cron:session): session closed for user root
2023-10-21T18:17:01.184351+08:00 kali CRON[40996]: pam_unix(cron:session): session opened for user root(uid=0
) by (uid=0)
2023-10-21T18:17:01.236838+08:00 kali CRON[40996]: pam_unix(cron:session): session closed for user root
2023-10-21T18:25:01.354422+08:00 kali CRON[41095]: pam_unix(cron:session): session opened for user root(uid=0
) by (uid=0)
2023-10-21T18:25:01.380411+08:00 kali CRON[41095]: pam_unix(cron:session): session closed for user root
```

Q3. When is the last login time for user root? **October 21, 2023 at 10:25 AM (converted to UTC)**