1. INTRODUCTION

Kali Linux is the world's most powerful and popular penetration testing platform, used by security. Professionals in a wide range of specializations, including penetration testing, forensics, Reverse Engineering, and vulnerability assessment. It is the culmination of years of refinement and the Result of a continuous evolution of the platform, from Knoppix to WHAX, to backtrack, and now to a complete penetration testing framework leveraging many features of Debian GNU/Linux and the vibrant open source community worldwide. Kali Linux has not been built to be a simple collection of tools, but rather a flexible framework that professional penetration testers, security enthusiasts, students, and amateurs can customize to fit their specific needs.

1.1Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

It was developed by MatiAharoni and Devon Kearns of Offensive Security through the rewrite of Backtrack, their previous information security testing Linux distribution based on Knoppix. The third core developer Raphael Hertzog joined them as a Debian expert. Kali Linux was released on the 13th march, 2013 as a complete, top to bottom. Rebuild of Backtrack Linux, adhering completely toDebian development standards.

* OS Family - UNIX like
* Working State – Active
* Platforms - x86, x86-64, armel, armhf
* Kernel Type - Monolithic kernel (Linux)
* Default UI - GNOME3
* Latest Release – 2017.2 - September 20, 2017

1.2 PENETRATION TESTING

Penetration testing (also called **pen testing**) is the practice of **testing** a computer system,network or Web application to find vulnerabilities that an attacker could exploit. Penetration testing tools are used as part of a penetration test (Pen Test) to automate certain tasks, improve testing efficiency and discover issues that might be difficult to find using manual analysis techniques alone. Two common penetration testing tools are static analysis tools and dynamic analysis tools. Veracode performs both dynamic and static code analysis and finds security vulnerabilities that include malicious code as well as the absence of functionality that may lead to security breaches.

A **penetration test**, or **pen-test**, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations or risky end-user behavior. **Performed for**: Websites/Servers/Networks.

1.2.1 Types of Penetration Testing

Network services test: This is one of the most common types of penetration tests, and involves finding target systems on the network, searching for openings in their base operating systems and available network services, and then exploiting them remotely. Some of these network service penetration tests take place remotely across the Internet, targeting the organization's perimeter networks. Others are launched locally, from the target's own business facilities, to assess the security of their internal network or the DMZ from within, seeing what kinds of vulnerabilities an internal user could learn.

Client-side test: This kind of penetration test is intended to find vulnerabilities in and exploit client-side software, such as web browsers, media players, document editing programs, etc.

Web application test: These penetration tests look for security vulnerabilities in the webbased applications and programs deployed and installed on the target environment.

Remote dial-up war dial: These penetration tests look for modems in a target environment, and normally involve password guessing or brute forcing to login to systems connected to discovered modems.

Wireless security test: These penetration tests involve discovering a target's physical environment to find unauthorized wireless access points or authorized wireless access points with security weaknesses.

Social engineering test: This type of penetration test involves attempting to make a user into revealing sensitive information such as a password or any other sensitive data. These tests are often conducted over the phone, targeting selected help desks, users or employees, evaluating processes, procedures, and user awareness.

1.3 VULNERABILITY TESTING

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat. Vulnerability and Penetration Testing (VAPT) are two types of vulnerability testing. The tests have different strengths and are often combined to achieve a more complete vulnerability

analysis. In short, Penetration Testing and Vulnerability Assessments perform two different tasks, usually with different results, within the same area of focus. Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot. Vulnerability

Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application. Penetration tests find exploitable flaws and measure the severity of each.

A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system. Together, penetration testing and vulnerability assessment tools provide a detailed picture of the flaws that exist in an application and the risks associated with those flaws.

Vulnerability Assessment and Penetration Testing (VAPT) provides enterprises with a more comprehensive application evaluation than any single test alone. Using the Vulnerability Assessment and Penetration Testing (VAPT) approach gives an organization a more detailed view of the threats facing its applications, enabling the business to better protect its systems and data from malicious attacks. Vulnerabilities can be found in applications from third-party vendors and internally made software, but most of these flaws are easily fixed once found. Using a VAPT provider enables IT security teams to focus on mitigating critical vulnerabilities while the VAPT provider continues to discover and classify vulnerabilities.

1.4 COMPUTER FORENSICS

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Computer forensics is a very important branch of computer science in relation to computer and Internet related crimes. Earlier, computers were only used to produce data but now it has expanded to all devices related to digital data. The goal of Computer forensics is to perform

crime investigations by using evidence from digital data to find who was the responsible for that particular crime.

For better research and investigation, developers have created many computer forensics tools. Police departments and investigation agencies select the tools based on various factors including budget and available experts on the team.

1.5 FORENSIC TOOLS

Forensic tools can also be classified into various categories:

* Disk and data capture tools
* File analysis tools
* Internet analysis tools
* Email analysis tools
* Mobile devices analysis tools
* Mac OS analysis tools
* Network forensics tools
* Database forensics tools

2. PHOTOREC

PhotoRec is file data recovery software designed to recover lost files including video, documents and archives from hard disks, CD-ROMs, and lost pictures (thus the Photo Recovery name) from digital camera memory. PhotoRec ignores the file system and goes after the underlying data, so it will still work even if your media's file system has been severely damaged or reformatted.

PhotoRec is free - this open source multi-platform application is distributed under GNU General Public License (GPLV v2+). PhotoRec is a companion program to TestDisk, an application for recovering lost partitions on a wide variety of file systems and making nonbootable disks bootable again. You can download them from this link.

For more safety, PhotoRec uses read-only access to handle the drive or memory card you are about to recover lost data from. Important: As soon as a picture or file is accidentally deleted, or you discover any missing, do NOT save any more pictures or files to that memory device or hard disk drive; otherwise you may overwrite your lost data. This means that while using PhotoRec, you must not choose to write the recovered files to the same partition they were stored on.

2.1 STEPS

* Run the command Photorec.
* Select a Disk and press Enter.
* Press [File opt] and specify the locating file formats.
* Press [search] option.
* Select the file system.
* Choose the directory to saving the recovered files.

* Start the recovery process.
* Recovery process is progressing until [stop] option is choose.
* Using [quit] option.
* Save the recovered files to the pre-determined directory.

2.2 FEATURES

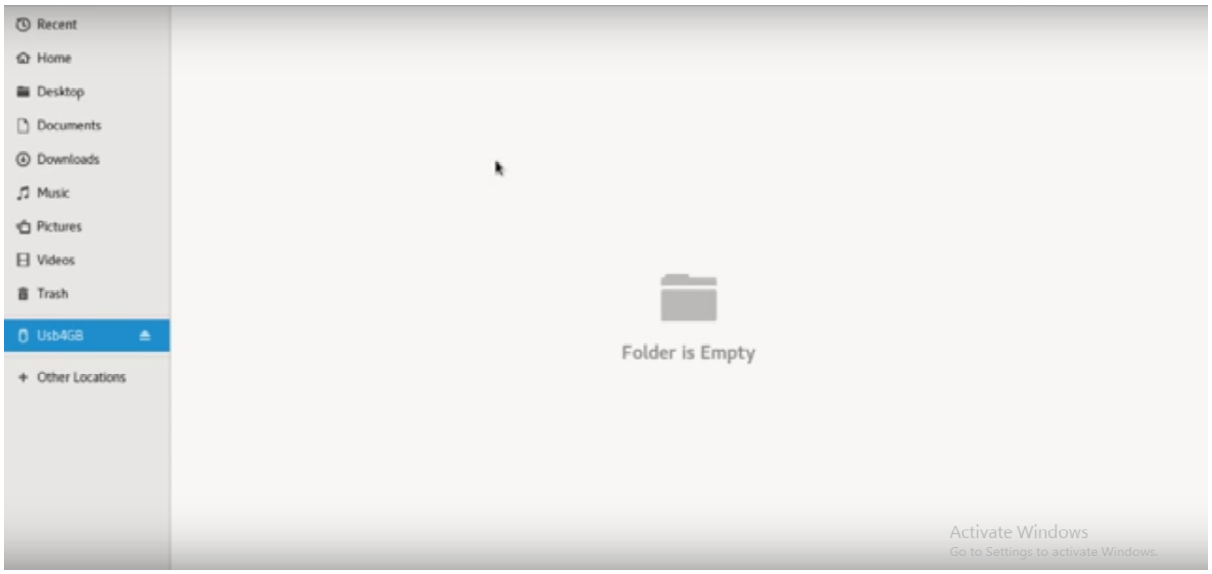
* Simplest method.
* Easy to understand.
* Recover all kind of lost files from all medias such as HDD, USB drive, Micro drive, memory cards etc.
* Open source.
* Multi – platform application.
* Photorec is compatible with almost all OS.

2.3 DRAWBACKS

* Time consuming
* Recovery depends on current memory status of the drive.

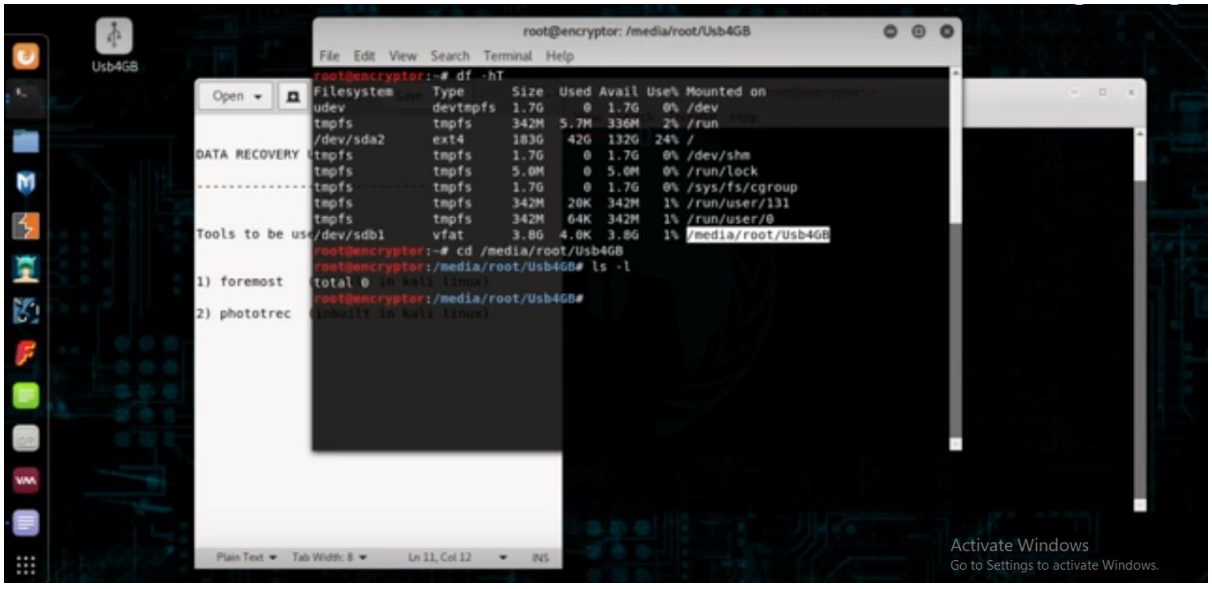
2.4 OPERATIONS USING PHOTOREC

* Open a formatd disk

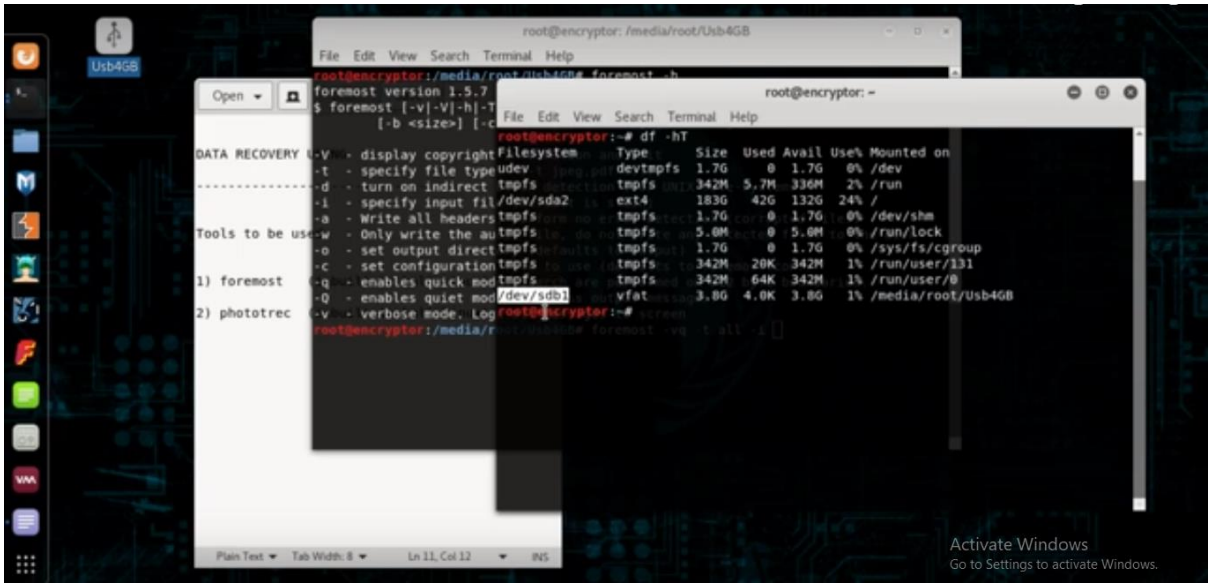


*Open formost tool

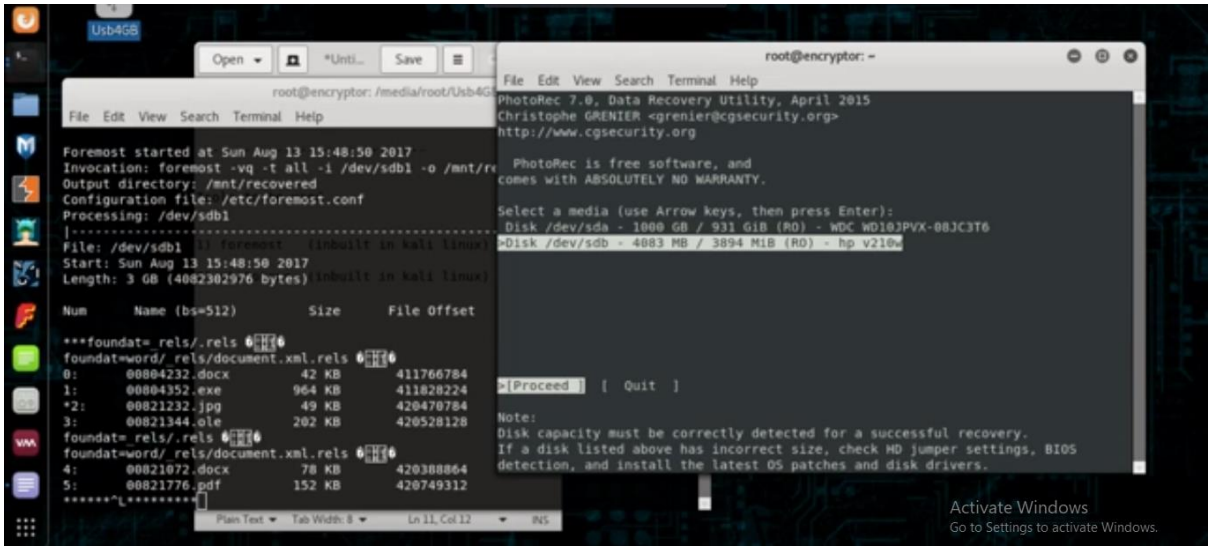
*Copy the root file path



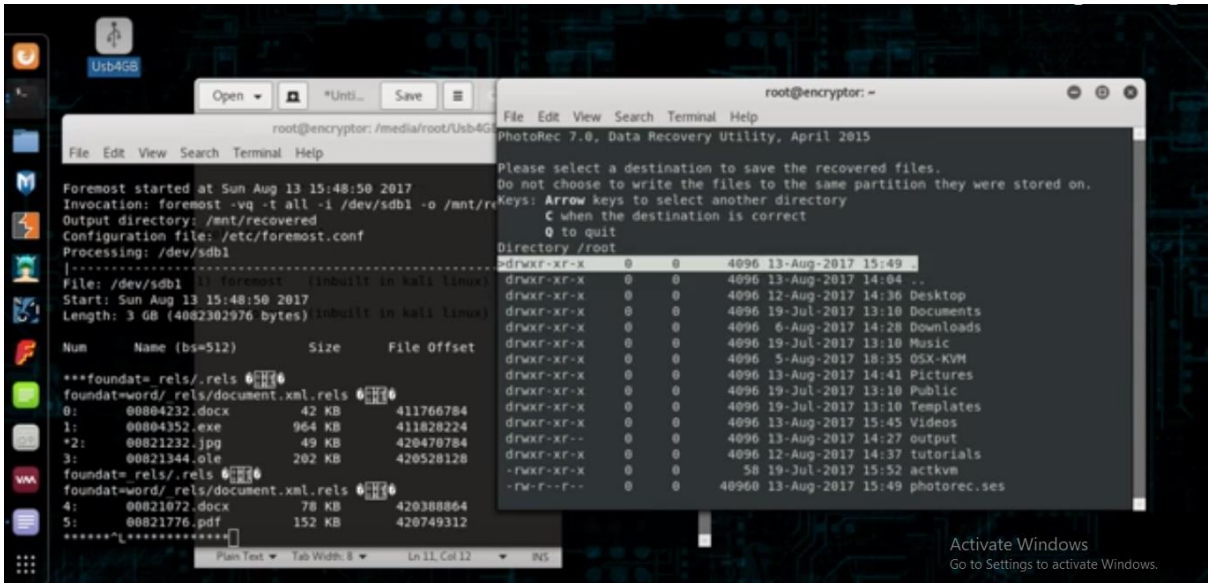
*Open a new terminal Copy the sub directory



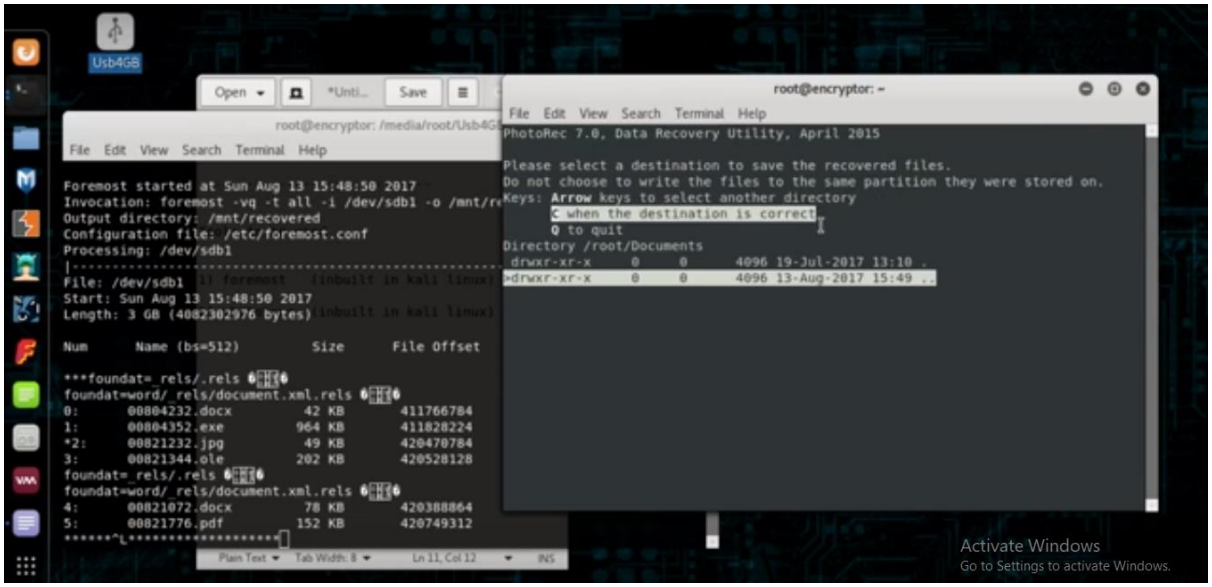
***Open photorec & Select disk**



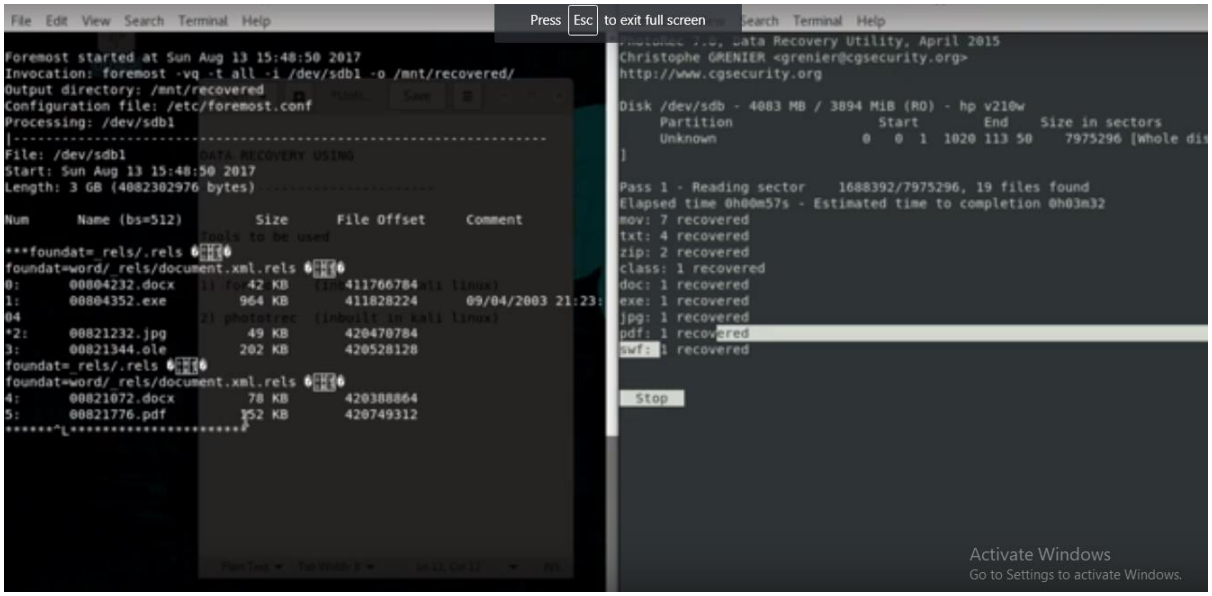
*Deleted files are retrived



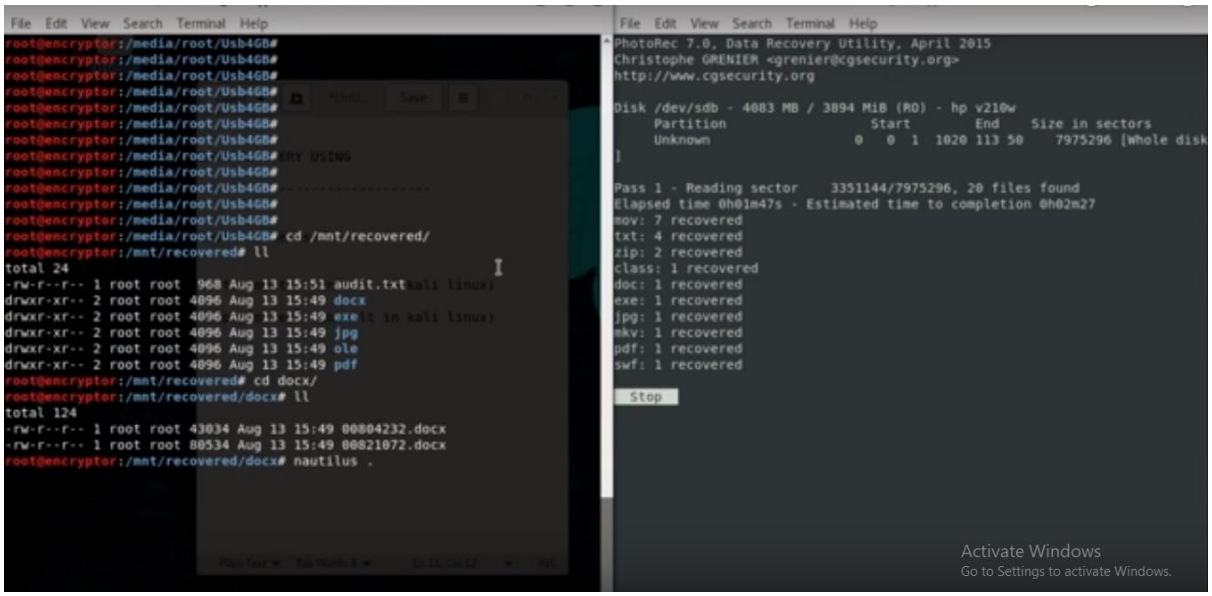
*Press c when the destination is correct



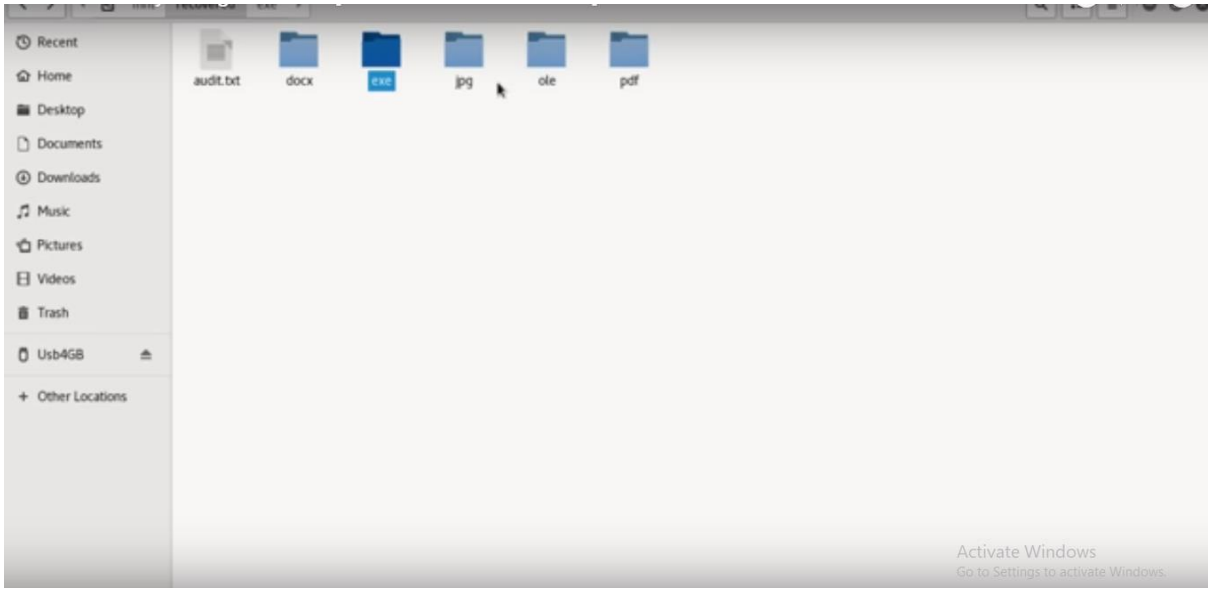
***Files are recovered**



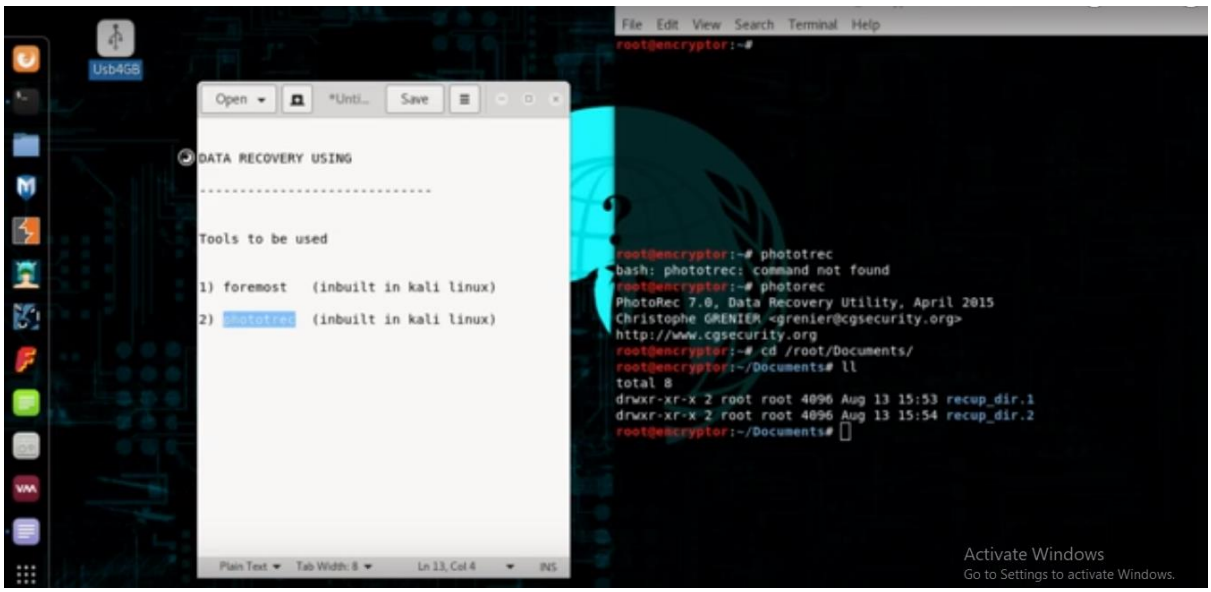
*Check the root directory



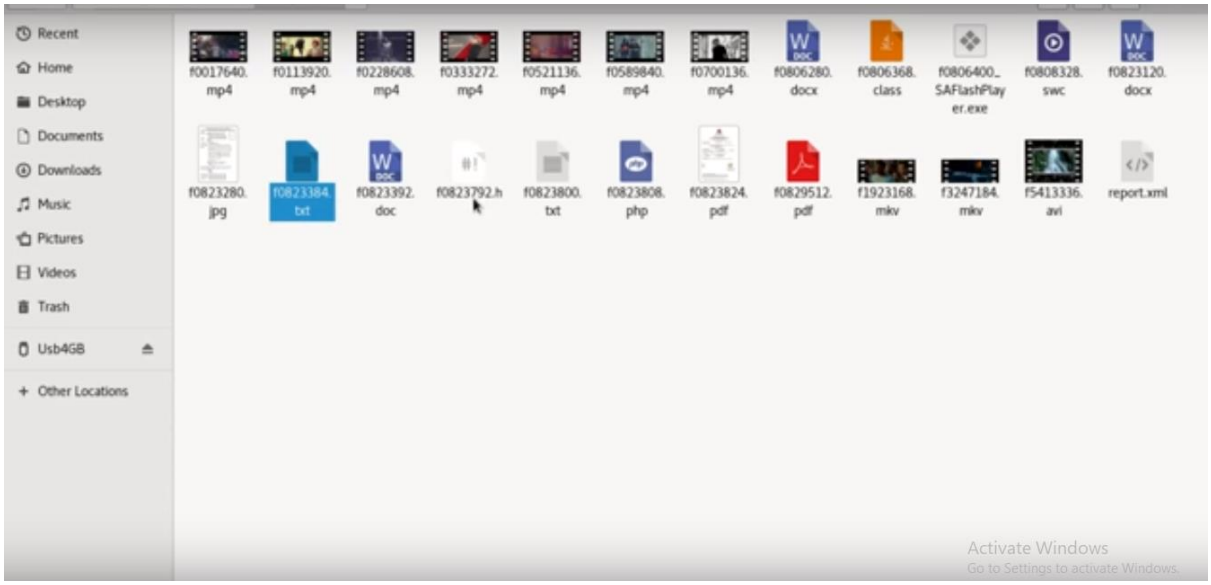
* Open the recovered folders



*Close the terminals



* Open different types of folders



3. CONCLUSION

Photorec has been used in various investigations.In case of recovery, Photorec tool is all in one tool. Photorec recover all kind of lost files from various medias such as HDD, USB drives, CD – ROM, memory cards, Micro drive etc.Easy and simple way of recovery.

For more safety, PhotoRec uses read-only access to handle the drive or memory card you are about to recover lost data from. Important: As soon as a picture or file is accidentally deleted, or you discover any missing, do NOT save any more pictures or files to that memory device or hard disk drive; otherwise you may overwrite your lost data. This means that while using PhotoRec, you must not choose to write the recovered files to the same partition they were stored on.

4. REFERENCES

* http://sourceforge.net/projects/photorec/

* http://www.wotsit.org

* https://tools.kali.org/forensics/photorec