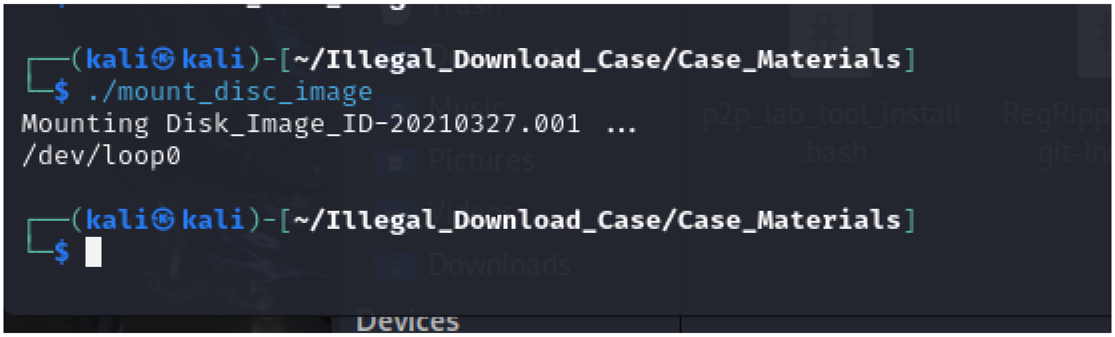
Daniella Boulos, Julianna Russo, Tyler Kaminer

NIST Case: Registry and File Directory

Sept 26, 2024

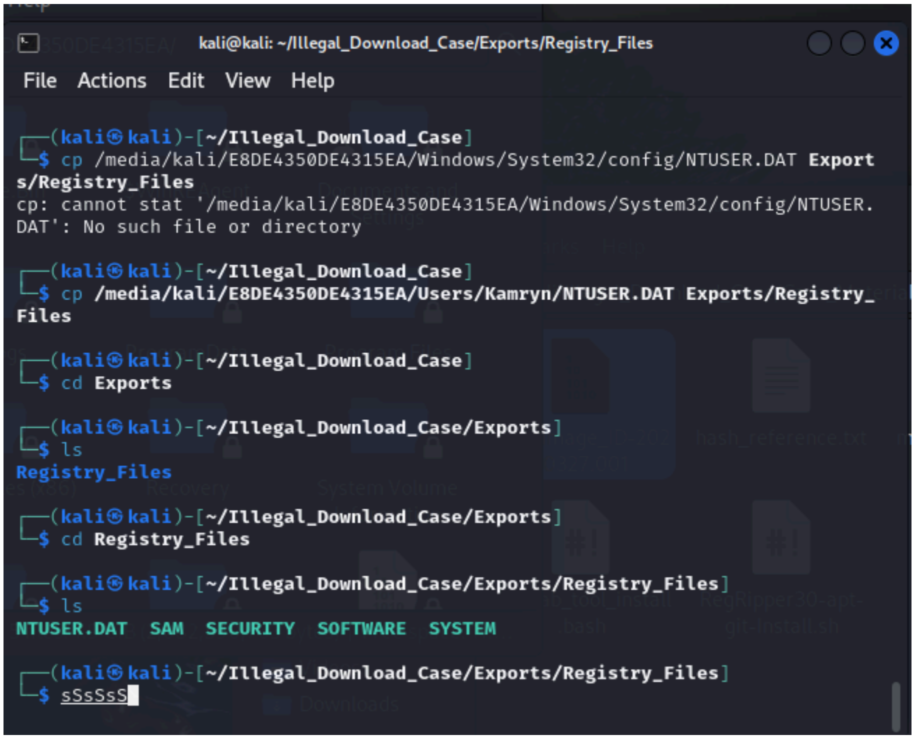
Computer Forensics

Mounting Disk Image:



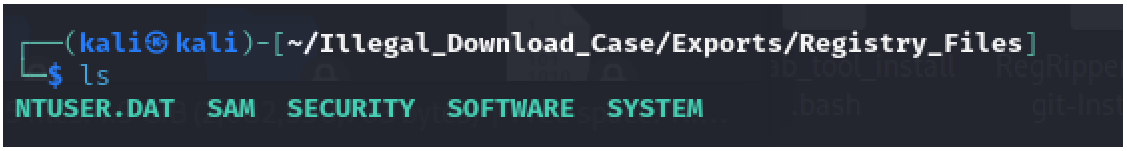
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Case_Materials]
└─$ ./mount_disc_image
Mounting Disk_Image_ID-20210327.001 ...
/dev/loop0

┌──(kali㉿kali)-[~/Illegal_Download_Case/Case_Materials]
└─$ 
```

Copy Registry Files:



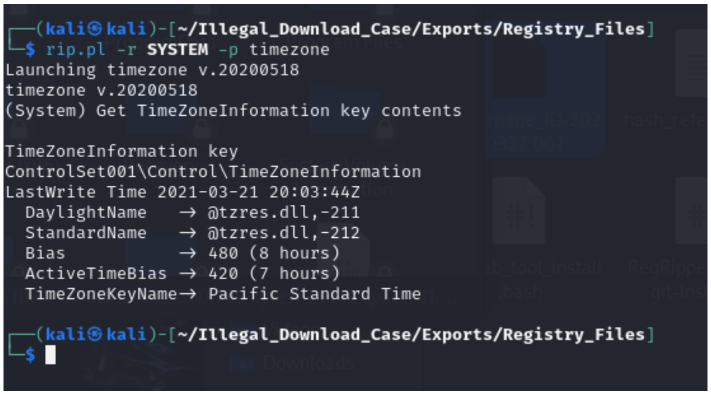
kali@kali: ~/Illegal_Download_Case/Exports/Registry_Files
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Illegal_Download_Case]
└─$ cp /media/kali/E8DE4350DE4315EA/Windows/System32/config/NTUSER.DAT Export
s/Registry_Files
cp: cannot stat '/media/kali/E8DE4350DE4315EA/Windows/System32/config/NTUSER.
DAT': No such file or directory

┌──(kali㉿kali)-[~/Illegal_Download_Case]
└─$ cp /media/kali/E8DE4350DE4315EA/Users/Kamryn/NTUSER.DAT Exports/Registry_
Files

┌──(kali㉿kali)-[~/Illegal_Download_Case]
└─$ cd Exports

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports]
└─$ ls
Registry_Files

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports]
└─$ cd Registry_Files

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ ls
NTUSER.DAT  SAM  SECURITY  SOFTWARE  SYSTEM

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ sSsSsS
```



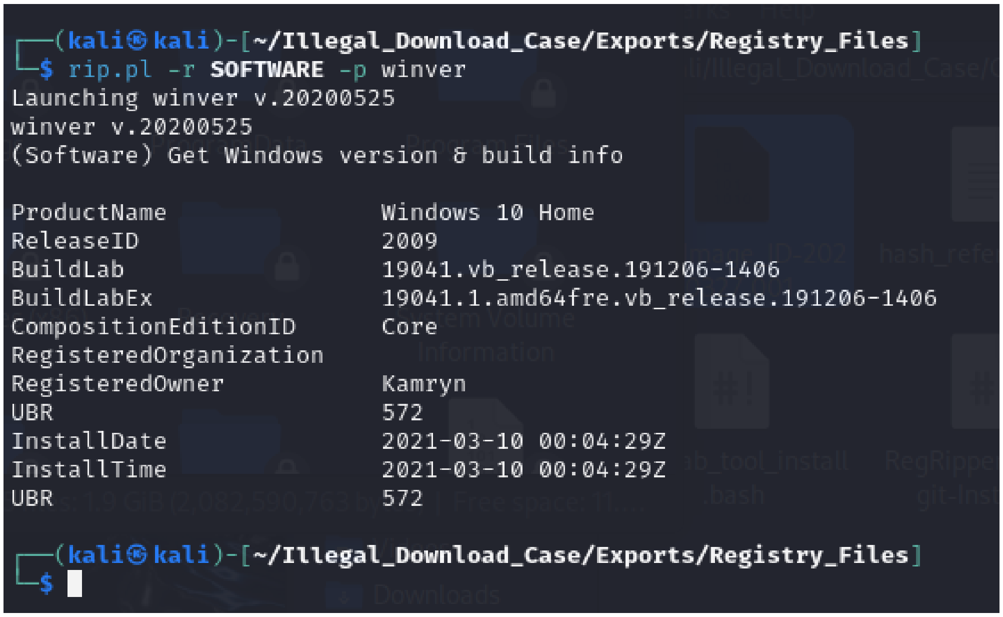
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ ls
NTUSER.DAT  SAM  SECURITY  SOFTWARE  SYSTEM
```

Regripper to check timezone:



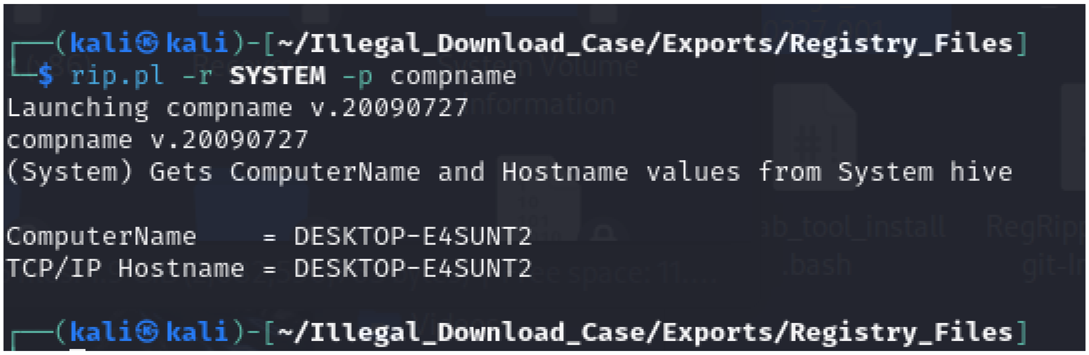
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ rip.pl -r SYSTEM -p timezone
Launching timezone v.20200518
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2021-03-21 20:03:44Z
  DaylightName   → @tzres.dll,-211
  StandardName   → @tzres.dll,-212
  Bias           → 480 (8 hours)
  ActiveTimeBias → 420 (7 hours)
  TimeZoneKeyName→ Pacific Standard Time

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ 
```

Regripper to check OS:



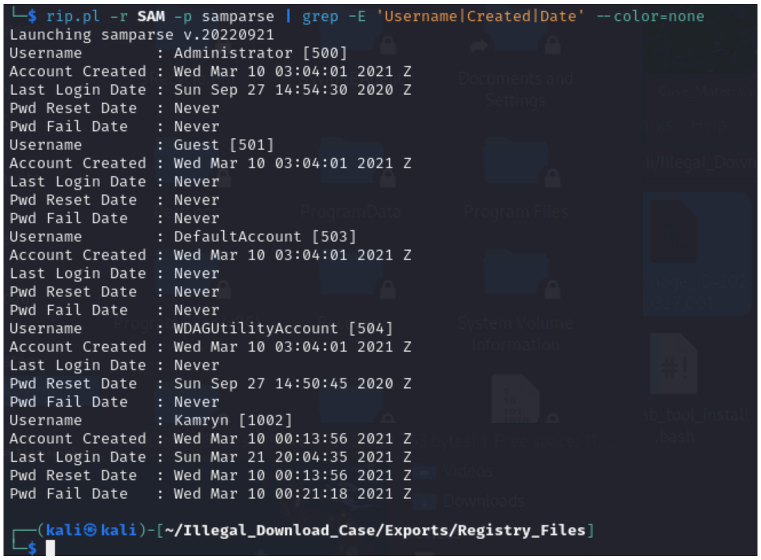
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ rip.pl -r SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName                Windows 10 Home
ReleaseID                  2009
BuildLab                   19041.vb_release.191206-1406
BuildLabEx                 19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID       Core
RegisteredOrganization
RegisteredOwner            Kamryn
UBR                        572
InstallDate                2021-03-10 00:04:29Z
InstallTime                2021-03-10 00:04:29Z
UBR                        572

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ 
```

Regripper to check system name:



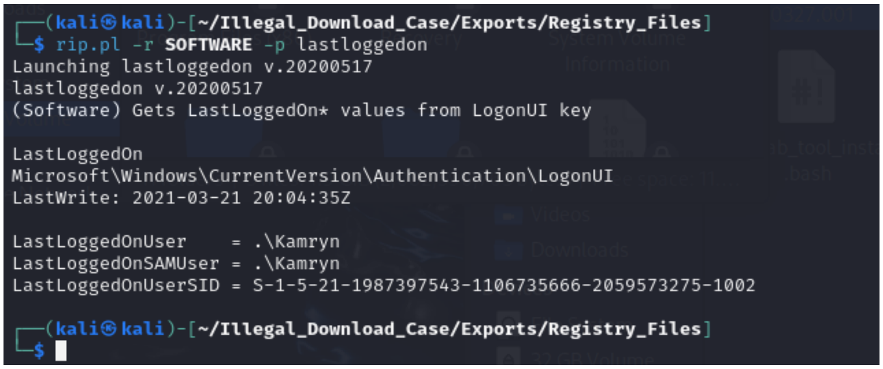
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ rip.pl -r SYSTEM -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName     = DESKTOP-E4SUNT2
TCP/IP Hostname = DESKTOP-E4SUNT2

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
```

Regripper to check user accounts:



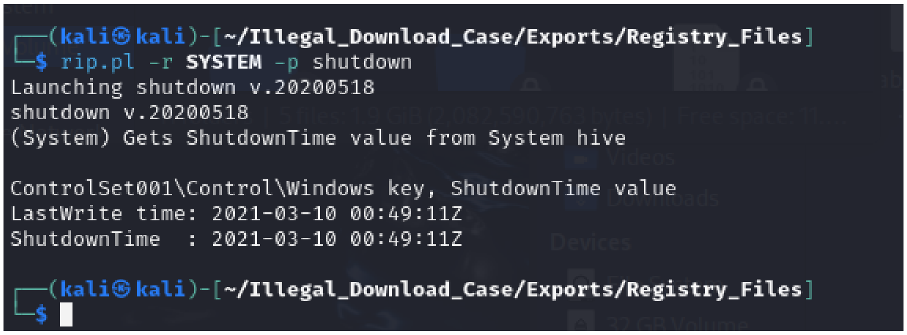
```
└─$ rip.pl -r SAM -p samparse | grep -E 'Username|Created|Date' --color=none
Launching samparse v.20220921
Username        : Administrator [500]
Account Created : Wed Mar 10 03:04:01 2021 Z
Last Login Date : Sun Sep 27 14:54:30 2020 Z
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Username        : Guest [501]
Account Created : Wed Mar 10 03:04:01 2021 Z
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Username        : DefaultAccount [503]
Account Created : Wed Mar 10 03:04:01 2021 Z
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Username        : WDAGUtilityAccount [504]
Account Created : Wed Mar 10 03:04:01 2021 Z
Last Login Date : Never
Pwd Reset Date  : Sun Sep 27 14:50:45 2020 Z
Pwd Fail Date   : Never
Username        : Kamryn [1002]
Account Created : Wed Mar 10 00:13:56 2021 Z
Last Login Date : Sun Mar 21 20:04:35 2021 Z
Pwd Reset Date  : Wed Mar 10 00:13:56 2021 Z
Pwd Fail Date   : Wed Mar 10 00:21:18 2021 Z

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ 
```

Regripper to check the last login:



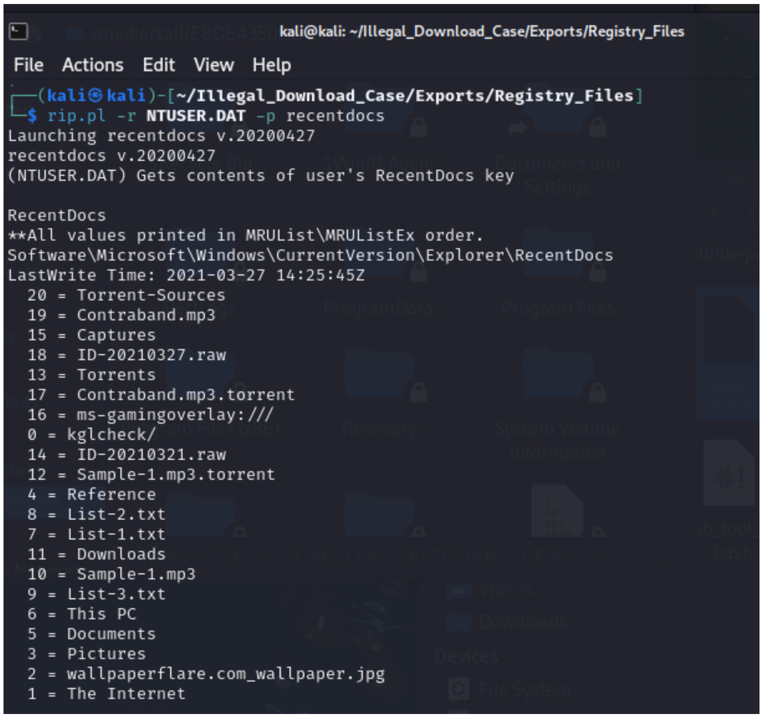
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ rip.pl -r SOFTWARE -p lastloggedon
Launching lastloggedon v.20200517
lastloggedon v.20200517
(Software) Gets LastLoggedOn* values from LogonUI key

LastLoggedOn
Microsoft\Windows\CurrentVersion\Authentication\LogonUI
LastWrite: 2021-03-21 20:04:35Z

LastLoggedOnUser     = .\Kamryn
LastLoggedOnSAMUser = .\Kamryn
LastLoggedOnUserSID = S-1-5-21-1987397543-1106735666-2059573275-1002

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ 
```

Regripper to check the most recent shutdown:



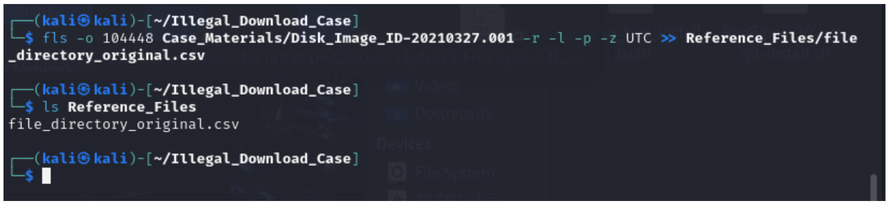
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ rip.pl -r SYSTEM -p shutdown
Launching shutdown v.20200518
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2021-03-10 00:49:11Z
ShutdownTime  : 2021-03-10 00:49:11Z

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ 
```

Regripper to check what user has recently opened:



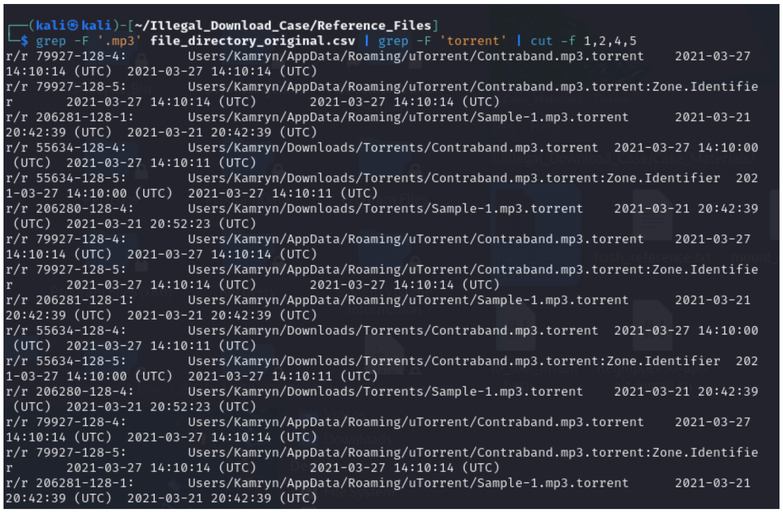
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/Registry_Files]
└─$ rip.pl -r NTUSER.DAT -p recentdocs
Launching recentdocs v.20200427
recentdocs v.20200427
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time: 2021-03-27 14:25:45Z
  20 = Torrent-Sources
  19 = Contraband.mp3
  15 = Captures
  18 = ID-20210327.raw
  13 = Torrents
  17 = Contraband.mp3.torrent
  16 = ms-gamingoverlay:///
  0 = kglcheck/
  14 = ID-20210321.raw
  12 = Sample-1.mp3.torrent
  4 = Reference
  8 = List-2.txt
  7 = List-1.txt
  11 = Downloads
  10 = Sample-1.mp3
  9 = List-3.txt
  6 = This PC
  5 = Documents
  3 = Pictures
  2 = wallpaperflare.com_wallpaper.jpg
  1 = The Internet
```

fls to generate directory listing:



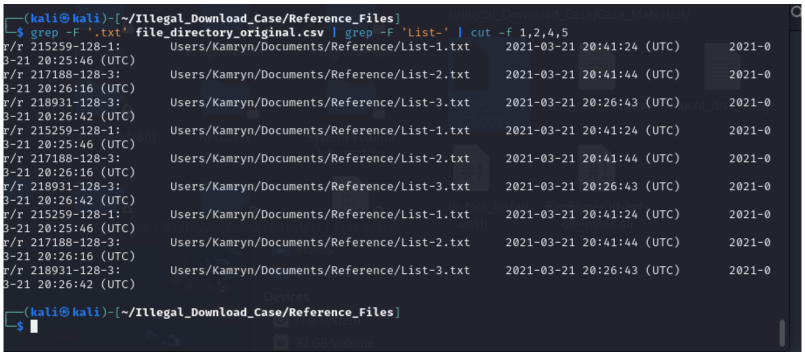
```
┌──(kali㉿kali)-[~/Illegal_Download_Case]
└─$ fls -o 104448 Case_Materials/Disk_Image_ID-20210327.001 -r -l -p -z UTC >> Reference_Files/file
_directory_original.csv

┌──(kali㉿kali)-[~/Illegal_Download_Case]
└─$ ls Reference_Files
file_directory_original.csv

┌──(kali㉿kali)-[~/Illegal_Download_Case]
└─$ 
```

grep to search for torrent files:



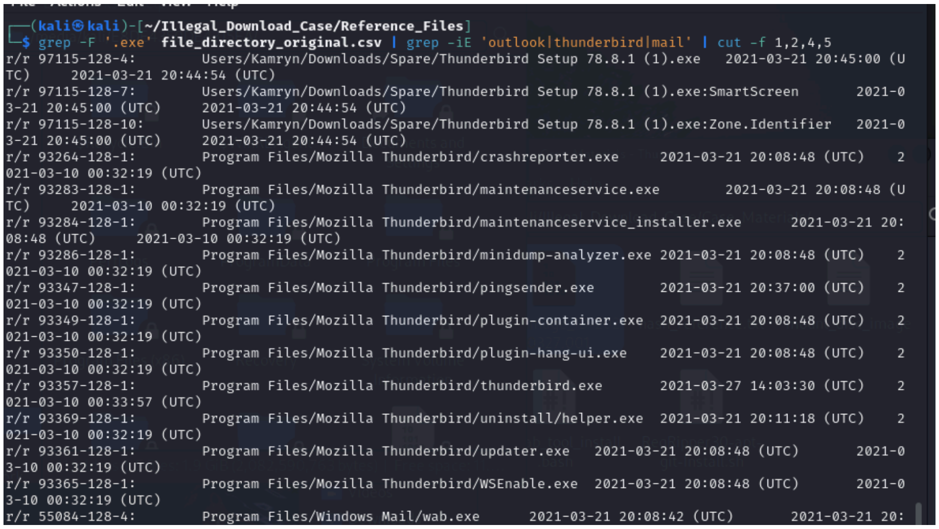
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ grep -F '.mp3' file_directory_original.csv | grep -F 'torrent' | cut -f 1,2,4,5
r/r 79927-128-4:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent    2021-03-27
14:10:14 (UTC)  2021-03-27 14:10:14 (UTC)
r/r 79927-128-5:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent:Zone.Identifie
r       2021-03-27 14:10:14 (UTC)       2021-03-27 14:10:14 (UTC)
r/r 206281-128-1:       Users/Kamryn/AppData/Roaming/uTorrent/Sample-1.mp3.torrent      2021-03-21
20:42:39 (UTC)  2021-03-21 20:42:39 (UTC)
r/r 55634-128-4:        Users/Kamryn/Downloads/Torrents/Contraband.mp3.torrent  2021-03-27 14:10:00
 (UTC)  2021-03-27 14:10:11 (UTC)
r/r 55634-128-5:        Users/Kamryn/Downloads/Torrents/Contraband.mp3.torrent:Zone.Identifier  202
1-03-27 14:10:00 (UTC)  2021-03-27 14:10:11 (UTC)
r/r 206280-128-4:       Users/Kamryn/Downloads/Torrents/Sample-1.mp3.torrent    2021-03-21 20:42:39
 (UTC)  2021-03-21 20:52:23 (UTC)
r/r 79927-128-4:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent    2021-03-27
14:10:14 (UTC)  2021-03-27 14:10:14 (UTC)
r/r 79927-128-5:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent:Zone.Identifie
r       2021-03-27 14:10:14 (UTC)       2021-03-27 14:10:14 (UTC)
r/r 206281-128-1:       Users/Kamryn/AppData/Roaming/uTorrent/Sample-1.mp3.torrent      2021-03-21
20:42:39 (UTC)  2021-03-21 20:42:39 (UTC)
r/r 55634-128-4:        Users/Kamryn/Downloads/Torrents/Contraband.mp3.torrent  2021-03-27 14:10:00
 (UTC)  2021-03-27 14:10:11 (UTC)
r/r 55634-128-5:        Users/Kamryn/Downloads/Torrents/Contraband.mp3.torrent:Zone.Identifier  202
1-03-27 14:10:00 (UTC)  2021-03-27 14:10:11 (UTC)
r/r 206280-128-4:       Users/Kamryn/Downloads/Torrents/Sample-1.mp3.torrent    2021-03-21 20:42:39
 (UTC)  2021-03-21 20:52:23 (UTC)
r/r 79927-128-4:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent    2021-03-27
14:10:14 (UTC)  2021-03-27 14:10:14 (UTC)
r/r 79927-128-5:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent:Zone.Identifie
r       2021-03-27 14:10:14 (UTC)       2021-03-27 14:10:14 (UTC)
r/r 206281-128-1:       Users/Kamryn/AppData/Roaming/uTorrent/Sample-1.mp3.torrent      2021-03-21
20:42:39 (UTC)  2021-03-21 20:42:39 (UTC)
```

grep to search for text files:



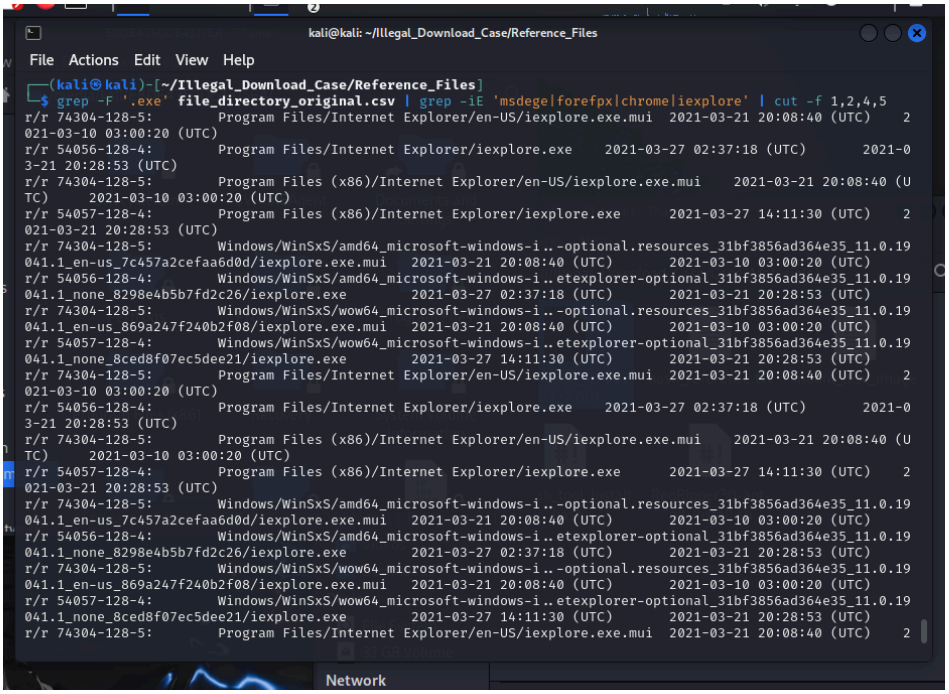
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ grep -F '.txt' file_directory_original.csv | grep -F 'List-' | cut -f 1,2,4,5
r/r 215259-128-1:       Users/Kamryn/Documents/Reference/List-1.txt     2021-03-21 20:41:24 (UTC)       2021-0
3-21 20:25:46 (UTC)
r/r 217188-128-3:       Users/Kamryn/Documents/Reference/List-2.txt     2021-03-21 20:41:44 (UTC)       2021-0
3-21 20:26:16 (UTC)
r/r 218931-128-3:       Users/Kamryn/Documents/Reference/List-3.txt     2021-03-21 20:26:43 (UTC)       2021-0
3-21 20:26:42 (UTC)
r/r 215259-128-1:       Users/Kamryn/Documents/Reference/List-1.txt     2021-03-21 20:41:24 (UTC)       2021-0
3-21 20:25:46 (UTC)
r/r 217188-128-3:       Users/Kamryn/Documents/Reference/List-2.txt     2021-03-21 20:41:44 (UTC)       2021-0
3-21 20:26:16 (UTC)
r/r 218931-128-3:       Users/Kamryn/Documents/Reference/List-3.txt     2021-03-21 20:26:43 (UTC)       2021-0
3-21 20:26:42 (UTC)
r/r 215259-128-1:       Users/Kamryn/Documents/Reference/List-1.txt     2021-03-21 20:41:24 (UTC)       2021-0
3-21 20:25:46 (UTC)
r/r 217188-128-3:       Users/Kamryn/Documents/Reference/List-2.txt     2021-03-21 20:41:44 (UTC)       2021-0
3-21 20:26:16 (UTC)
r/r 218931-128-3:       Users/Kamryn/Documents/Reference/List-3.txt     2021-03-21 20:26:43 (UTC)       2021-0
3-21 20:26:42 (UTC)

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ █
```

grep to search for email client:



```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ grep -F '.exe' file_directory_original.csv | grep -iE 'outlook|thunderbird|mail' | cut -f 1,2,4,5
r/r 97115-128-4:        Users/Kamryn/Downloads/Spare/Thunderbird Setup 78.8.1 (1).exe   2021-03-21 20:45:00 (U
TC)     2021-03-21 20:44:54 (UTC)
r/r 97115-128-7:        Users/Kamryn/Downloads/Spare/Thunderbird Setup 78.8.1 (1).exe:SmartScreen       2021-0
3-21 20:45:00 (UTC)     2021-03-21 20:44:54 (UTC)
r/r 97115-128-10:       Users/Kamryn/Downloads/Spare/Thunderbird Setup 78.8.1 (1).exe:Zone.Identifier   2021-0
3-21 20:45:00 (UTC)     2021-03-21 20:44:54 (UTC)
r/r 93264-128-1:        Program Files/Mozilla Thunderbird/crashreporter.exe     2021-03-21 20:08:48 (UTC)    2
021-03-10 00:32:19 (UTC)
r/r 93283-128-1:        Program Files/Mozilla Thunderbird/maintenanceservice.exe        2021-03-21 20:08:48 (U
TC)     2021-03-10 00:32:19 (UTC)
r/r 93284-128-1:        Program Files/Mozilla Thunderbird/maintenanceservice_installer.exe      2021-03-21 20:
08:48 (UTC)     2021-03-10 00:32:19 (UTC)
r/r 93286-128-1:        Program Files/Mozilla Thunderbird/minidump-analyzer.exe 2021-03-21 20:08:48 (UTC)    2
021-03-10 00:32:19 (UTC)
r/r 93347-128-1:        Program Files/Mozilla Thunderbird/pingsender.exe        2021-03-21 20:37:00 (UTC)    2
021-03-10 00:32:19 (UTC)
r/r 93349-128-1:        Program Files/Mozilla Thunderbird/plugin-container.exe  2021-03-21 20:08:48 (UTC)    2
021-03-10 00:32:19 (UTC)
r/r 93350-128-1:        Program Files/Mozilla Thunderbird/plugin-hang-ui.exe    2021-03-21 20:08:48 (UTC)    2
021-03-10 00:32:19 (UTC)
r/r 93357-128-1:        Program Files/Mozilla Thunderbird/thunderbird.exe       2021-03-27 14:03:30 (UTC)    2
021-03-10 00:33:57 (UTC)
r/r 93369-128-1:        Program Files/Mozilla Thunderbird/uninstall/helper.exe  2021-03-21 20:11:18 (UTC)    2
021-03-10 00:32:19 (UTC)
r/r 93361-128-1:        Program Files/Mozilla Thunderbird/updater.exe   2021-03-21 20:08:48 (UTC)       2021-0
3-10 00:32:19 (UTC)
r/r 93365-128-1:        Program Files/Mozilla Thunderbird/WSEnable.exe  2021-03-21 20:08:48 (UTC)       2021-0
3-10 00:32:19 (UTC)
r/r 55084-128-4:        Program Files/Windows Mail/wab.exe      2021-03-21 20:08:42 (UTC)       2021-03-21 20:
```

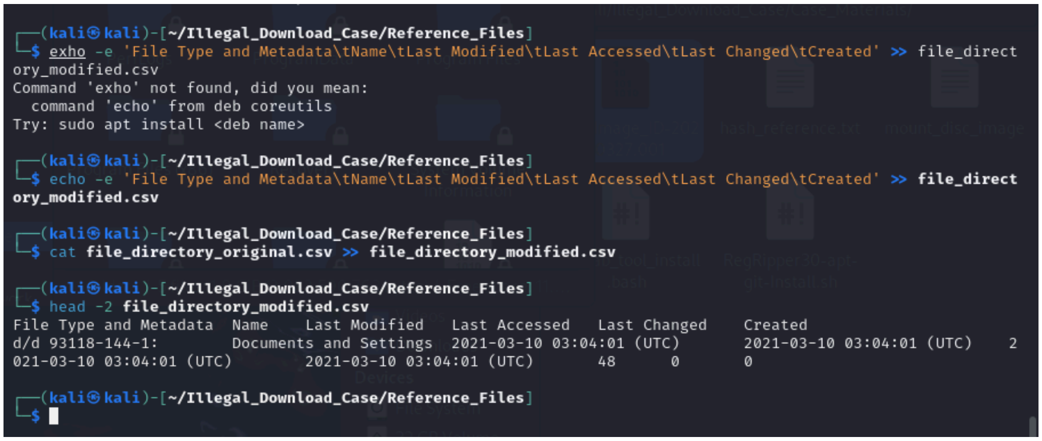
grep to search web browser:



kali@kali: ~/Illegal_Download_Case/Reference_Files
File Actions Edit View Help
Network

```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ grep -F '.exe' file_directory_original.csv | grep -iE 'msdege|forefpx|chrome|iexplore' | cut -f 1,2,4,5
r/r 74304-128-5:        Program Files/Internet Explorer/en-US/iexplore.exe.mui  2021-03-21 20:08:40 (UTC)    2
021-03-10 03:00:20 (UTC)
r/r 54056-128-4:        Program Files/Internet Explorer/iexplore.exe    2021-03-27 02:37:18 (UTC)       2021-0
3-21 20:28:53 (UTC)
r/r 74304-128-5:        Program Files (x86)/Internet Explorer/en-US/iexplore.exe.mui    2021-03-21 20:08:40 (U
TC)     2021-03-10 03:00:20 (UTC)
r/r 54057-128-4:        Program Files (x86)/Internet Explorer/iexplore.exe      2021-03-27 14:11:30 (UTC)    2
021-03-21 20:28:53 (UTC)
r/r 74304-128-5:        Windows/WinSxS/amd64_microsoft-windows-i..-optional.resources_31bf3856ad364e35_11.0.19
041.1_en-us_7c457a2cefaa6d0d/iexplore.exe.mui   2021-03-21 20:08:40 (UTC)       2021-03-10 03:00:20 (UTC)
r/r 54056-128-4:        Windows/WinSxS/amd64_microsoft-windows-i..etexplorer-optional_31bf3856ad364e35_11.0.19
041.1_none_8298e4b5b7fd2c26/iexplore.exe        2021-03-27 02:37:18 (UTC)       2021-03-21 20:28:53 (UTC)
r/r 74304-128-5:        Windows/WinSxS/wow64_microsoft-windows-i..-optional.resources_31bf3856ad364e35_11.0.19
041.1_en-us_869a247f240b2f08/iexplore.exe.mui   2021-03-21 20:08:40 (UTC)       2021-03-10 03:00:20 (UTC)
r/r 54057-128-4:        Windows/WinSxS/wow64_microsoft-windows-i..etexplorer-optional_31bf3856ad364e35_11.0.19
041.1_none_8ced8f07ec5dee21/iexplore.exe        2021-03-27 14:11:30 (UTC)       2021-03-21 20:28:53 (UTC)
r/r 74304-128-5:        Program Files/Internet Explorer/en-US/iexplore.exe.mui  2021-03-21 20:08:40 (UTC)    2
021-03-10 03:00:20 (UTC)
r/r 54056-128-4:        Program Files/Internet Explorer/iexplore.exe    2021-03-27 02:37:18 (UTC)       2021-0
3-21 20:28:53 (UTC)
r/r 74304-128-5:        Program Files (x86)/Internet Explorer/en-US/iexplore.exe.mui    2021-03-21 20:08:40 (U
TC)     2021-03-10 03:00:20 (UTC)
r/r 54057-128-4:        Program Files (x86)/Internet Explorer/iexplore.exe      2021-03-27 14:11:30 (UTC)    2
021-03-21 20:28:53 (UTC)
r/r 74304-128-5:        Windows/WinSxS/amd64_microsoft-windows-i..-optional.resources_31bf3856ad364e35_11.0.19
041.1_en-us_7c457a2cefaa6d0d/iexplore.exe.mui   2021-03-21 20:08:40 (UTC)       2021-03-10 03:00:20 (UTC)
r/r 54056-128-4:        Windows/WinSxS/amd64_microsoft-windows-i..etexplorer-optional_31bf3856ad364e35_11.0.19
041.1_none_8298e4b5b7fd2c26/iexplore.exe        2021-03-27 02:37:18 (UTC)       2021-03-21 20:28:53 (UTC)
r/r 74304-128-5:        Windows/WinSxS/wow64_microsoft-windows-i..-optional.resources_31bf3856ad364e35_11.0.19
041.1_en-us_869a247f240b2f08/iexplore.exe.mui   2021-03-21 20:08:40 (UTC)       2021-03-10 03:00:20 (UTC)
r/r 54057-128-4:        Windows/WinSxS/wow64_microsoft-windows-i..etexplorer-optional_31bf3856ad364e35_11.0.19
041.1_none_8ced8f07ec5dee21/iexplore.exe        2021-03-27 14:11:30 (UTC)       2021-03-21 20:28:53 (UTC)
r/r 74304-128-5:        Program Files/Internet Explorer/en-US/iexplore.exe.mui  2021-03-21 20:08:40 (UTC)    2
```

Using echo to make columns and then cat to output contents:



```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ exho -e 'File Type and Metadata\tName\tLast Modified\tLast Accessed\tLast Changed\tCreated' >> file_direct
ory_modified.csv
Command 'exho' not found, did you mean:
  command 'echo' from deb coreutils
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ echo -e 'File Type and Metadata\tName\tLast Modified\tLast Accessed\tLast Changed\tCreated' >> file_direct
ory_modified.csv

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ cat file_directory_original.csv >> file_directory_modified.csv

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ head -2 file_directory_modified.csv
File Type and Metadata  Name    Last Modified   Last Accessed   Last Changed    Created
d/d 93118-144-1:        Documents and Settings  2021-03-10 03:04:01 (UTC)       2021-03-10 03:04:01 (UTC)    2
021-03-10 03:04:01 (UTC)        2021-03-10 03:04:01 (UTC)       48      0       0

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ █
```