Title: Use PhotoRec to recover lost files, audio or video content from the HDD/USB Drive using file carving

Objective:

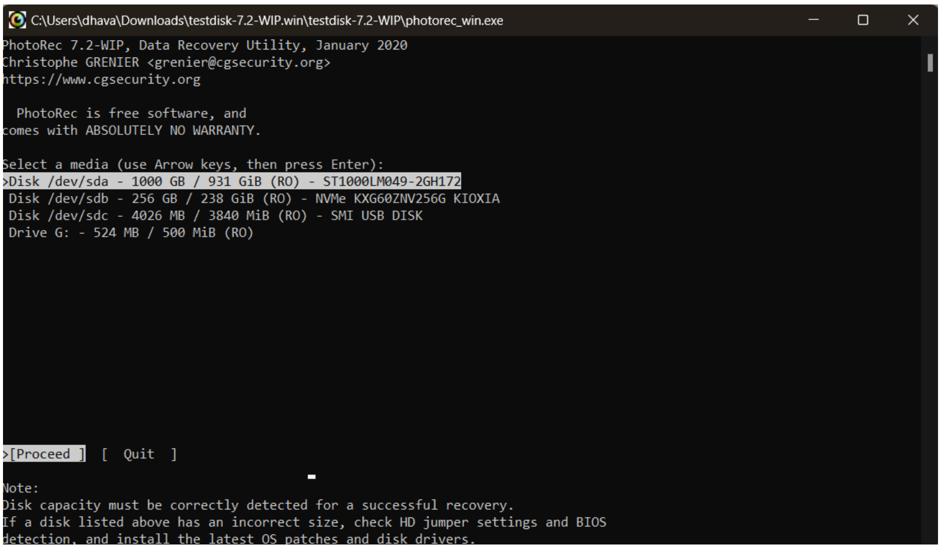
The objective of this experiment is to utilize PhotoRec, a file recovery tool, to recover lost files, including audio and video content, from an HDD or USB drive using file carving techniques.

Requirements:

PhotoRec
Disk or drive contain lost file for recovery

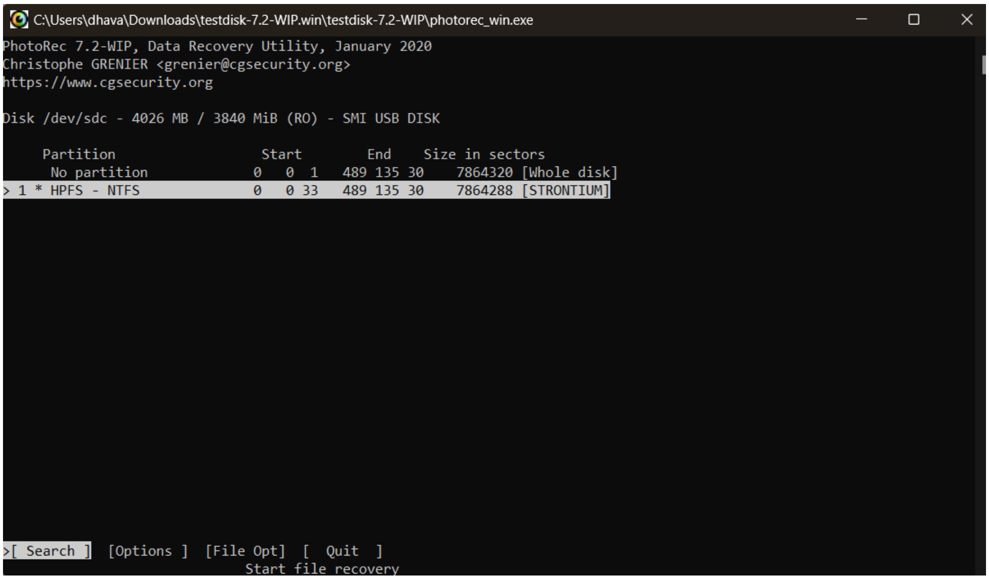
Procedure/Experiment Steps:

1. Prepare the Environment: Ensure that the computer meets the system requirements for running PhotoRec. Install PhotoRec on the computer.
2. Connect HDD/USB Drive: Connect the HDD or USB drive containing the lost files to be recovered to the computer.
3. Launch PhotoRec: Start PhotoRec from the installed location or command-line interface.


C:\Users\dhava\Downloads\testdisk-7.2-WIP.win\testdisk-7.2-WIP\photorec_win.exe

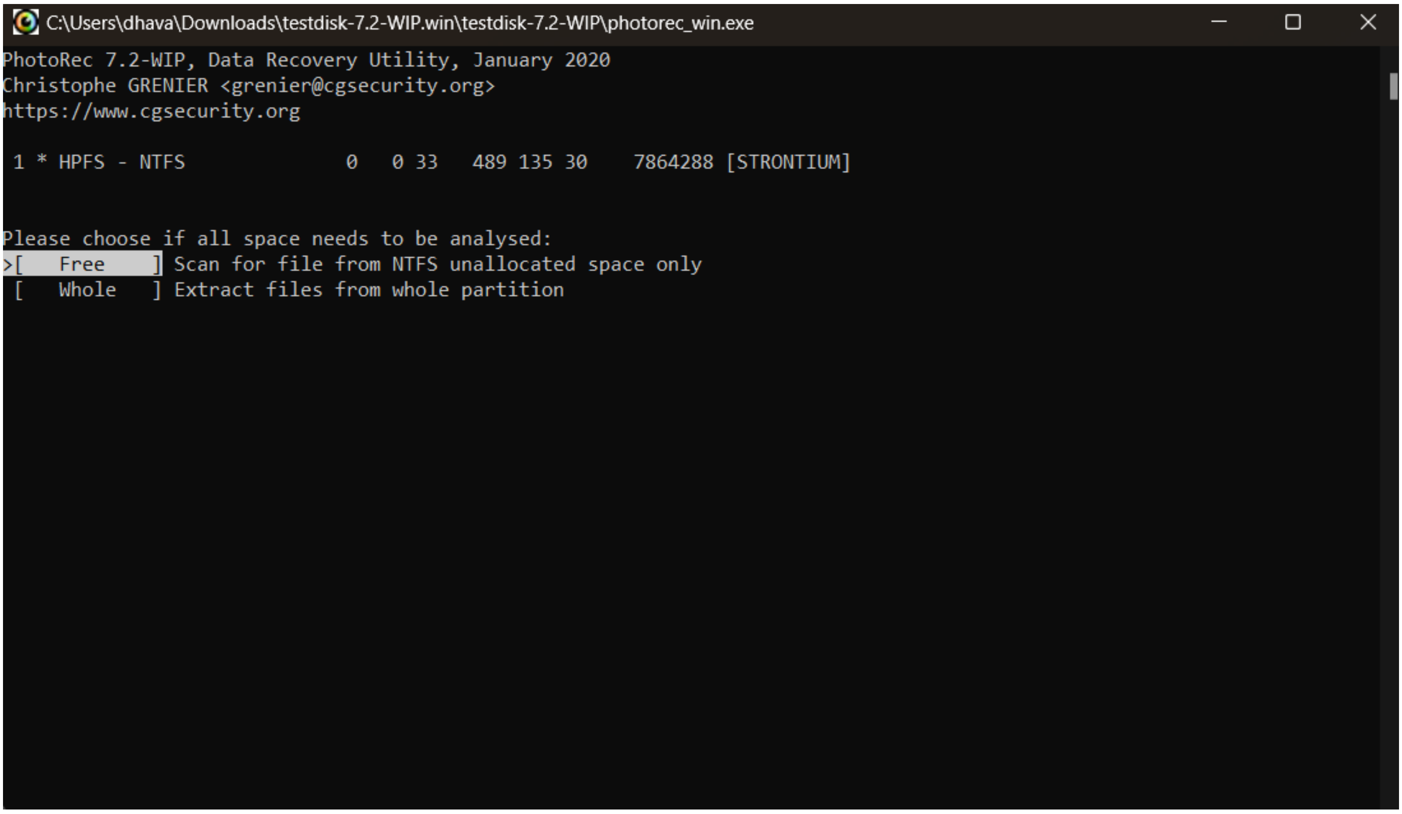
```
PhotoRec 7.2-WIP, Data Recovery Utility, January 2020
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

  PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk /dev/sda - 1000 GB / 931 GiB (RO) - ST1000LM049-2GH172
 Disk /dev/sdb - 256 GB / 238 GiB (RO) - NVMe KXG60ZNV256G KIOXIA
 Disk /dev/sdc - 4026 MB / 3840 MiB (RO) - SMI USB DISK
 Drive G: - 524 MB / 500 MiB (RO)




>[Proceed ]  [  Quit  ]

Note:
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has an incorrect size, check HD jumper settings and BIOS
detection, and install the latest OS patches and disk drivers.
```

4. Select Target Drive: Choose the target drive (HDD or USB drive) from which the lost files need to be recovered using PhotoRec.


C:\Users\dhava\Downloads\testdisk-7.2-WIP.win\testdisk-7.2-WIP\photorec_win.exe

```
PhotoRec 7.2-WIP, Data Recovery Utility, January 2020
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdc - 4026 MB / 3840 MiB (RO) - SMI USB DISK

     Partition                  Start        End    Size in sectors
      No partition             0   0  1   489 135 30    7864320 [Whole disk]
> 1 * HPFS - NTFS              0   0 33   489 135 30    7864288 [STRONTIUM]




>[ Search ]  [Options ]  [File Opt]  [  Quit  ]
                              Start file recovery
```

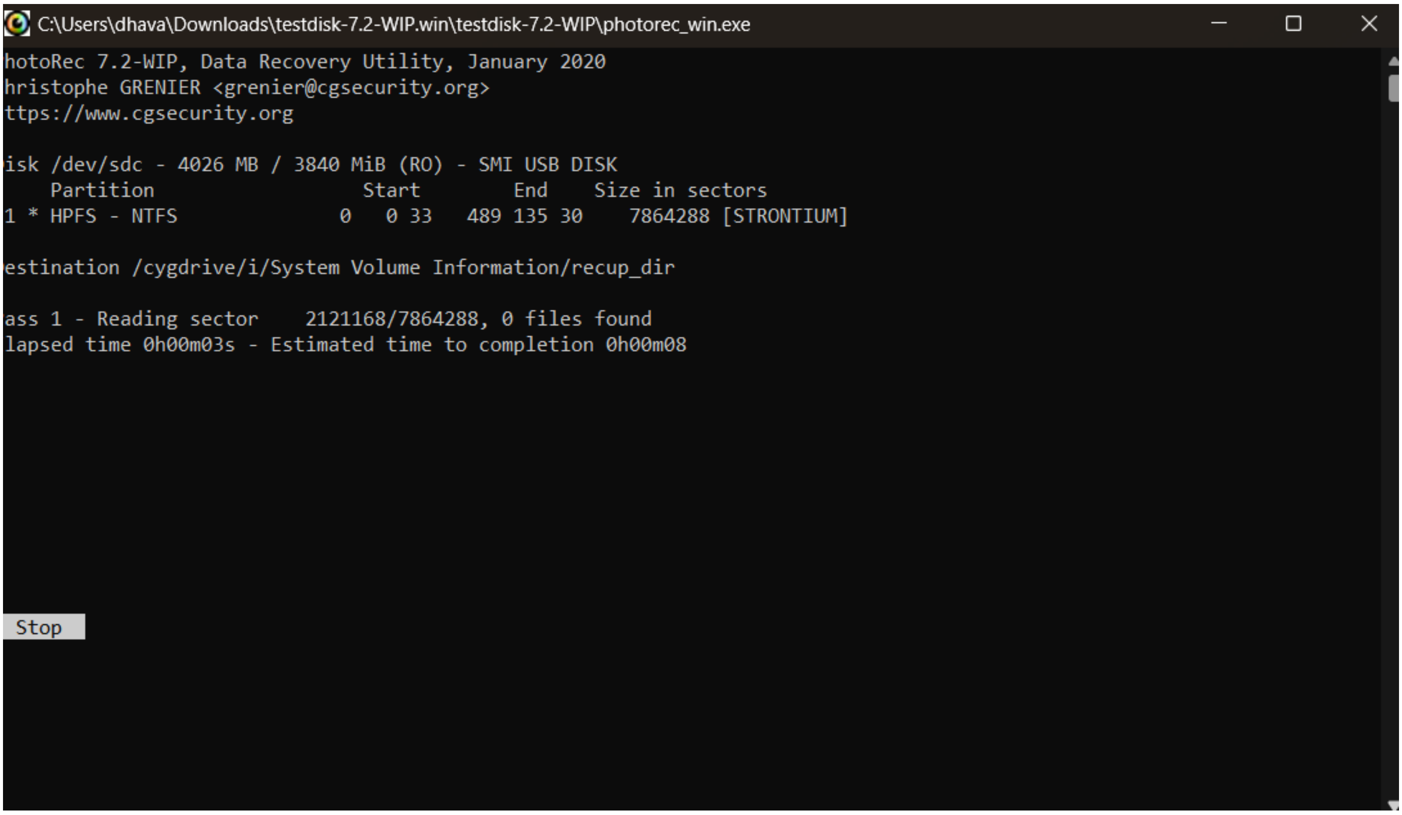
5. Configure File Carving Settings: Configure the file carving settings within PhotoRec, such as the file types to recover (e.g., audio, video), block size, and other advanced options as needed.



C:\Users\dhava\Downloads\testdisk-7.2-WIP.win\testdisk-7.2-WIP\photorec_win.exe

```
PhotoRec 7.2-WIP, Data Recovery Utility, January 2020
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

 1 * HPFS - NTFS              0   0 33   489 135 30    7864288 [STRONTIUM]


Please choose if all space needs to be analysed:
>[   Free    ] Scan for file from NTFS unallocated space only
 [   Whole   ] Extract files from whole partition
```

6. Start Recovery Process: Initiate the file recovery process in PhotoRec to scan the target drive for lost files and employ file carving techniques to recover them.

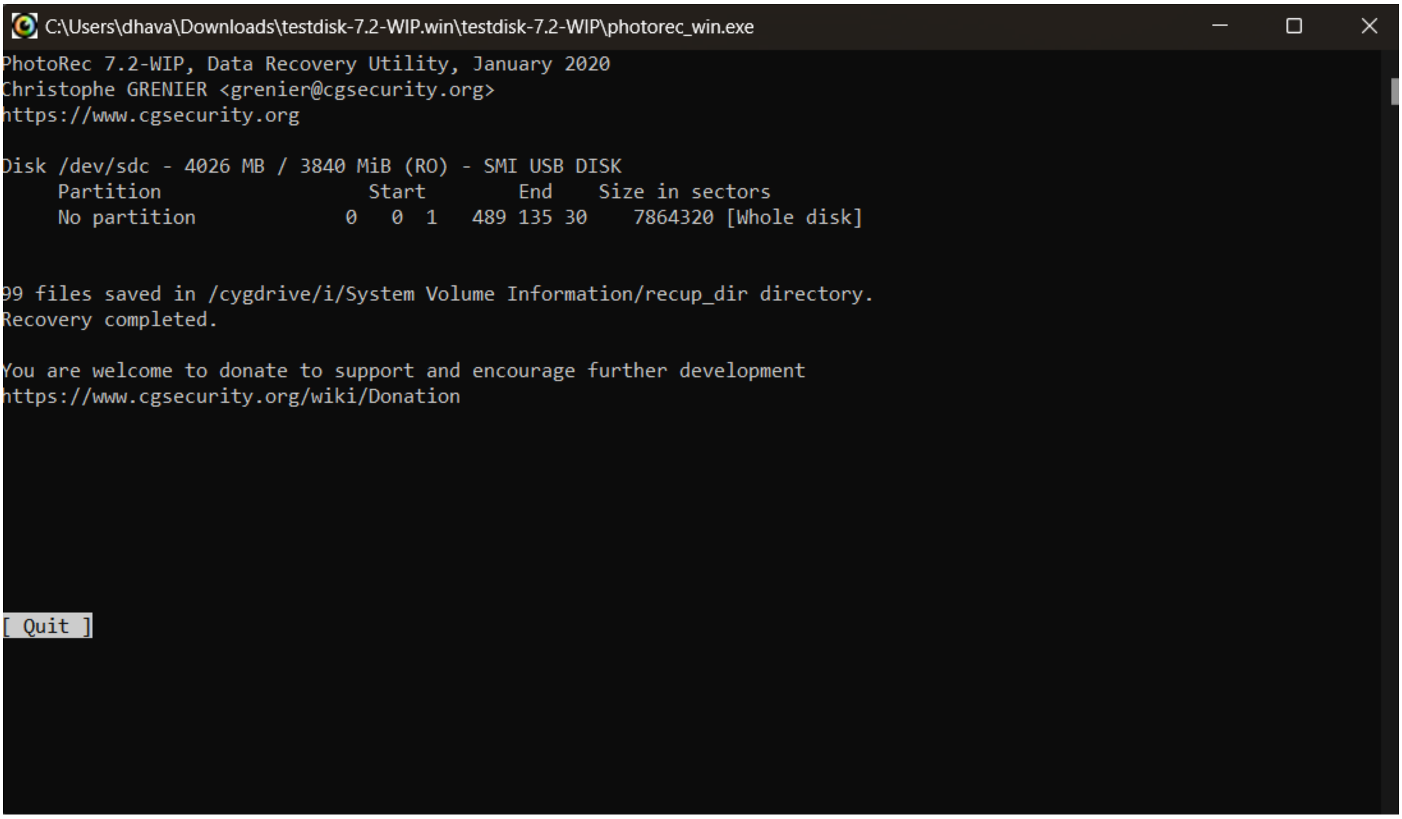


C:\Users\dhava\Downloads\testdisk-7.2-WIP.win\testdisk-7.2-WIP\photorec_win.exe

```
hotoRec 7.2-WIP, Data Recovery Utility, January 2020
hristophe GRENIER <grenier@cgsecurity.org>
ttps://www.cgsecurity.org

isk /dev/sdc - 4026 MB / 3840 MiB (RO) - SMI USB DISK
    Partition                  Start        End    Size in sectors
1 * HPFS - NTFS              0   0 33   489 135 30    7864288 [STRONTIUM]

estination /cygdrive/i/System Volume Information/recup_dir

ass 1 - Reading sector    2121168/7864288, 0 files found
lapsed time 0h00m03s - Estimated time to completion 0h00m08






 Stop
```

7. Monitor Recovery Progress: Monitor the recovery progress within PhotoRec, allowing the tool to scan and analyze the target drive for recoverable files.

8. Review Recovered Files: Once the recovery process is complete, review the recovered files within PhotoRec. Verify the integrity of the recovered files and organize them accordingly.


C:\Users\dhava\Downloads\testdisk-7.2-WIP.win\testdisk-7.2-WIP\photorec_win.exe

```
PhotoRec 7.2-WIP, Data Recovery Utility, January 2020
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdc - 4026 MB / 3840 MiB (RO) - SMI USB DISK
     Partition                  Start        End    Size in sectors
     No partition             0   0  1   489 135 30    7864320 [Whole disk]


99 files saved in /cygdrive/i/System Volume Information/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation
```

9. Document Findings: Record the details of the recovery process, including notable recovered files, their original locations (if available), and any other relevant observations.

Result:

Using PhotoRec, we successfully recovered lost files, including audio and video content, from the HDD/USB drive. By selecting the target drive and configuring the file carving settings, we initiated the recovery process in PhotoRec. Upon completion, we reviewed the recovered files, verified their integrity, and organized them for further analysis. Notable findings, including recovered files and relevant observations, were documented for future reference.

Conclusion:

PhotoRec proved to be an effective file recovery tool for retrieving lost files, including audio and video content, from an HDD or USB drive using file carving techniques. Through its usage, we were able to scan and recover files that were no longer accessible through conventional means. File carving plays a crucial role in forensic investigations, data recovery processes, and restoring important data from various storage devices.

Future Scope:

1. Advanced file carving techniques: Explore PhotoRec's advanced options and techniques for specific file types, fragmented files, or customized file signatures.
2. Disk imaging integration: Integrate PhotoRec with disk imaging tools to recover files from disk images, improving the efficiency and flexibility of file recovery processes.
3. Automated recovery workflows: Investigate the automation capabilities of PhotoRec, enabling the creation of custom recovery workflows and scripts to streamline the recovery process.
4. Integration with other forensic tools: Explore the integration of PhotoRec with other digital forensic tools to enhance analysis, cross-validation of findings, and a more comprehensive recovery process.

5. Stay updated with PhotoRec: Regularly update PhotoRec to benefit from the latest features, improvements, and support for new file formats or carving techniques, ensuring efficient and accurate file recovery.