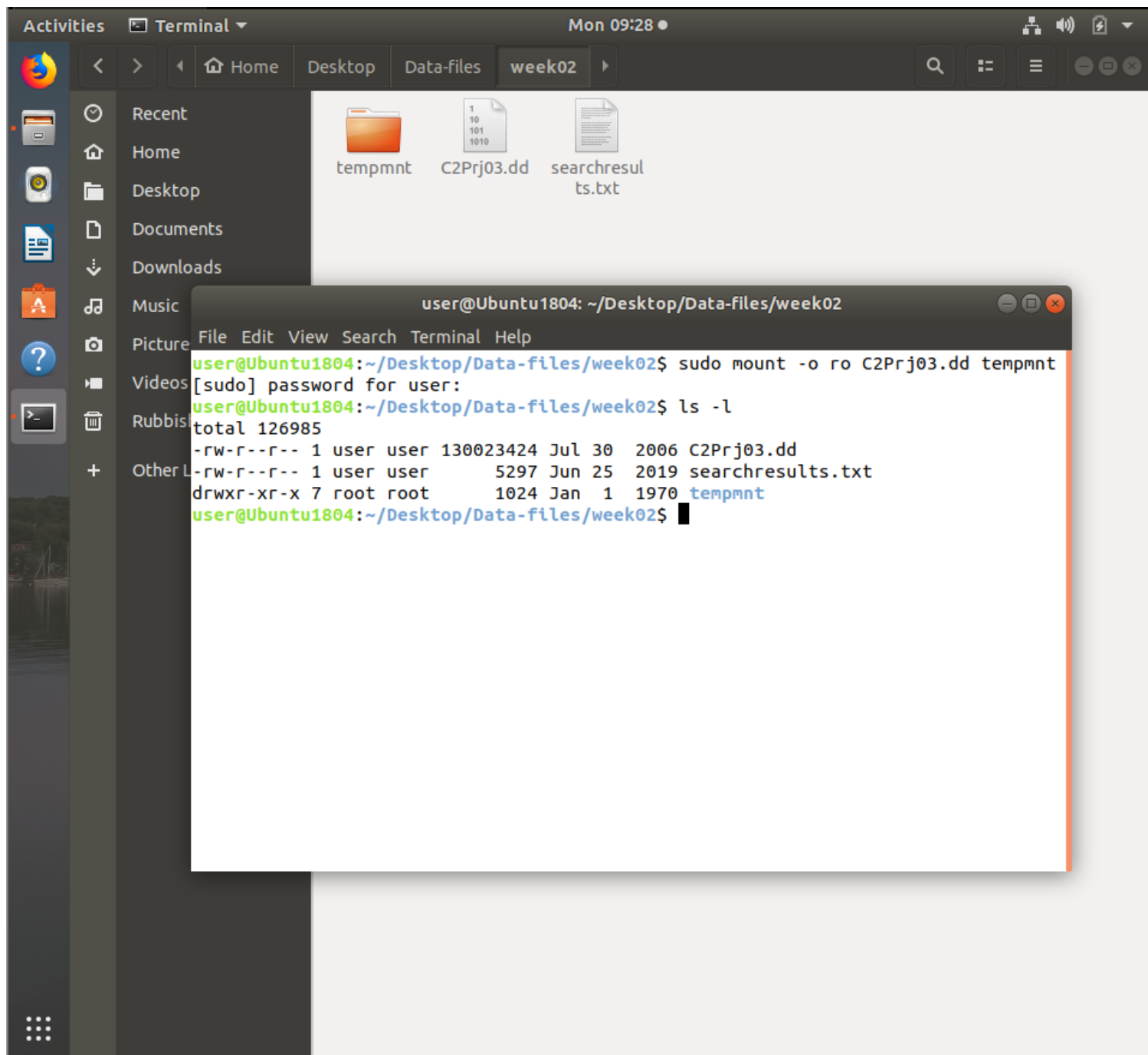
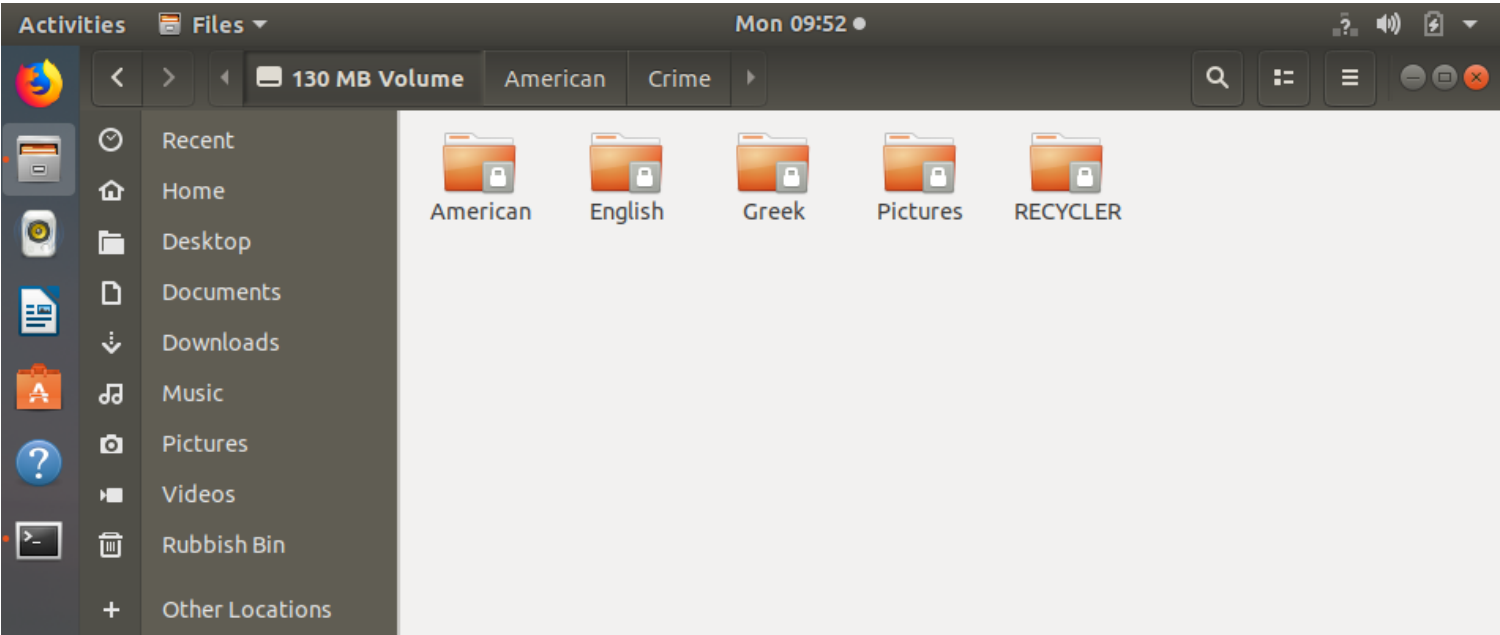


Introducing Linux mount

First, I launched the terminal and navigated to the `~/Desktop/Data files/week02` directory, then typed in the command `"sudo mount -o ro C2Prj03.dd tempmnt"` to mount the image and the mount process will be completed.

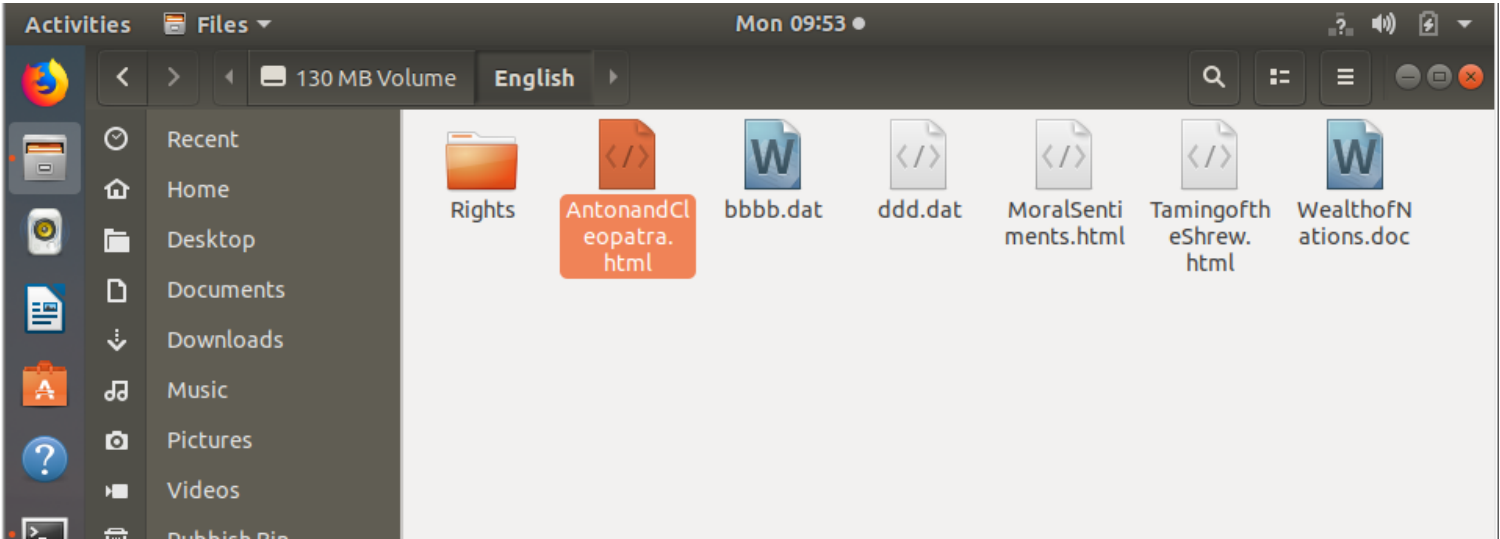


Then I used the file browser tool to navigate through the image. This image contains a few folders with contents and a RECYCLER folder with the information of deleted files.

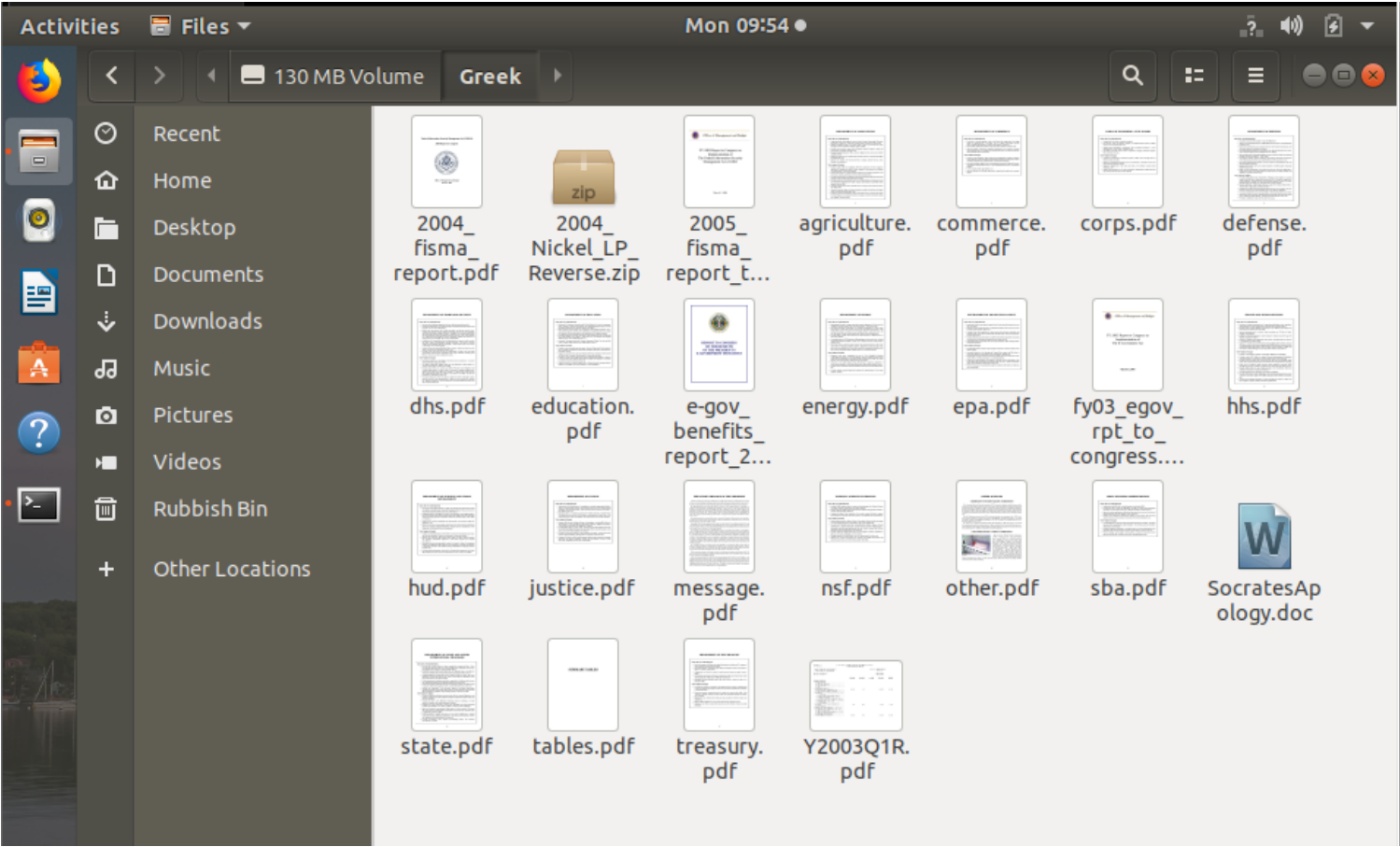


Then I went through all the directories

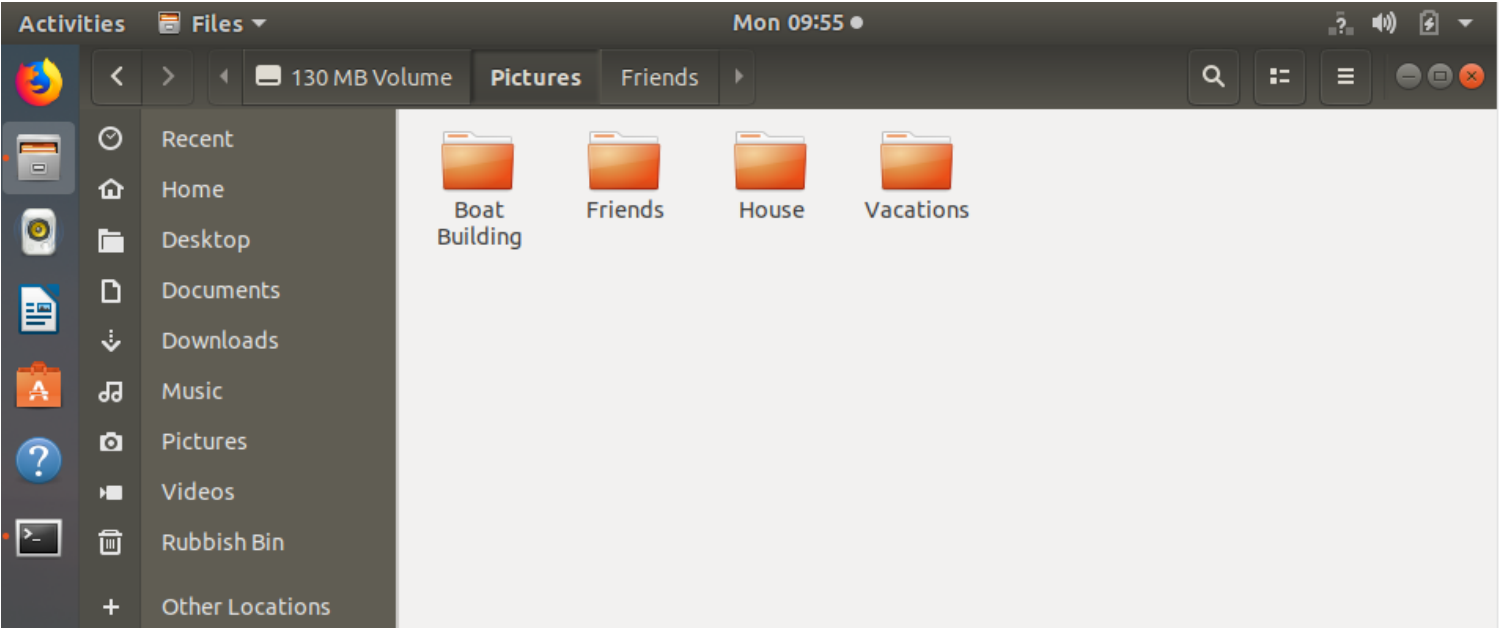
English

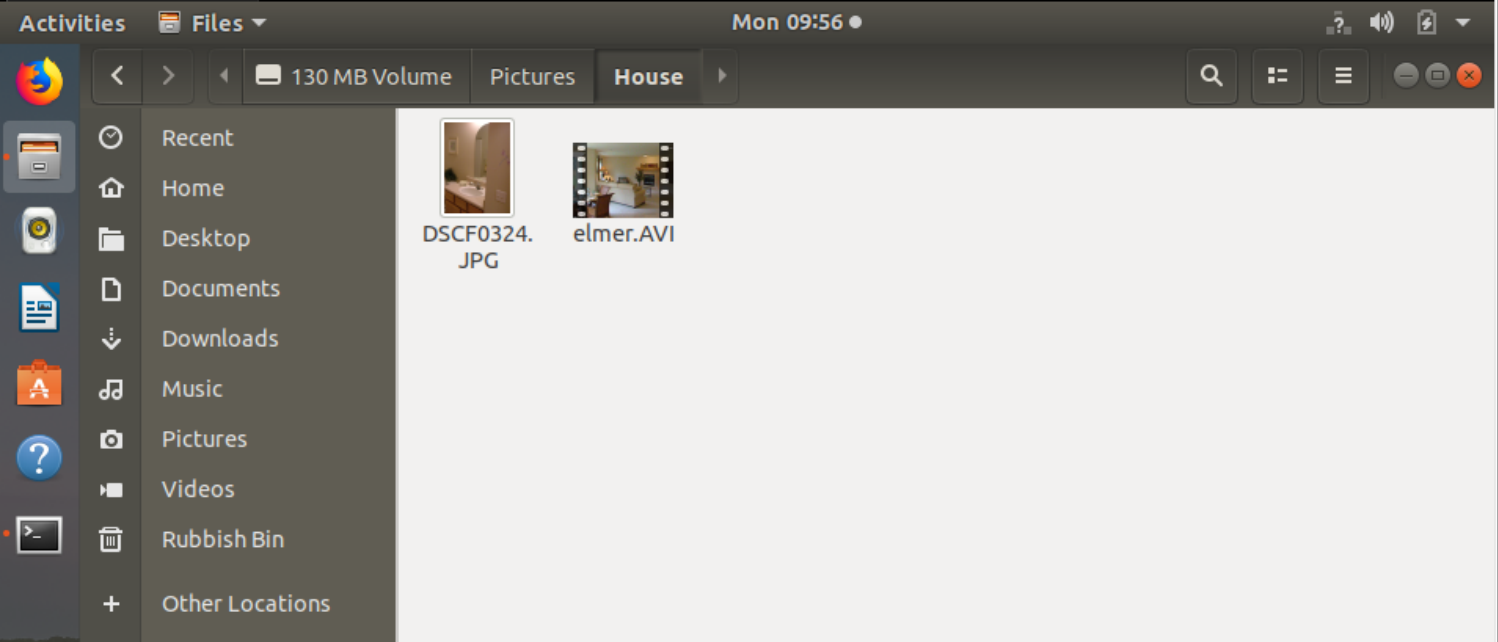


Greek

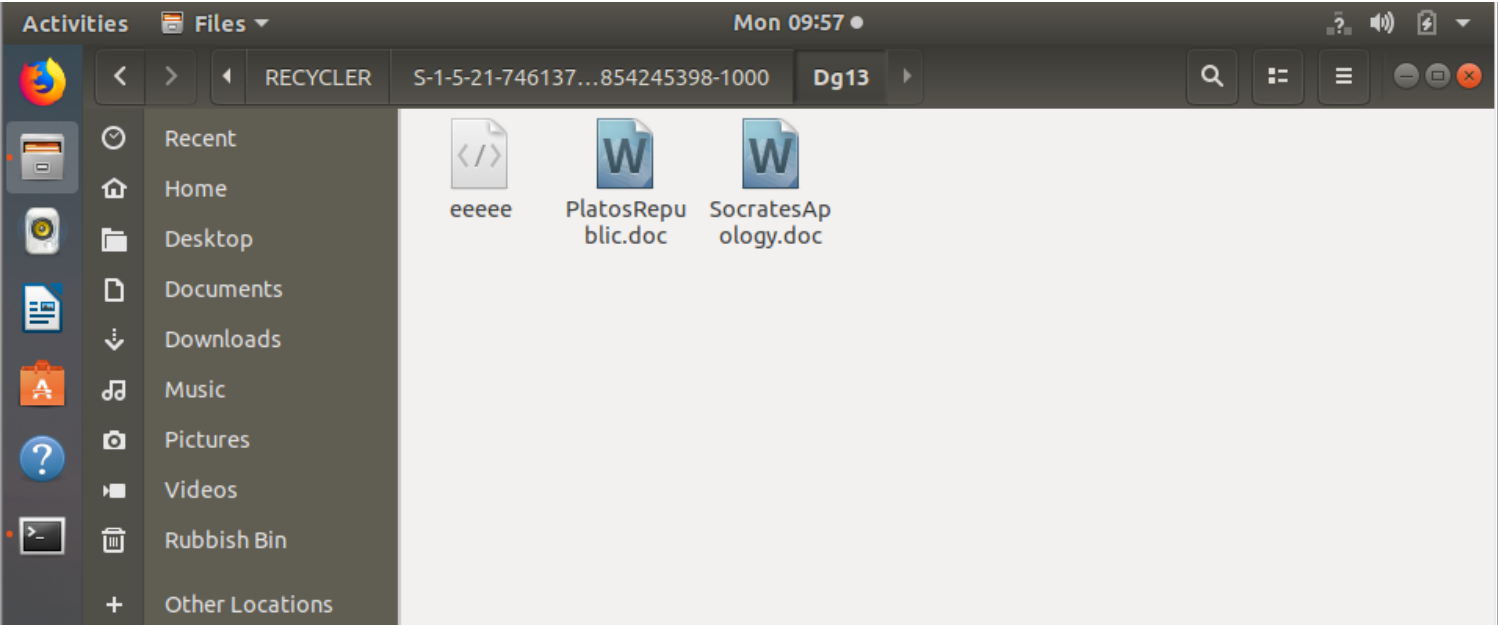


Pictures

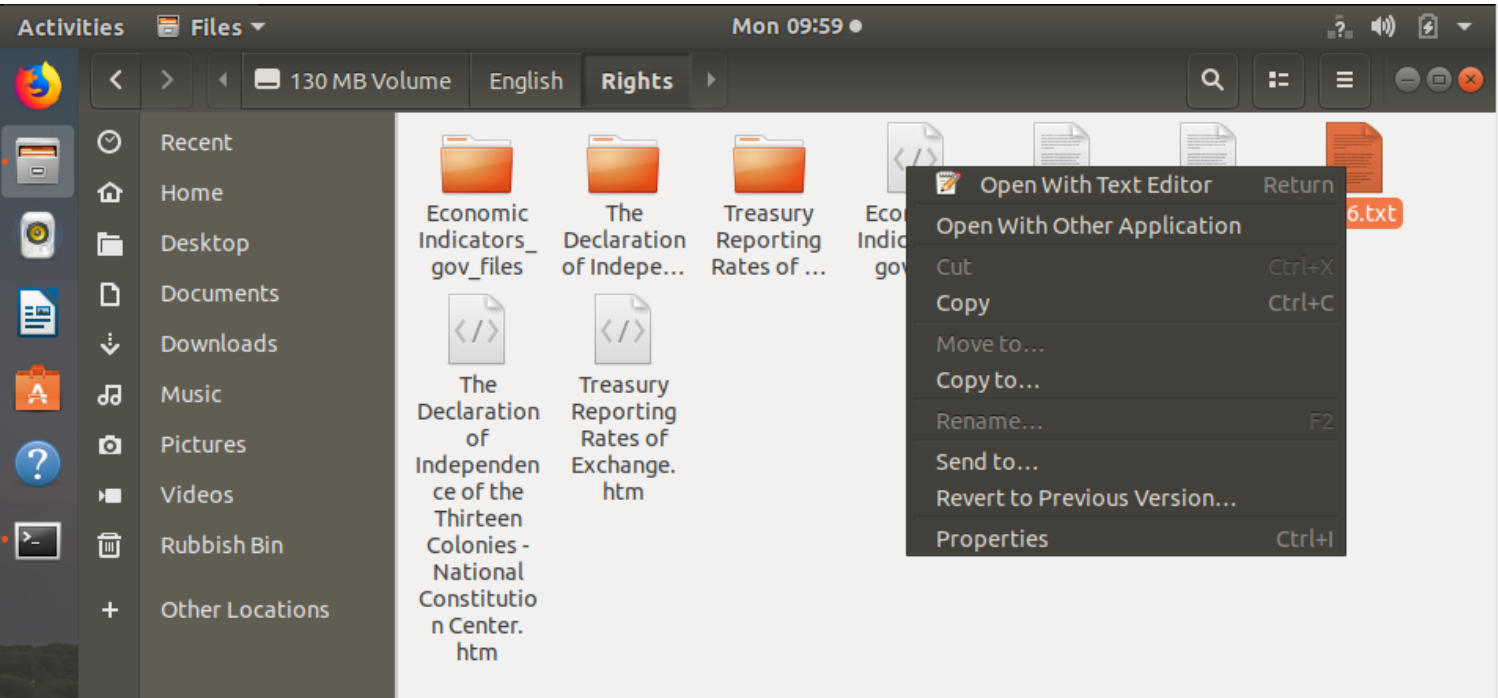




Recycler



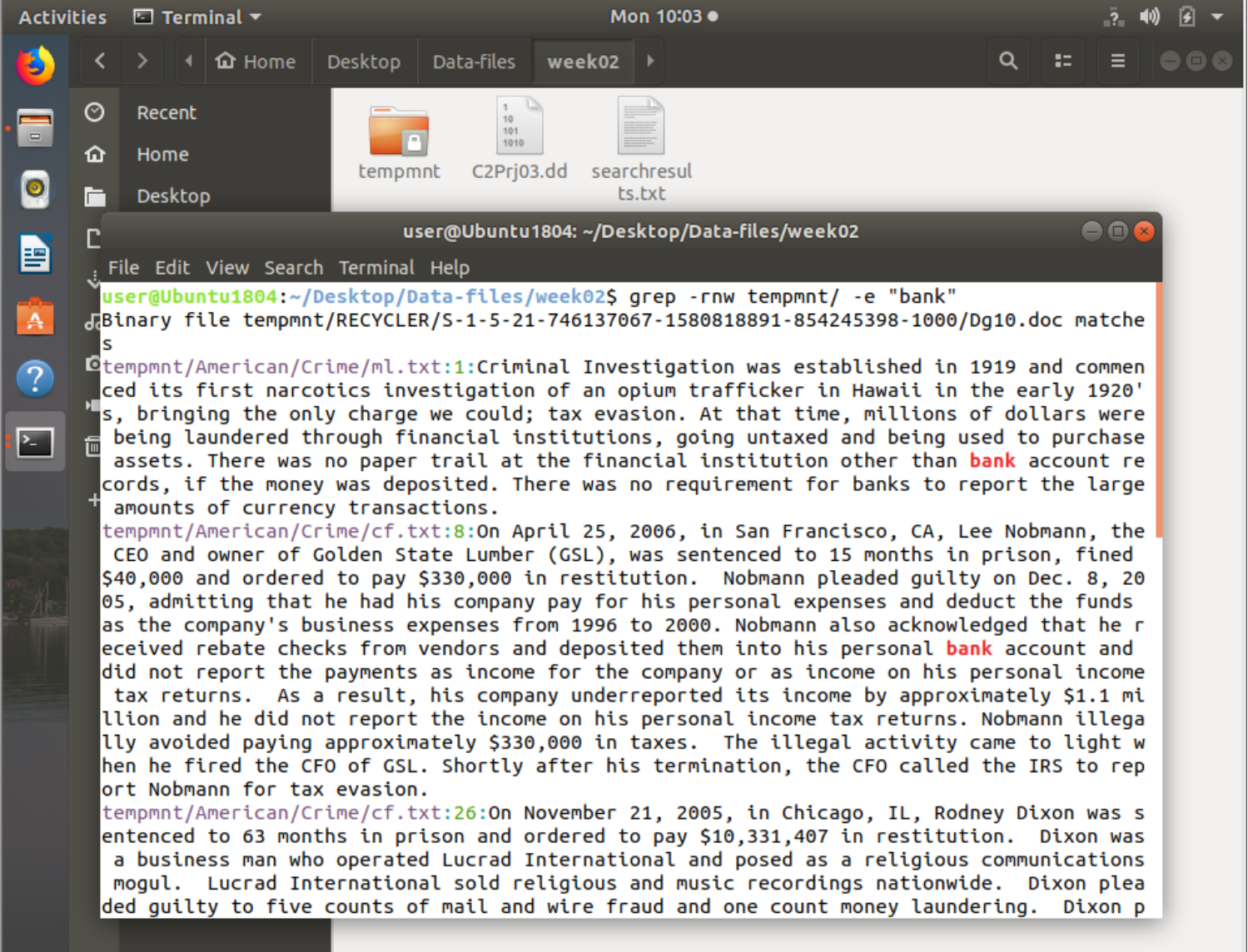
Then I tried to alter the files in the image, by trying to delete and create new folders. It didn't work because in the command I gave as read-only while mounting the image.





Search Contents with the tool grep

Here I started off with the command given in the assignment “`grep -rnw tempmnt -e “bank”`” to search for the keyword “bank” on the disk image mounted.

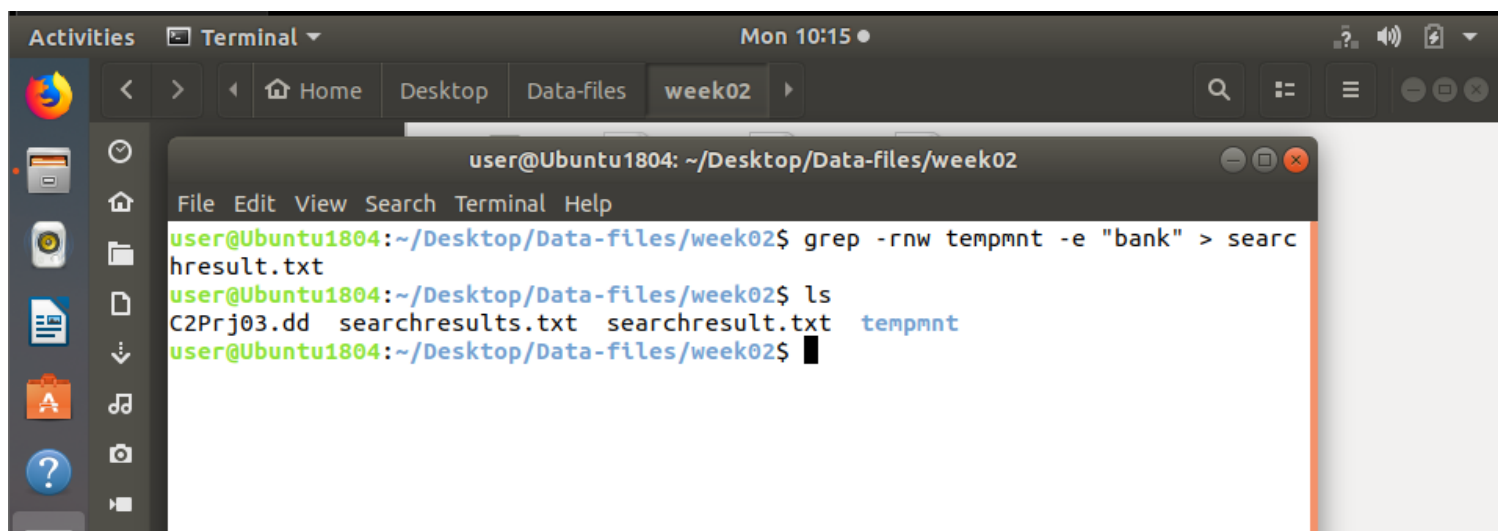


The screenshot shows a Linux desktop environment. A file manager window is open, displaying the contents of the `~/Desktop/Data-files/week02` directory. The files listed are `tempmnt`, `C2Prj03.dd`, and `searchresults.txt`. A terminal window is also open, showing the execution of the `grep` command to search for the keyword "bank" in the `tempmnt` directory. The terminal output shows matches in two files: `tempmnt/RECYCLER/S-1-5-21-746137067-1580818891-854245398-1000/Dg10.doc` and `tempmnt/American/Crime/ml.txt`. The first match is on line 1 of `ml.txt`, and the second is on line 8 of `cf.txt`. The terminal output is as follows:

```
user@Ubuntu1804: ~/Desktop/Data-files/week02
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/week02$ grep -rnw tempmnt/ -e "bank"
Binary file tempmnt/RECYCLER/S-1-5-21-746137067-1580818891-854245398-1000/Dg10.doc matches
tempmnt/American/Crime/ml.txt:1:Criminal Investigation was established in 1919 and commenced its first narcotics investigation of an opium trafficker in Hawaii in the early 1920's, bringing the only charge we could; tax evasion. At that time, millions of dollars were being laundered through financial institutions, going untaxed and being used to purchase assets. There was no paper trail at the financial institution other than bank account records, if the money was deposited. There was no requirement for banks to report the large amounts of currency transactions.
tempmnt/American/Crime/cf.txt:8:On April 25, 2006, in San Francisco, CA, Lee Nobmann, the CEO and owner of Golden State Lumber (GSL), was sentenced to 15 months in prison, fined $40,000 and ordered to pay $330,000 in restitution. Nobmann pleaded guilty on Dec. 8, 2005, admitting that he had his company pay for his personal expenses and deduct the funds as the company's business expenses from 1996 to 2000. Nobmann also acknowledged that he received rebate checks from vendors and deposited them into his personal bank account and did not report the payments as income for the company or as income on his personal income tax returns. As a result, his company underreported its income by approximately $1.1 million and he did not report the income on his personal income tax returns. Nobmann illegally avoided paying approximately $330,000 in taxes. The illegal activity came to light when he fired the CFO of GSL. Shortly after his termination, the CFO called the IRS to report Nobmann for tax evasion.
tempmnt/American/Crime/cf.txt:26:On November 21, 2005, in Chicago, IL, Rodney Dixon was sentenced to 63 months in prison and ordered to pay $10,331,407 in restitution. Dixon was a business man who operated Lucrad International and posed as a religious communications mogul. Lucrad International sold religious and music recordings nationwide. Dixon pleaded guilty to five counts of mail and wire fraud and one count money laundering. Dixon p
```

Then I tried some other commands from grep as well:

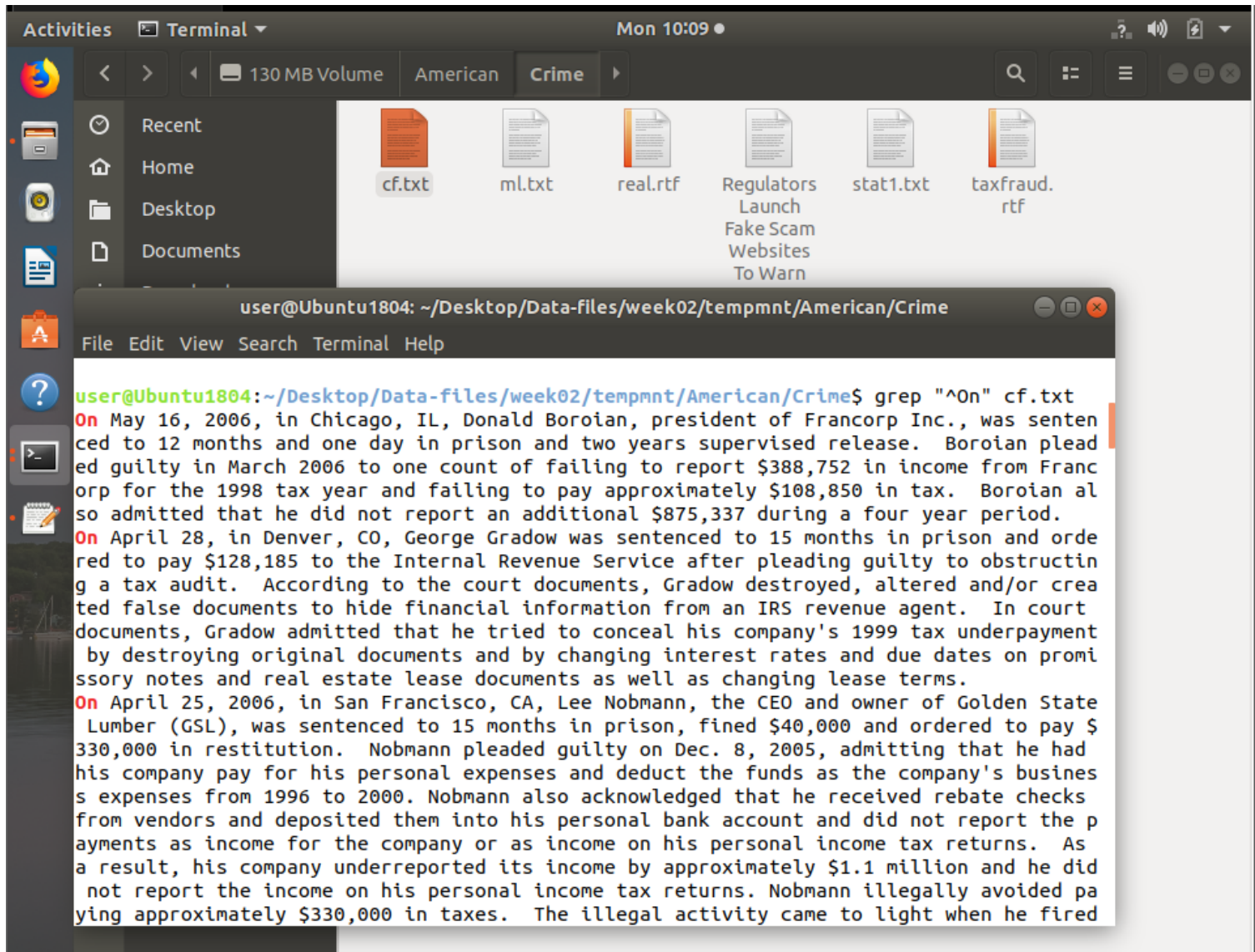
This will extract the output to another file and save it as a text file, in this case I have given the name searchresult.txt



The screenshot shows a terminal window titled "user@Ubuntu1804: ~/Desktop/Data-files/week02". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal shows the following commands and output:

```
user@Ubuntu1804:~/Desktop/Data-files/week02$ grep -rnw tempmnt -e "bank" > searchresult.txt
user@Ubuntu1804:~/Desktop/Data-files/week02$ ls
C2Prj03.dd  searchresults.txt  searchresult.txt  tempmnt
user@Ubuntu1804:~/Desktop/Data-files/week02$
```


Then this command will show the lines where the word "On" comes first in the text file called cf.txt

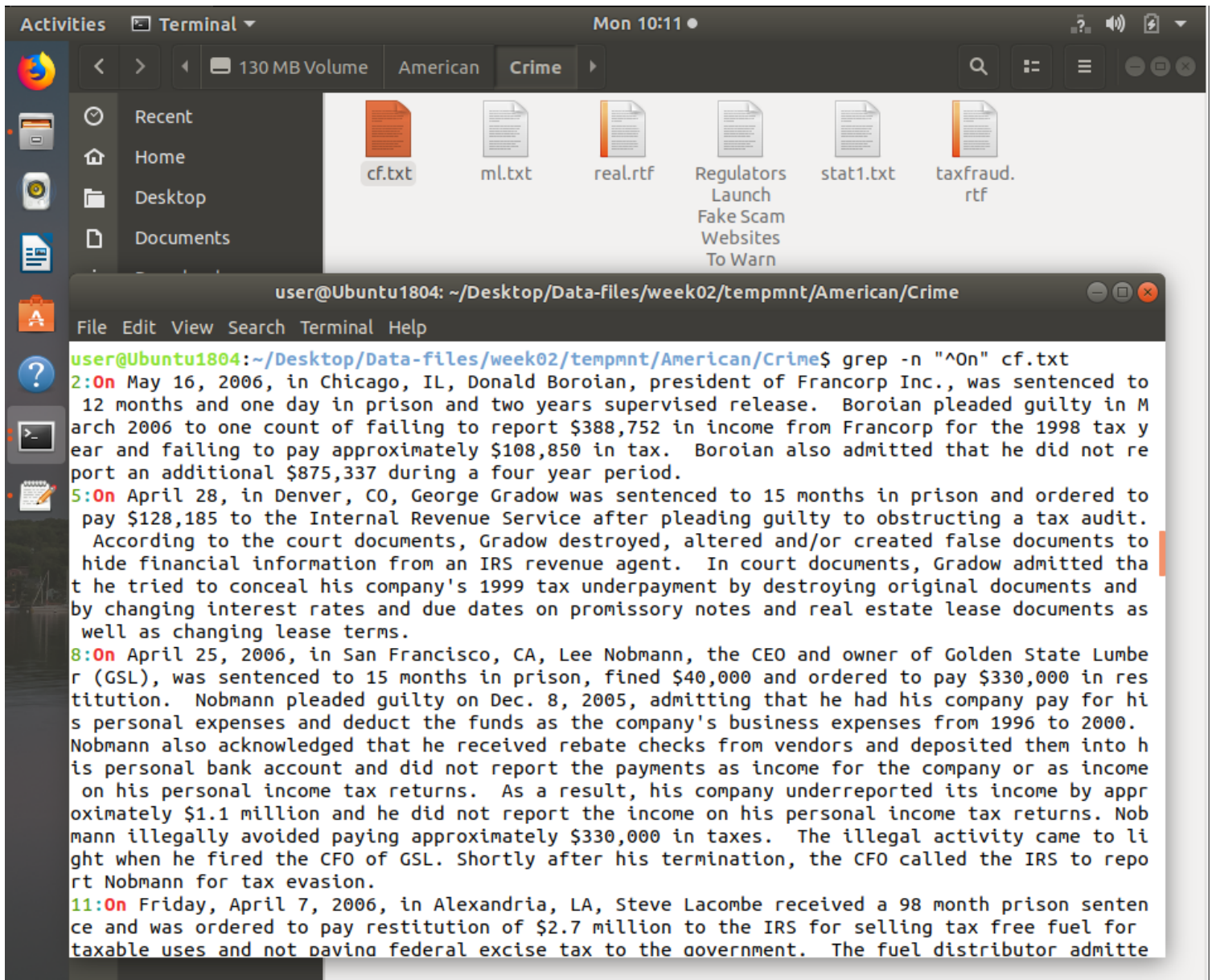


The screenshot shows a Linux desktop environment. In the background, a file manager window displays a directory named "Crime" containing several files: "cf.txt", "ml.txt", "real.rtf", "Regulators Launch Fake Scam Websites To Warn", "stat1.txt", and "taxfraud.rtf". In the foreground, a terminal window is open with the command `grep "^On" cf.txt` executed. The terminal output shows three lines of text, each starting with "On", followed by a detailed description of a criminal case.

```
user@Ubuntu1804: ~/Desktop/Data-files/week02/tempmnt/American/Crime
File Edit View Search Terminal Help

user@Ubuntu1804:~/Desktop/Data-files/week02/tempmnt/American/Crime$ grep "^On" cf.txt
On May 16, 2006, in Chicago, IL, Donald Boroian, president of Francorp Inc., was sentenced to 12 months and one day in prison and two years supervised release. Boroian pleaded guilty in March 2006 to one count of failing to report $388,752 in income from Francorp for the 1998 tax year and failing to pay approximately $108,850 in tax. Boroian also admitted that he did not report an additional $875,337 during a four year period.
On April 28, in Denver, CO, George Gradow was sentenced to 15 months in prison and ordered to pay $128,185 to the Internal Revenue Service after pleading guilty to obstructing a tax audit. According to the court documents, Gradow destroyed, altered and/or created false documents to hide financial information from an IRS revenue agent. In court documents, Gradow admitted that he tried to conceal his company's 1999 tax underpayment by destroying original documents and by changing interest rates and due dates on promissory notes and real estate lease documents as well as changing lease terms.
On April 25, 2006, in San Francisco, CA, Lee Nobmann, the CEO and owner of Golden State Lumber (GSL), was sentenced to 15 months in prison, fined $40,000 and ordered to pay $330,000 in restitution. Nobmann pleaded guilty on Dec. 8, 2005, admitting that he had his company pay for his personal expenses and deduct the funds as the company's business expenses from 1996 to 2000. Nobmann also acknowledged that he received rebate checks from vendors and deposited them into his personal bank account and did not report the payments as income for the company or as income on his personal income tax returns. As a result, his company underreported its income by approximately $1.1 million and he did not report the income on his personal income tax returns. Nobmann illegally avoided paying approximately $330,000 in taxes. The illegal activity came to light when he fired
```

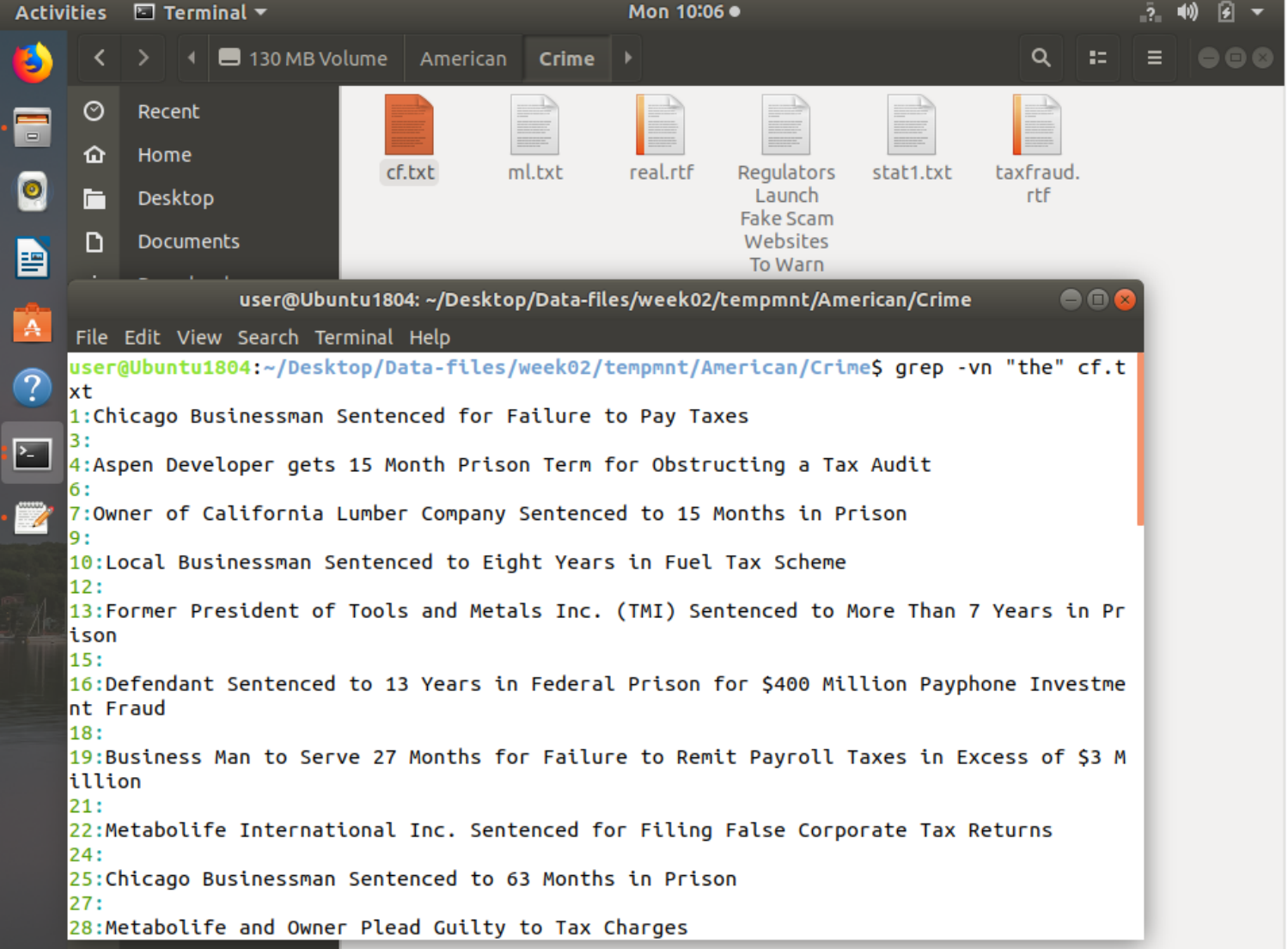
Then this command will show on which line does the word “On” comes first in the text file called cf.txt



The screenshot shows a Linux desktop environment. In the background, a file manager window is open, displaying a directory named "Crime" which contains several files: "cf.txt", "ml.txt", "real.rtf", "Regulators Launch Fake Scam Websites To Warn", "stat1.txt", and "taxfraud.rtf". In the foreground, a terminal window is open with the title "user@Ubuntu1804: ~/Desktop/Data-files/week02/tempmnt/American/Crime". The terminal shows the command `grep -n "^On" cf.txt` being executed, which returns the following results:

```
user@Ubuntu1804:~/Desktop/Data-files/week02/tempmnt/American/Crime$ grep -n "^On" cf.txt
2:On May 16, 2006, in Chicago, IL, Donald Boroian, president of Francorp Inc., was sentenced to
12 months and one day in prison and two years supervised release. Boroian pleaded guilty in M
arch 2006 to one count of failing to report $388,752 in income from Francorp for the 1998 tax y
ear and failing to pay approximately $108,850 in tax. Boroian also admitted that he did not re
port an additional $875,337 during a four year period.
5:On April 28, in Denver, CO, George Gradow was sentenced to 15 months in prison and ordered to
pay $128,185 to the Internal Revenue Service after pleading guilty to obstructing a tax audit.
According to the court documents, Gradow destroyed, altered and/or created false documents to
hide financial information from an IRS revenue agent. In court documents, Gradow admitted tha
t he tried to conceal his company's 1999 tax underpayment by destroying original documents and
by changing interest rates and due dates on promissory notes and real estate lease documents as
well as changing lease terms.
8:On April 25, 2006, in San Francisco, CA, Lee Nobmann, the CEO and owner of Golden State Lumbe
r (GSL), was sentenced to 15 months in prison, fined $40,000 and ordered to pay $330,000 in res
titution. Nobmann pleaded guilty on Dec. 8, 2005, admitting that he had his company pay for hi
s personal expenses and deduct the funds as the company's business expenses from 1996 to 2000.
Nobmann also acknowledged that he received rebate checks from vendors and deposited them into h
is personal bank account and did not report the payments as income for the company or as income
on his personal income tax returns. As a result, his company underreported its income by appr
oximately $1.1 million and he did not report the income on his personal income tax returns. Nob
mann illegally avoided paying approximately $330,000 in taxes. The illegal activity came to li
ght when he fired the CFO of GSL. Shortly after his termination, the CFO called the IRS to repo
rt Nobmann for tax evasion.
11:On Friday, April 7, 2006, in Alexandria, LA, Steve Lacombe received a 98 month prison senten
ce and was ordered to pay restitution of $2.7 million to the IRS for selling tax free fuel for
taxable uses and not paying federal excise tax to the government. The fuel distributor admitte
```

Then at last this command will remove the lines with the word “the” in the text file called cf.txt and still show the number of all the lines



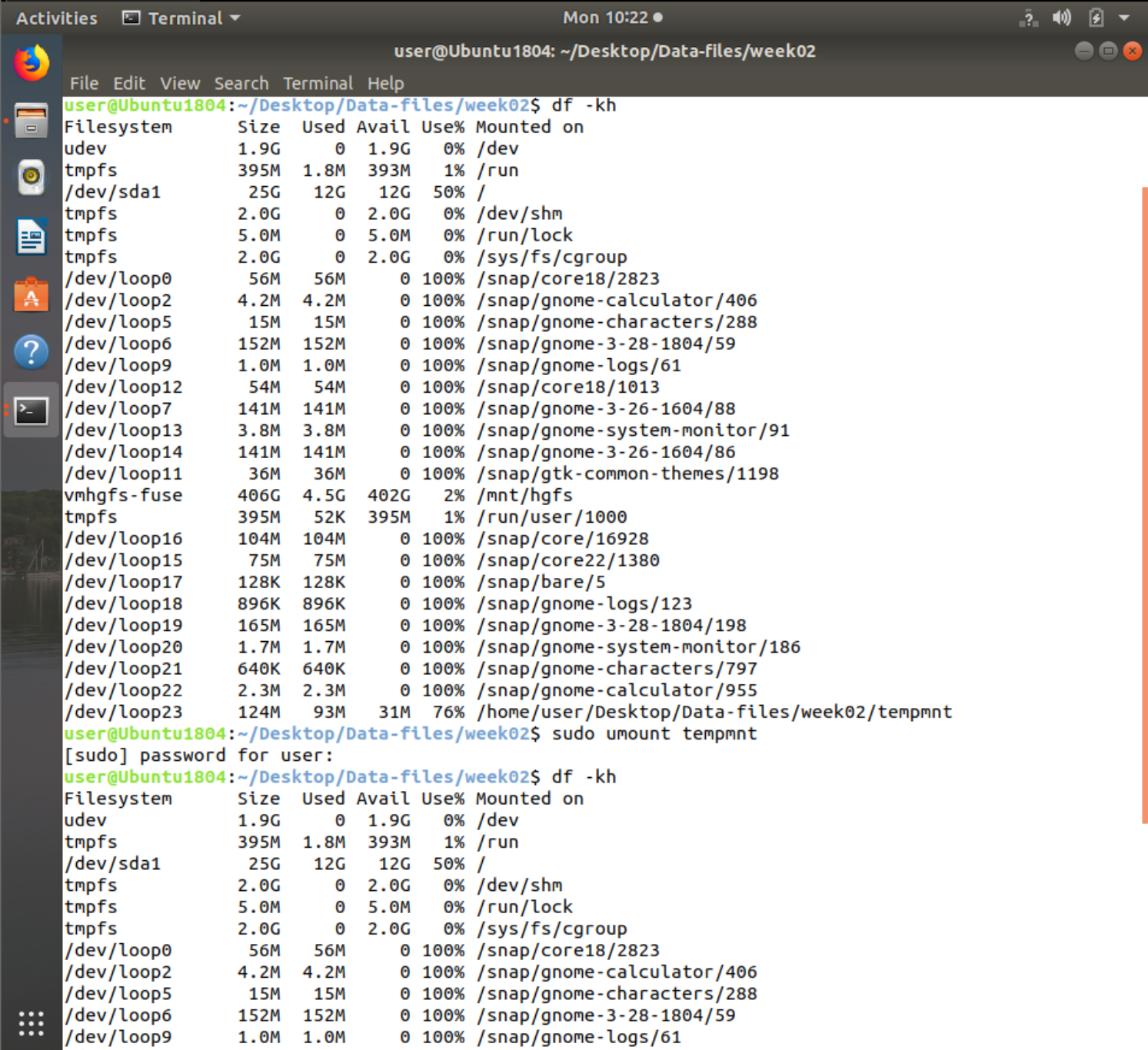
The screenshot shows a Linux desktop environment. In the background, a file manager window is open, displaying a directory named 'Crime' which contains several files: 'cf.txt', 'ml.txt', 'real.rtf', 'Regulators Launch Fake Scam Websites To Warn', 'stat1.txt', and 'taxfraud.rtf'. In the foreground, a terminal window is open with the command `grep -vn "the" cf.txt` executed. The terminal output shows the line numbers of the file 'cf.txt' that do not contain the word 'the'.

```
user@Ubuntu1804: ~/Desktop/Data-files/week02/tempmnt/American/Crime
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/week02/tempmnt/American/Crime$ grep -vn "the" cf.txt
1:Chicago Businessman Sentenced for Failure to Pay Taxes
3:
4:Aspen Developer gets 15 Month Prison Term for Obstructing a Tax Audit
6:
7:Owner of California Lumber Company Sentenced to 15 Months in Prison
9:
10:Local Businessman Sentenced to Eight Years in Fuel Tax Scheme
12:
13:Former President of Tools and Metals Inc. (TMI) Sentenced to More Than 7 Years in Prison
15:
16:Defendant Sentenced to 13 Years in Federal Prison for $400 Million Payphone Investment Fraud
18:
19:Business Man to Serve 27 Months for Failure to Remit Payroll Taxes in Excess of $3 Million
21:
22:Metabolife International Inc. Sentenced for Filing False Corporate Tax Returns
24:
25:Chicago Businessman Sentenced to 63 Months in Prison
27:
28:Metabolife and Owner Plead Guilty to Tax Charges
```

Introducing the tool umount

Now I will be unmounting the image since I'm done with the investigation. For that I will be using a tool called umount, using the command called **"sudo umount tempmnt"**.

First, I check for the available images using the command **df -kh**, the image was still mounted, then I typed the command mentioned above to unmount it. Finally, to check whether the unmount process is successful, I again used the **df -kh** to check for the available images. Since the image is not found, it means it has been unmounted successfully.



The screenshot shows a terminal window titled "user@Ubuntu1804: ~/Desktop/Data-files/week02". The terminal displays the output of the `df -kh` command twice. The first output shows that the file system `/home/user/Desktop/Data-files/week02/tempmnt` is mounted with 76% usage. The user then enters `sudo umount tempmnt`, and the terminal prompts for a password. After the password is entered, the user runs `df -kh` again, and the output shows that the file system is no longer listed, indicating it has been successfully unmounted.

```
user@Ubuntu1804: ~/Desktop/Data-files/week02
user@Ubuntu1804:~/Desktop/Data-files/week02$ df -kh
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0    1.9G   0% /dev
tmpfs           395M  1.8M  393M   1% /run
/dev/sda1       25G   12G   12G   50% /
tmpfs           2.0G   0    2.0G   0% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           2.0G   0    2.0G   0% /sys/fs/cgroup
/dev/loop0      56M   56M   0 100% /snap/core18/2823
/dev/loop2      4.2M  4.2M   0 100% /snap/gnome-calculator/406
/dev/loop5      15M   15M   0 100% /snap/gnome-characters/288
/dev/loop6     152M  152M   0 100% /snap/gnome-3-28-1804/59
/dev/loop9      1.0M  1.0M   0 100% /snap/gnome-logs/61
/dev/loop12     54M   54M   0 100% /snap/core18/1013
/dev/loop7     141M  141M   0 100% /snap/gnome-3-26-1604/88
/dev/loop13     3.8M  3.8M   0 100% /snap/gnome-system-monitor/91
/dev/loop14     141M  141M   0 100% /snap/gnome-3-26-1604/86
/dev/loop11     36M   36M   0 100% /snap/gtk-common-themes/1198
vmhgfs-fuse    406G  4.5G  402G   2% /mnt/hgfs
tmpfs           395M   52K  395M   1% /run/user/1000
/dev/loop16     104M  104M   0 100% /snap/core/16928
/dev/loop15     75M   75M   0 100% /snap/core22/1380
/dev/loop17     128K  128K   0 100% /snap/bare/5
/dev/loop18     896K  896K   0 100% /snap/gnome-logs/123
/dev/loop19     165M  165M   0 100% /snap/gnome-3-28-1804/198
/dev/loop20     1.7M  1.7M   0 100% /snap/gnome-system-monitor/186
/dev/loop21     640K  640K   0 100% /snap/gnome-characters/797
/dev/loop22     2.3M  2.3M   0 100% /snap/gnome-calculator/955
/dev/loop23     124M   93M   31M  76% /home/user/Desktop/Data-files/week02/tempmnt
user@Ubuntu1804:~/Desktop/Data-files/week02$ sudo umount tempmnt
[sudo] password for user:
user@Ubuntu1804:~/Desktop/Data-files/week02$ df -kh
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0    1.9G   0% /dev
tmpfs           395M  1.8M  393M   1% /run
/dev/sda1       25G   12G   12G   50% /
tmpfs           2.0G   0    2.0G   0% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           2.0G   0    2.0G   0% /sys/fs/cgroup
/dev/loop0      56M   56M   0 100% /snap/core18/2823
/dev/loop2      4.2M  4.2M   0 100% /snap/gnome-calculator/406
/dev/loop5      15M   15M   0 100% /snap/gnome-characters/288
/dev/loop6     152M  152M   0 100% /snap/gnome-3-28-1804/59
/dev/loop9      1.0M  1.0M   0 100% /snap/gnome-logs/61
```


File Edit View Search Terminal Help

```
/dev/loop14    141M   141M    0 100% /snap/gnome-3-26-1604/86
/dev/loop11     36M    36M    0 100% /snap/gtk-common-themes/1198
vmhgfs-fuse    406G   4.5G   402G   2% /mnt/hgfs
tmpfs          395M    52K   395M    1% /run/user/1000
/dev/loop16    104M   104M    0 100% /snap/core/16928
/dev/loop15     75M    75M    0 100% /snap/core22/1380
/dev/loop17    128K   128K    0 100% /snap/bare/5
/dev/loop18    896K   896K    0 100% /snap/gnome-logs/123
/dev/loop19    165M   165M    0 100% /snap/gnome-3-28-1804/198
/dev/loop20     1.7M   1.7M    0 100% /snap/gnome-system-monitor/186
/dev/loop21    640K   640K    0 100% /snap/gnome-characters/797
/dev/loop22     2.3M   2.3M    0 100% /snap/gnome-calculator/955
/dev/loop23    124M    93M    31M   76% /home/user/Desktop/Data-files/week02/tempmnt
```

```
user@Ubuntu1804:~/Desktop/Data-files/week02$ sudo umount tempmnt
```

```
[sudo] password for user:
```

```
user@Ubuntu1804:~/Desktop/Data-files/week02$ df -kh
```

Filesystem	Size	Used	Avail	Use%	Mounted on
udev	1.9G	0	1.9G	0%	/dev
tmpfs	395M	1.8M	393M	1%	/run
/dev/sda1	25G	12G	12G	50%	/
tmpfs	2.0G	0	2.0G	0%	/dev/shm
tmpfs	5.0M	0	5.0M	0%	/run/lock
tmpfs	2.0G	0	2.0G	0%	/sys/fs/cgroup
/dev/loop0	56M	56M	0	100%	/snap/core18/2823
/dev/loop2	4.2M	4.2M	0	100%	/snap/gnome-calculator/406
/dev/loop5	15M	15M	0	100%	/snap/gnome-characters/288
/dev/loop6	152M	152M	0	100%	/snap/gnome-3-28-1804/59
/dev/loop9	1.0M	1.0M	0	100%	/snap/gnome-logs/61
/dev/loop12	54M	54M	0	100%	/snap/core18/1013
/dev/loop7	141M	141M	0	100%	/snap/gnome-3-26-1604/88
/dev/loop13	3.8M	3.8M	0	100%	/snap/gnome-system-monitor/91
/dev/loop14	141M	141M	0	100%	/snap/gnome-3-26-1604/86
/dev/loop11	36M	36M	0	100%	/snap/gtk-common-themes/1198
vmhgfs-fuse	406G	4.5G	402G	2%	/mnt/hgfs
tmpfs	395M	44K	395M	1%	/run/user/1000
/dev/loop16	104M	104M	0	100%	/snap/core/16928
/dev/loop15	75M	75M	0	100%	/snap/core22/1380
/dev/loop17	128K	128K	0	100%	/snap/bare/5
/dev/loop18	896K	896K	0	100%	/snap/gnome-logs/123
/dev/loop19	165M	165M	0	100%	/snap/gnome-3-28-1804/198
/dev/loop20	1.7M	1.7M	0	100%	/snap/gnome-system-monitor/186
/dev/loop21	640K	640K	0	100%	/snap/gnome-characters/797
/dev/loop22	2.3M	2.3M	0	100%	/snap/gnome-calculator/955

```
user@Ubuntu1804:~/Desktop/Data-files/week02$
```