Information Security Analysis and Audit

Course Code: CSE3501

Slot: L47-48

Faculty: Dr. Anil Kumar K

Assessment: 2

18BCI0247

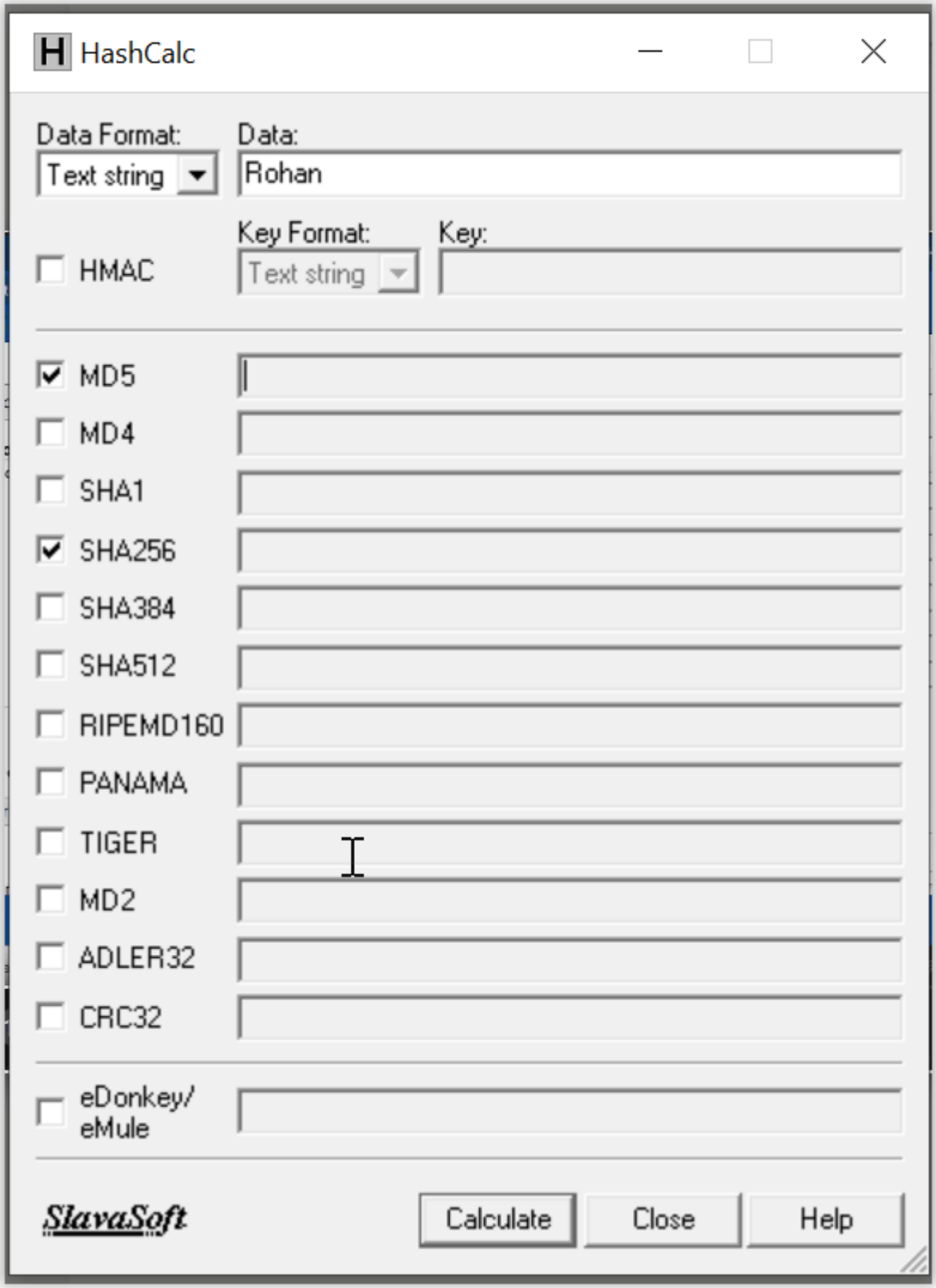
Rohan Allen

Exercise 1:

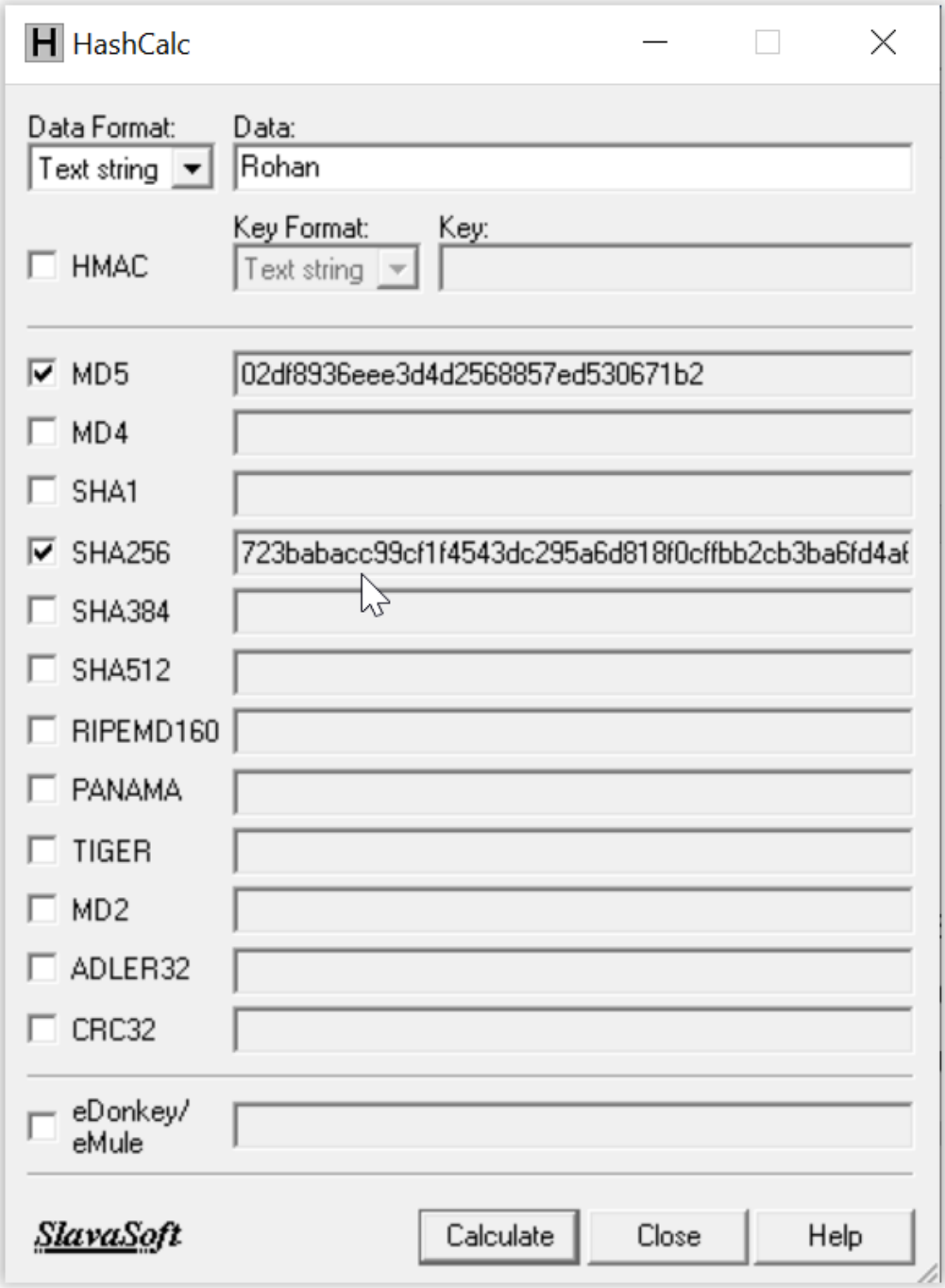
Experiments in HashCalc software.

This is a software that returns a hash value of any input. It uses multiple hash functions like SHA1, SHA256, MD5, etc.

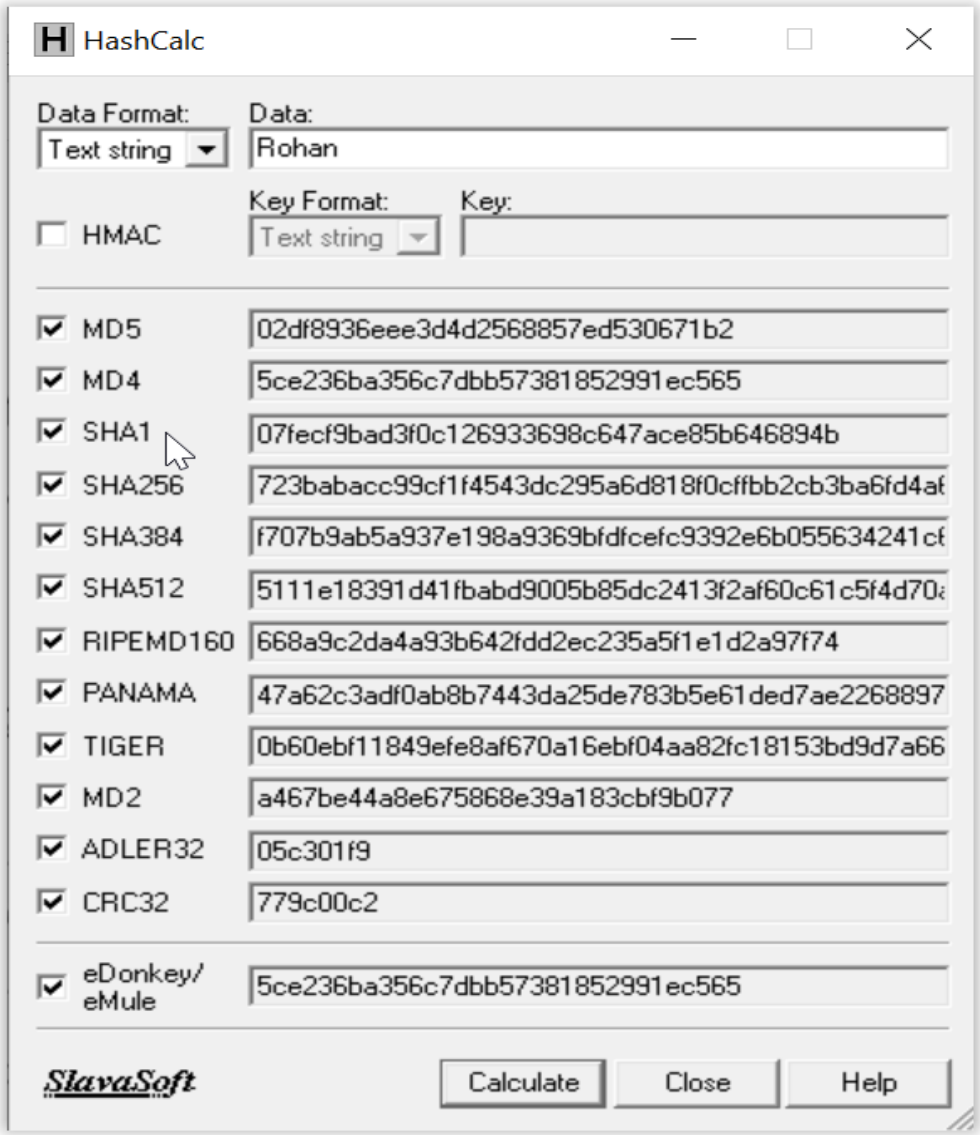
Enter input text “Rohan”.



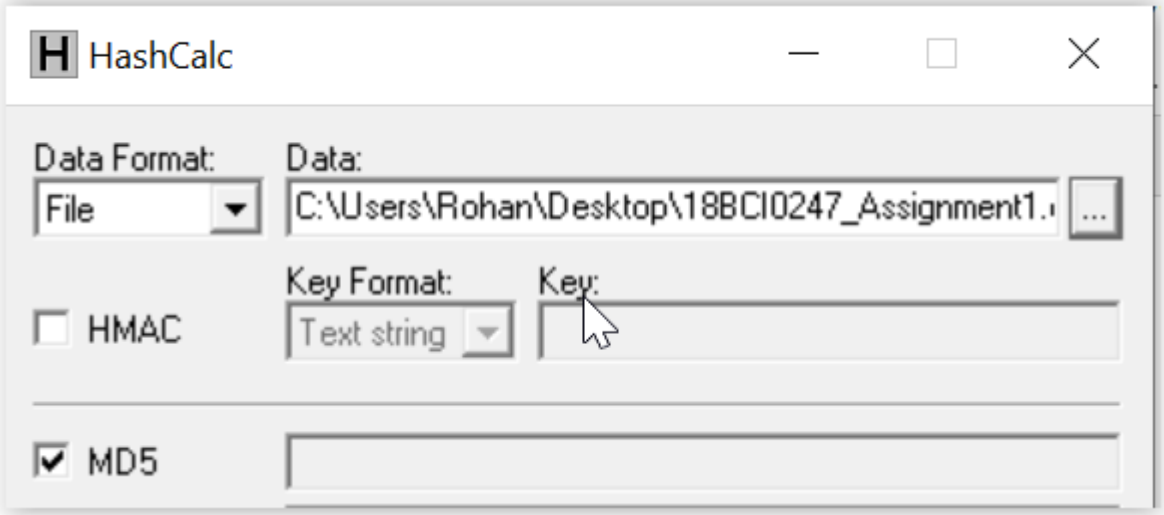
Hash value using MD5 and SHA256 hash algorithm.



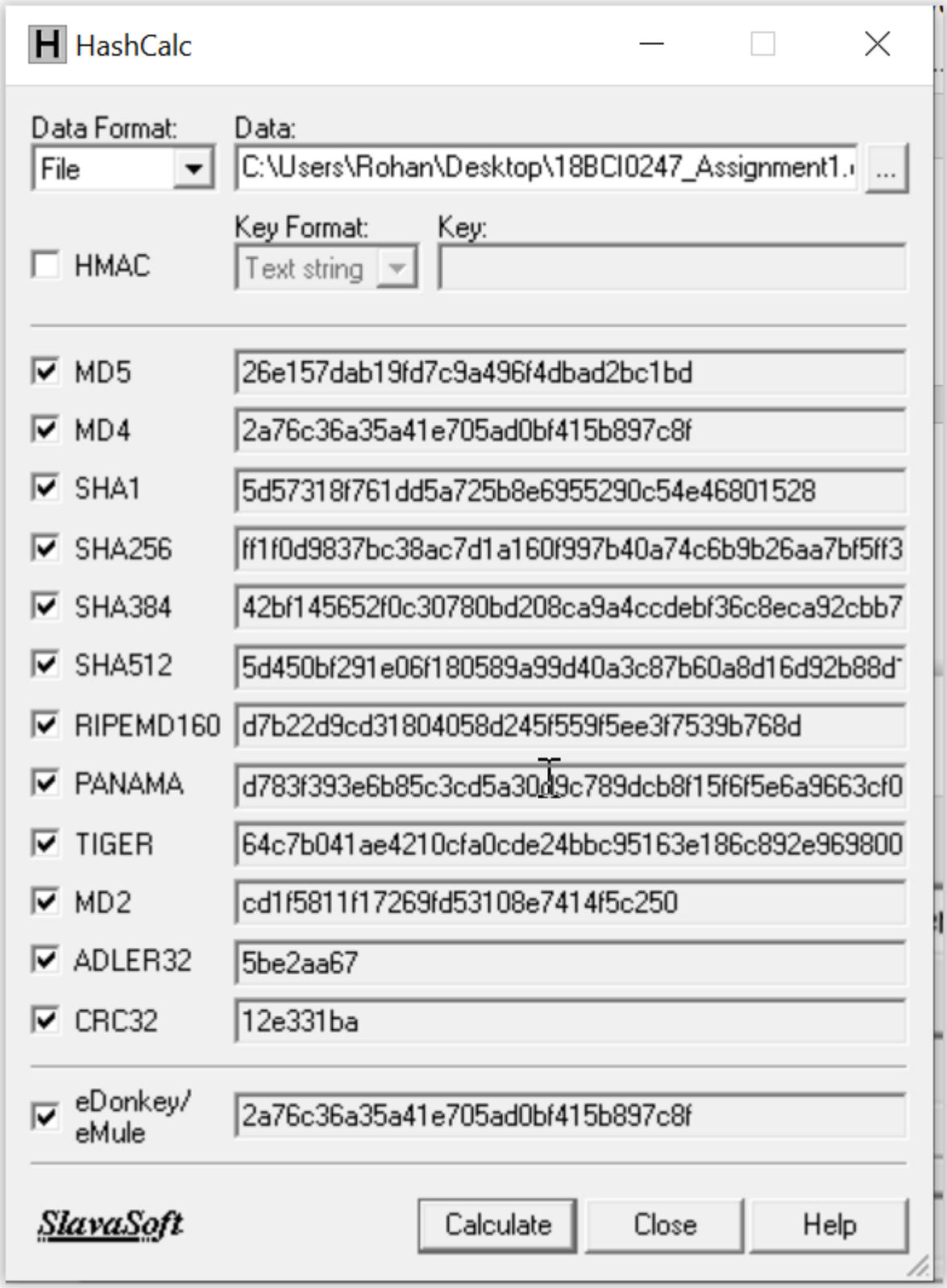
Hash value using all the hash functions available.



Selecting a file to hash



Hash values of the file.

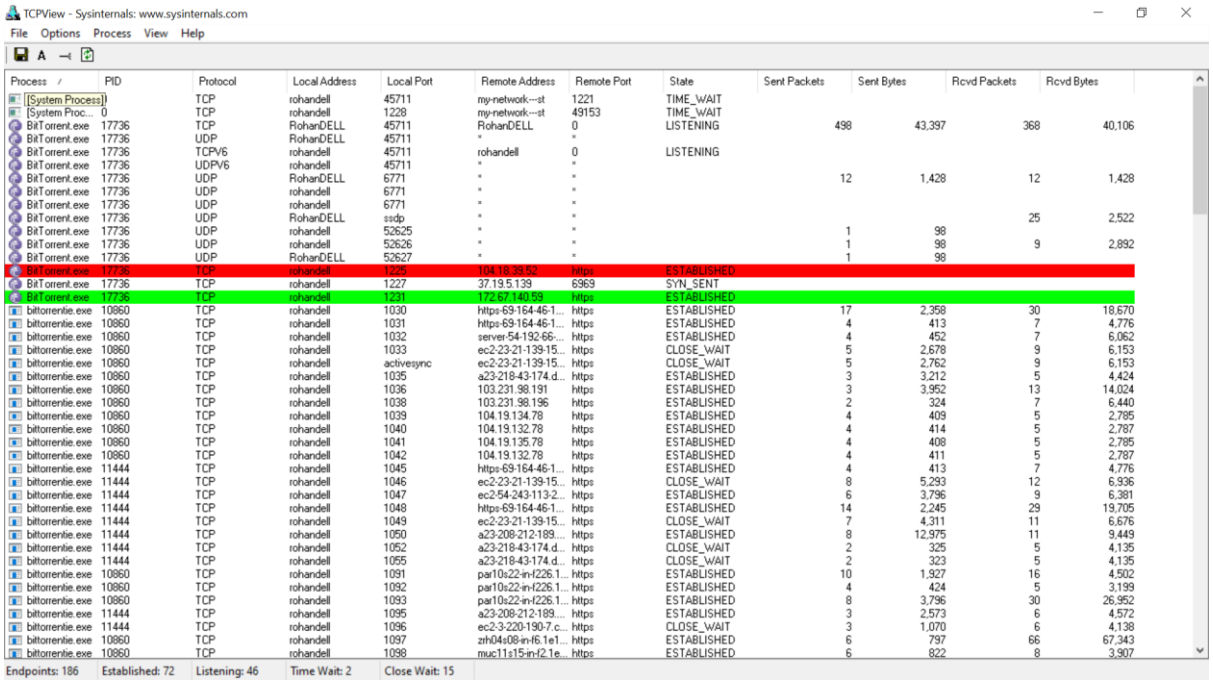


Exercise 2:

Experimenting with SysInternal tools:

Tool 1: TCPView v3.05

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections



TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Process]		TCP	rohandell	45711	my-network---st	1221	TIME_WAIT				
[System Proc...	0	TCP	rohandell	1228	my-network---st	49153	TIME_WAIT				
BitTorrent.exe	17736	TCP	RohanDELL	45711	RohanDELL	0	LISTENING	498	43,397	368	40,106
BitTorrent.exe	17736	UDP	RohanDELL	45711	*	*					
BitTorrent.exe	17736	TCPV6	rohandell	45711	rohandell	0	LISTENING				
BitTorrent.exe	17736	UDPV6	rohandell	45711	*	*					
BitTorrent.exe	17736	UDP	RohanDELL	6771	*	*		12	1,428	12	1,428
BitTorrent.exe	17736	UDP	rohandell	6771	*	*					
BitTorrent.exe	17736	UDP	rohandell	6771	*	*					
BitTorrent.exe	17736	UDP	RohanDELL	ssdp	*	*				25	2,522
BitTorrent.exe	17736	UDP	rohandell	52625	*	*		1	98		
BitTorrent.exe	17736	UDP	rohandell	52626	*	*		1	98	9	2,892
BitTorrent.exe	17736	UDP	RohanDELL	52627	*	*		1	98		
BitTorrent.exe	17736	TCP	rohandell	1225	104.18.39.52	https	ESTABLISHED				
BitTorrent.exe	17736	TCP	rohandell	1227	37.19.5.139	6969	SYN_SENT				
BitTorrent.exe	17736	TCP	rohandell	1231	172.67.140.59	https	ESTABLISHED				
bittorrentie.exe	10860	TCP	rohandell	1030	https-69-164-46-1...	https	ESTABLISHED	17	2,358	30	18,670
bittorrentie.exe	10860	TCP	rohandell	1031	https-69-164-46-1...	https	ESTABLISHED	4	413	7	4,776
bittorrentie.exe	10860	TCP	rohandell	1032	server-54-192-66-...	https	ESTABLISHED	4	452	7	6,062
bittorrentie.exe	10860	TCP	rohandell	1033	ec2-23-21-139-15...	https	CLOSE_WAIT	5	2,678	9	6,153
bittorrentie.exe	10860	TCP	rohandell	activesync	ec2-23-21-139-15...	https	CLOSE_WAIT	5	2,762	9	6,153
bittorrentie.exe	10860	TCP	rohandell	1035	a23-218-43-174.d...	https	ESTABLISHED	3	3,212	5	4,424
bittorrentie.exe	10860	TCP	rohandell	1036	103.231.98.191	https	ESTABLISHED	3	3,952	13	14,024
bittorrentie.exe	10860	TCP	rohandell	1038	103.231.98.196	https	ESTABLISHED	2	324	7	6,440
bittorrentie.exe	10860	TCP	rohandell	1039	104.19.134.78	https	ESTABLISHED	4	409	5	2,785
bittorrentie.exe	10860	TCP	rohandell	1040	104.19.132.78	https	ESTABLISHED	4	414	5	2,787
bittorrentie.exe	10860	TCP	rohandell	1041	104.19.135.78	https	ESTABLISHED	4	408	5	2,785
bittorrentie.exe	10860	TCP	rohandell	1042	104.19.132.78	https	ESTABLISHED	4	411	5	2,787
bittorrentie.exe	11444	TCP	rohandell	1045	https-69-164-46-1...	https	ESTABLISHED	4	413	7	4,776
bittorrentie.exe	11444	TCP	rohandell	1046	ec2-23-21-139-15...	https	CLOSE_WAIT	8	5,293	12	6,936
bittorrentie.exe	11444	TCP	rohandell	1047	ec2-54-243-113-2...	https	ESTABLISHED	6	3,796	9	6,381
bittorrentie.exe	11444	TCP	rohandell	1048	https-69-164-46-1...	https	ESTABLISHED	14	2,245	29	19,705
bittorrentie.exe	11444	TCP	rohandell	1049	ec2-23-21-139-15...	https	CLOSE_WAIT	7	4,311	11	6,676
bittorrentie.exe	11444	TCP	rohandell	1050	a23-208-212-189....	https	ESTABLISHED	8	12,975	11	9,449
bittorrentie.exe	11444	TCP	rohandell	1052	a23-218-43-174.d...	https	CLOSE_WAIT	2	325	5	4,135
bittorrentie.exe	11444	TCP	rohandell	1055	a23-218-43-174.d...	https	CLOSE_WAIT	2	323	5	4,135
bittorrentie.exe	10860	TCP	rohandell	1091	par10s22-in-f226.1...	https	ESTABLISHED	10	1,927	16	4,502
bittorrentie.exe	10860	TCP	rohandell	1092	par10s22-in-f226.1...	https	ESTABLISHED	4	424	5	3,199
bittorrentie.exe	10860	TCP	rohandell	1093	par10s22-in-f226.1...	https	ESTABLISHED	8	3,796	30	26,952
bittorrentie.exe	11444	TCP	rohandell	1095	a23-208-212-189....	https	ESTABLISHED	3	2,573	6	4,572
bittorrentie.exe	11444	TCP	rohandell	1096	ec2-3-220-190-7.c...	https	CLOSE_WAIT	3	1,070	6	4,138
bittorrentie.exe	10860	TCP	rohandell	1097	zrh04s08-in-f6.1e1...	https	ESTABLISHED	6	797	66	67,343
bittorrentie.exe	10860	TCP	rohandell	1098	muc11s15-in-f2.1e...	https	ESTABLISHED	6	822	8	3,907

Endpoints: 186 Established: 72 Listening: 46 Time Wait: 2 Close Wait: 15

TCPView - Sysinternals: www.sysinternals.com

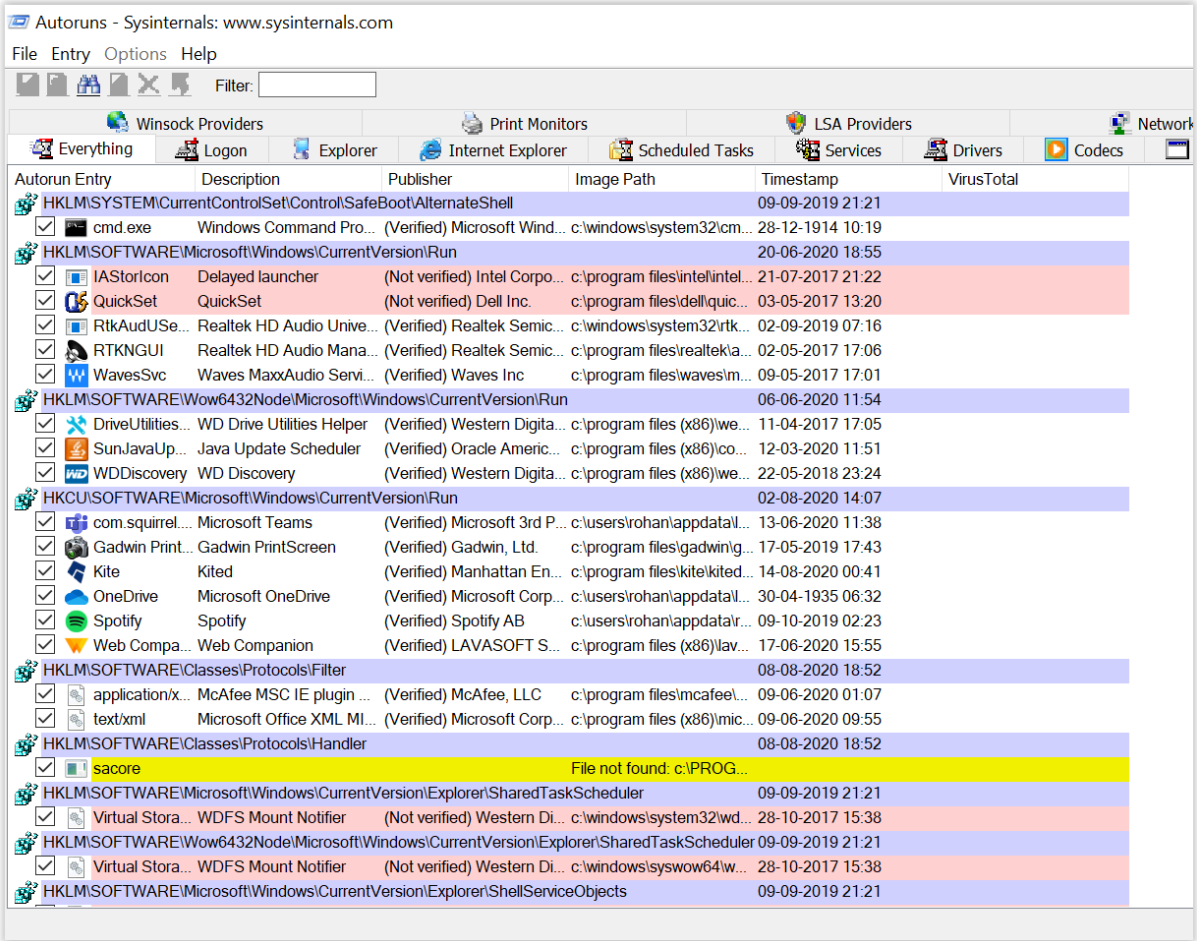
File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc...	0	TCP	rohandell	52401	161.69.165.70	https	TIME_WAIT				
[System Proc...	0	TCP	rohandell	52402	104.208.16.0	https	TIME_WAIT				
[System Proc...	0	TCP	rohandell	52422	192.168.1.2	49153	TIME_WAIT				
[System Proc...	0	TCP	rohandell	52403	40.90.22.186	https	TIME_WAIT				
[System Proc...	0	TCP	rohandell	52404	40.90.22.186	https	TIME_WAIT				
chrome.exe	12628	TCP	rohandell	51917	34.231.108.170	https	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	51940	52.31.9.183	https	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	51955	66.102.1.188	5228	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	52259	111.221.29.254	https	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	52372	111.221.29.254	https	ESTABLISHED	2	7,327	2	872
chrome.exe	12628	TCP	rohandell	52377	152.199.19.160	https	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	52381	151.101.140.133	https	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	52382	151.101.140.133	https	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	52383	40.81.31.55	https	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	52384	151.101.142.217	https	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	52385	204.79.197.200	https	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	52389	51.11.30.100	https	ESTABLISHED				
chrome.exe	12628	TCP	rohandell	52419	13.35.180.75	https	ESTABLISHED	5	1,012	3	560
chrome.exe	12628	TCP	rohandell	52420	34.251.2.121	https	ESTABLISHED	1	517	1	1,452
chrome.exe	11708	UDP	RohanDELL	5353	*	*					
chrome.exe	11708	UDP	RohanDELL	5353	*	*					
chrome.exe	12628	UDP	RohanDELL	62903	*	*		2	831	3	118
chrome.exe	11708	UDP	RohanDELL	5353	*	*					
chrome.exe	11708	UDP	RohanDELL	5353	*	*					
chrome.exe	11708	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	11708	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	12628	UDP	RohanDELL	50299	*	*		5	1,965	6	2,479
dasHost.exe	3676	UDP	RohanDELL	ws-discovery	*	*					
dasHost.exe	3676	UDP	RohanDELL	ws-discovery	*	*					
dasHost.exe	3676	UDP	RohanDELL	55767	*	*					
dasHost.exe	3676	UDPV6	[0:0:0:0:0:0:0:0]	3702	*	*					
dasHost.exe	3676	UDPV6	[0:0:0:0:0:0:0:0]	3702	*	*					
dasHost.exe	3676	UDPV6	[0:0:0:0:0:0:0:0]	55768	*	*					
explorer.exe	9360	TCP	RohanDELL	52391	localhost	50039	ESTABLISHED				
jhi_service.exe	13980	TCPV6	[0:0:0:0:0:0:0:1]	49783	[0:0:0:0:0:0:0:0]	0	LISTENING				
kdd	13352	TCP	RohanDELL	49988	RohanDELL	0	LISTENING				
kdd	13352	TCP	RohanDELL	49988	localhost	50041	ESTABLISHED				
kited.exe	2788	TCP	RohanDELL	46624	RohanDELL	0	LISTENING				
kited.exe	2788	TCP	rohandell	51919	216.58.208.238	http	ESTABLISHED	1	112	1	83
kited.exe	2788	TCP	rohandell	52276	34.105.42.221	https	ESTABLISHED				
lsass.exe	956	TCP	RohanDELL	49664	RohanDELL	0	LISTENING				
lsass.exe	956	TCPV6	[0:0:0:0:0:0:0:0]	49664	[0:0:0:0:0:0:0:0]	0	LISTENING				
MMSSHOST...	5996	TCP	RohanDELL	6646	RohanDELL	0	LISTENING				

Endpoints: 122 | Established: 36 | Listening: 40 | Time Wait: 5 | Close Wait: 0

Tool 2: Autoruns for Windows v13.98

This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer and media players.



In Internet Explorer:

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

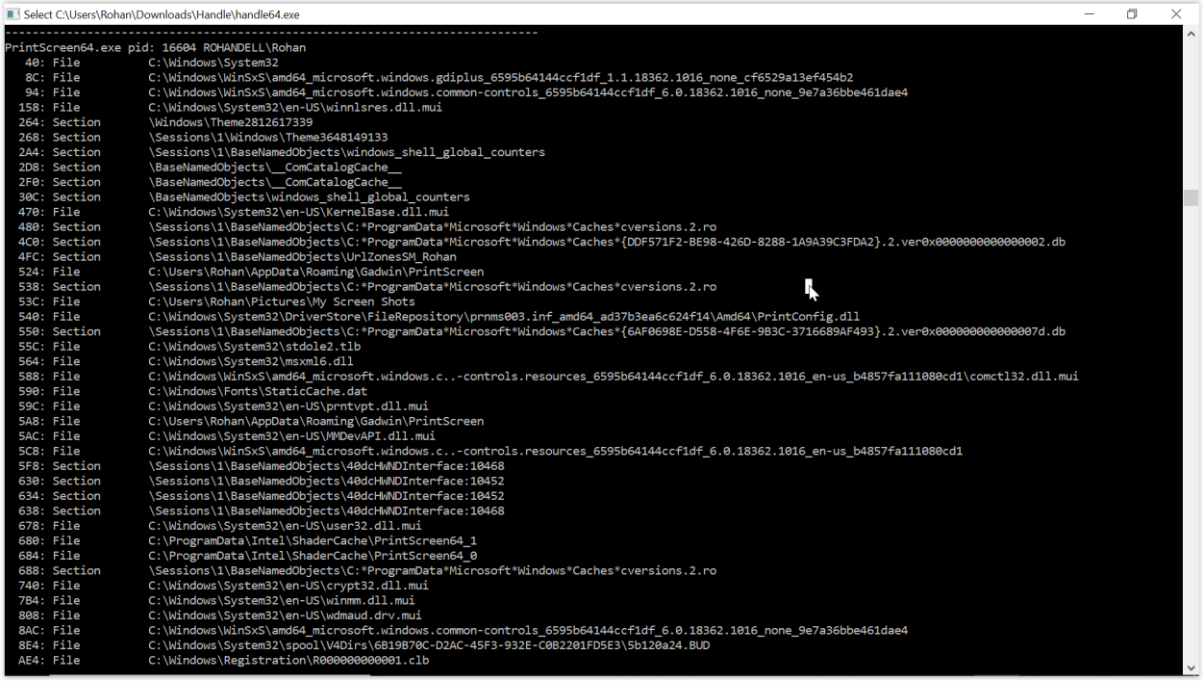
Winsock Providers | Print Monitors | LSA Providers | Netv

Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers | Codecs

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				30-07-2020 06:32	
IEToEdge B...	IEToEdge BHO	(Verified) Microsoft Corp...	c:\program files (x86)\mic...	11-08-2020 05:40	
McAfee We...	McAfee WebAdvisor	(Verified) McAfee, LLC	c:\program files\mcafee\...	05-08-2020 17:32	
Skype for B...	Skype for Business	(Verified) Microsoft Corp...	c:\program files (x86)\mic...	08-12-2019 05:33	
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				30-07-2020 06:32	
IEToEdge B...	IEToEdge BHO	(Verified) Microsoft Corp...	c:\program files (x86)\mic...	11-08-2020 05:40	
Java(tm) Plu...	Java(TM) Platform SE bi...	(Verified) Oracle Americ...	c:\program files (x86)\jav...	12-03-2020 10:48	
Java(tm) Plu...	Java(TM) Platform SE bi...	(Verified) Oracle Americ...	c:\program files (x86)\jav...	12-03-2020 10:51	
McAfee We...	McAfee WebAdvisor	(Verified) McAfee, LLC	c:\program files\mcafee\...	05-08-2020 17:17	
HKLM\Software\Microsoft\Internet Explorer\Extensions				01-06-2020 23:07	
Lync Click to...	Skype for Business	(Verified) Microsoft Corp...	c:\program files (x86)\mic...	08-12-2019 05:33	
McAfee We...	McAfee WebAdvisor	(Verified) McAfee, LLC	c:\program files\mcafee\...	05-08-2020 17:32	
OneNote Lin...	Microsoft OneNote Inter...	(Verified) Microsoft Corp...	c:\program files (x86)\mic...	02-07-2020 21:36	
Se&nd to O...	Microsoft OneNote Inter...	(Verified) Microsoft Corp...	c:\program files (x86)\mic...	29-06-2020 14:58	
HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Extensions				01-06-2020 23:07	
McAfee We...	McAfee WebAdvisor	(Verified) McAfee, LLC	c:\program files\mcafee\...	05-08-2020 17:17	
OneNote Lin...	Microsoft OneNote Inter...	(Verified) Microsoft Corp...	c:\program files (x86)\mic...	11-07-2020 14:25	
Se&nd to O...	Microsoft OneNote Inter...	(Verified) Microsoft Corp...	c:\program files (x86)\mic...	11-07-2020 14:25	

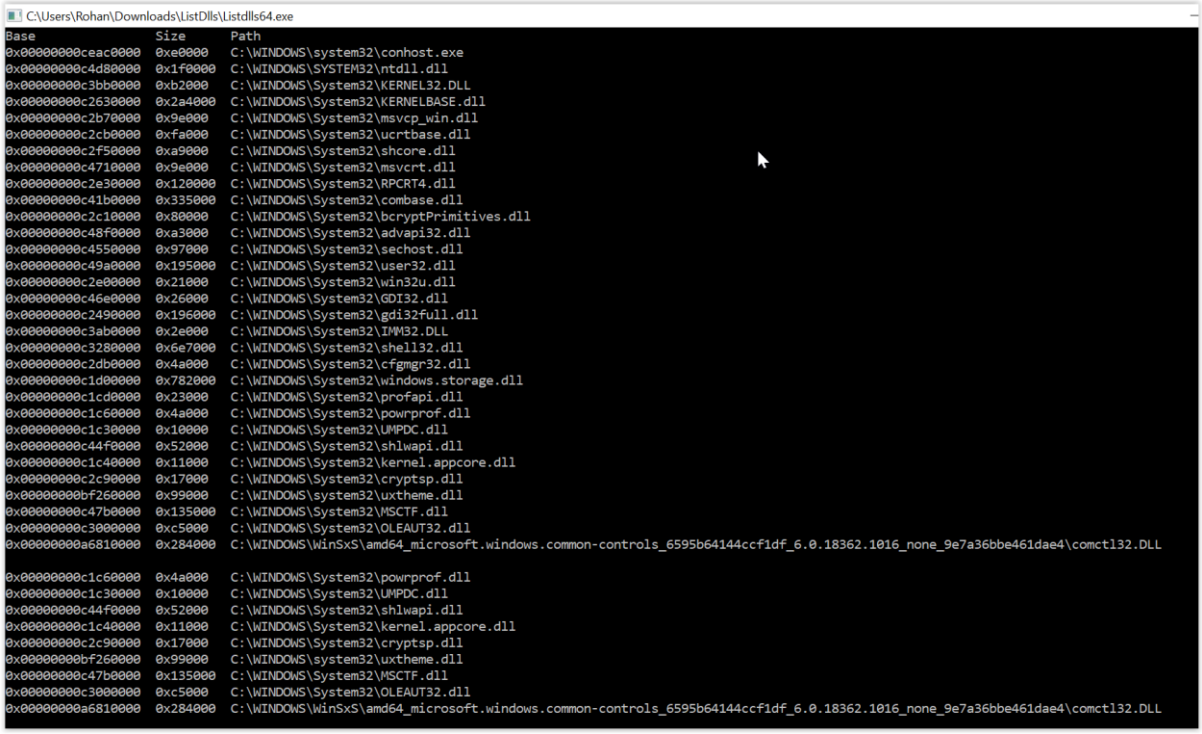
Tool 3: Handle for Windows v13.98

Ever wondered which program has a particular file or directory open? Now you can find out. *Handle* is a utility that displays information about open handles for any process in the system. You can use it to see the programs that have a file open, or to see the object types and names of all the handles of a program.



Tool 4: ListDLLs v3.2

ListDLLs is a utility that reports the DLLs loaded into processes. You can use it to list all DLLs loaded into all processes, into a specific process, or to list the processes that have a particular DLL loaded. ListDLLs can also display full version information for DLLs, including their digital signature, and can be used to scan processes for unsigned DLLs.

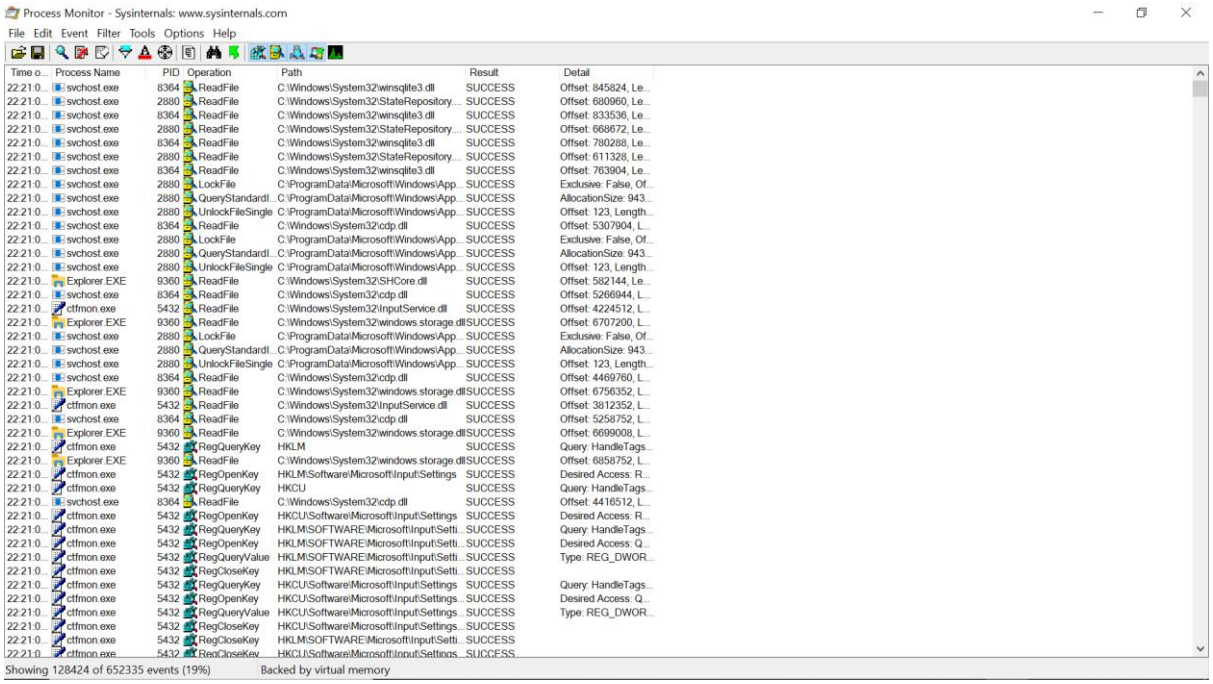


```
C:\Users\Rohan\Downloads\ListDlls\Listdlls64.exe
Base               Size      Path
0x00000000ceac0000  0xe0000   C:\WINDOWS\system32\conhost.exe
0x00000000c4d80000  0x1f0000  C:\WINDOWS\SYSTEM32\ntdll.dll
0x00000000c3bb0000  0xb2000   C:\WINDOWS\System32\KERNEL32.DLL
0x00000000c2630000  0x2a4000  C:\WINDOWS\System32\KERNELBASE.dll
0x00000000c2b70000  0x9e000   C:\WINDOWS\System32\msvcp_win.dll
0x00000000c2cb0000  0xfa000   C:\WINDOWS\System32\ucrtbase.dll
0x00000000c2f50000  0xa9000   C:\WINDOWS\System32\shcore.dll
0x00000000c4710000  0x9e000   C:\WINDOWS\System32\msvcrt.dll
0x00000000c2e30000  0x120000  C:\WINDOWS\System32\RPCRT4.dll
0x00000000c41b0000  0x335000  C:\WINDOWS\System32\combase.dll
0x00000000c2c10000  0x80000   C:\WINDOWS\System32\bcryptPrimitives.dll
0x00000000c48f0000  0xa3000   C:\WINDOWS\System32\advapi32.dll
0x00000000c4550000  0x97000   C:\WINDOWS\System32\sechost.dll
0x00000000c49a0000  0x195000  C:\WINDOWS\System32\user32.dll
0x00000000c2e00000  0x21000   C:\WINDOWS\System32\win32u.dll
0x00000000c46e0000  0x26000   C:\WINDOWS\System32\GDI32.dll
0x00000000c2490000  0x196000  C:\WINDOWS\System32\gdi32full.dll
0x00000000c3ab0000  0x2e000   C:\WINDOWS\System32\IMM32.DLL
0x00000000c3280000  0x6e7000  C:\WINDOWS\System32\shell32.dll
0x00000000c2db0000  0x4a000   C:\WINDOWS\System32\cfgmgr32.dll
0x00000000c1d00000  0x782000  C:\WINDOWS\System32\windows.storage.dll
0x00000000c1cd0000  0x23000   C:\WINDOWS\System32\profapi.dll
0x00000000c1c60000  0x4a000   C:\WINDOWS\System32\powrprof.dll
0x00000000c1c30000  0x10000   C:\WINDOWS\System32\UMPDC.dll
0x00000000c44f0000  0x52000   C:\WINDOWS\System32\shlwapi.dll
0x00000000c1c40000  0x11000   C:\WINDOWS\System32\kernel.appcore.dll
0x00000000c2c90000  0x17000   C:\WINDOWS\System32\cryptsp.dll
0x00000000bf260000  0x99000   C:\WINDOWS\system32\uxtheme.dll
0x00000000c47b0000  0x135000  C:\WINDOWS\System32\MSCTF.dll
0x00000000c3000000  0xc5000   C:\WINDOWS\System32\OLEAUT32.dll
0x00000000a6810000  0x284000  C:\WINDOWS\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.18362.1016_none_9e7a36bbe461dae4\comctl32.DLL

0x00000000c1c60000  0x4a000   C:\WINDOWS\System32\powrprof.dll
0x00000000c1c30000  0x10000   C:\WINDOWS\System32\UMPDC.dll
0x00000000c44f0000  0x52000   C:\WINDOWS\System32\shlwapi.dll
0x00000000c1c40000  0x11000   C:\WINDOWS\System32\kernel.appcore.dll
0x00000000c2c90000  0x17000   C:\WINDOWS\System32\cryptsp.dll
0x00000000bf260000  0x99000   C:\WINDOWS\system32\uxtheme.dll
0x00000000c47b0000  0x135000  C:\WINDOWS\System32\MSCTF.dll
0x00000000c3000000  0xc5000   C:\WINDOWS\System32\OLEAUT32.dll
0x00000000a6810000  0x284000  C:\WINDOWS\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.18362.1016_none_9e7a36bbe461dae4\comctl32.DLL
```

Tool 4: Process Monitor v3.53

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.



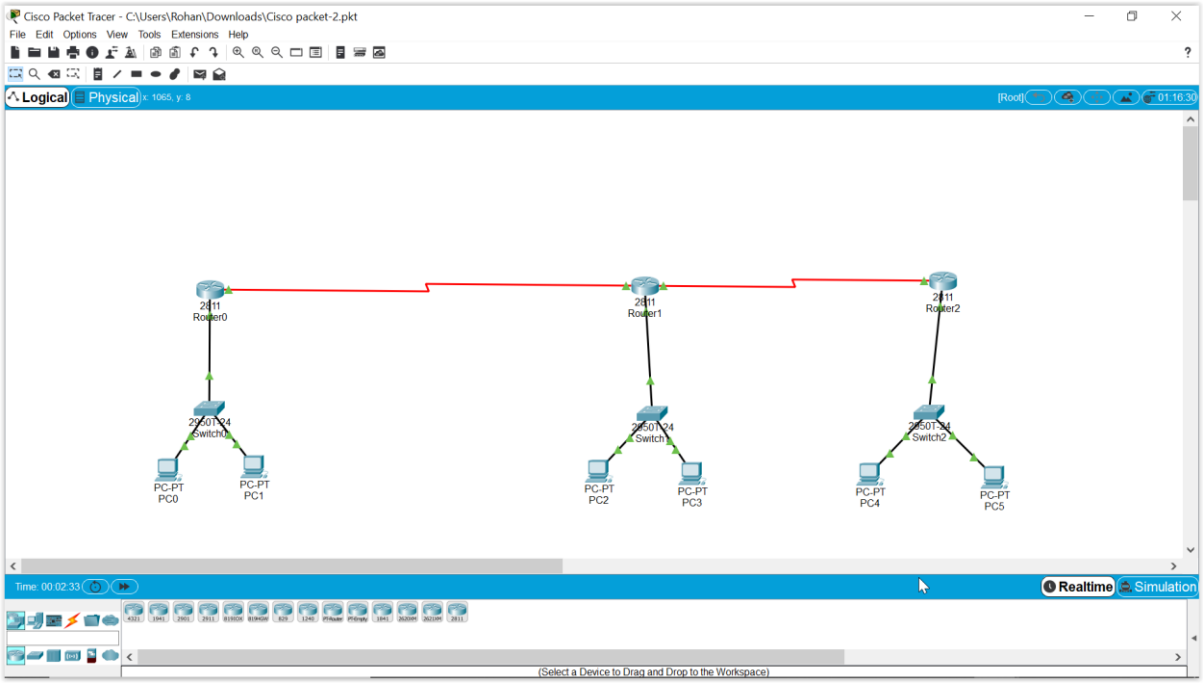
Exercise 3:

Experiments in Cisco Packet Tracer software.

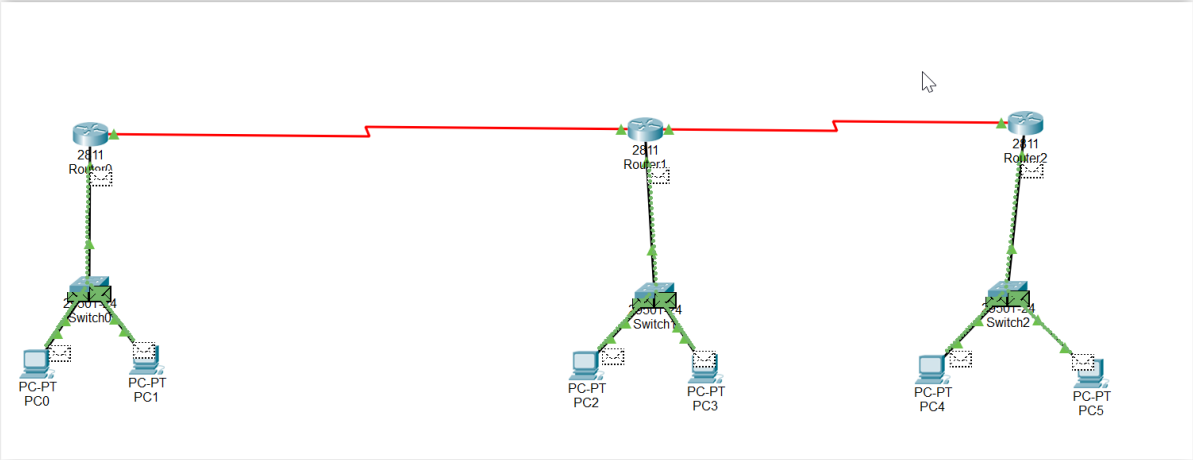
Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

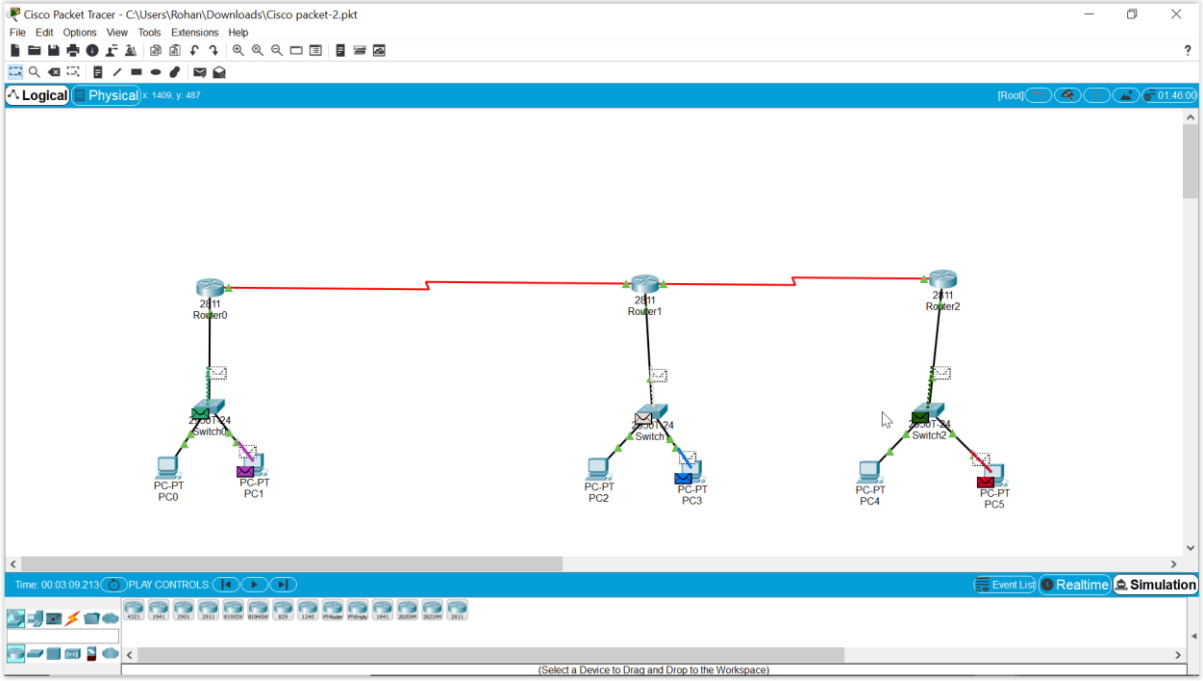
Aim:

1) To get this network topology:



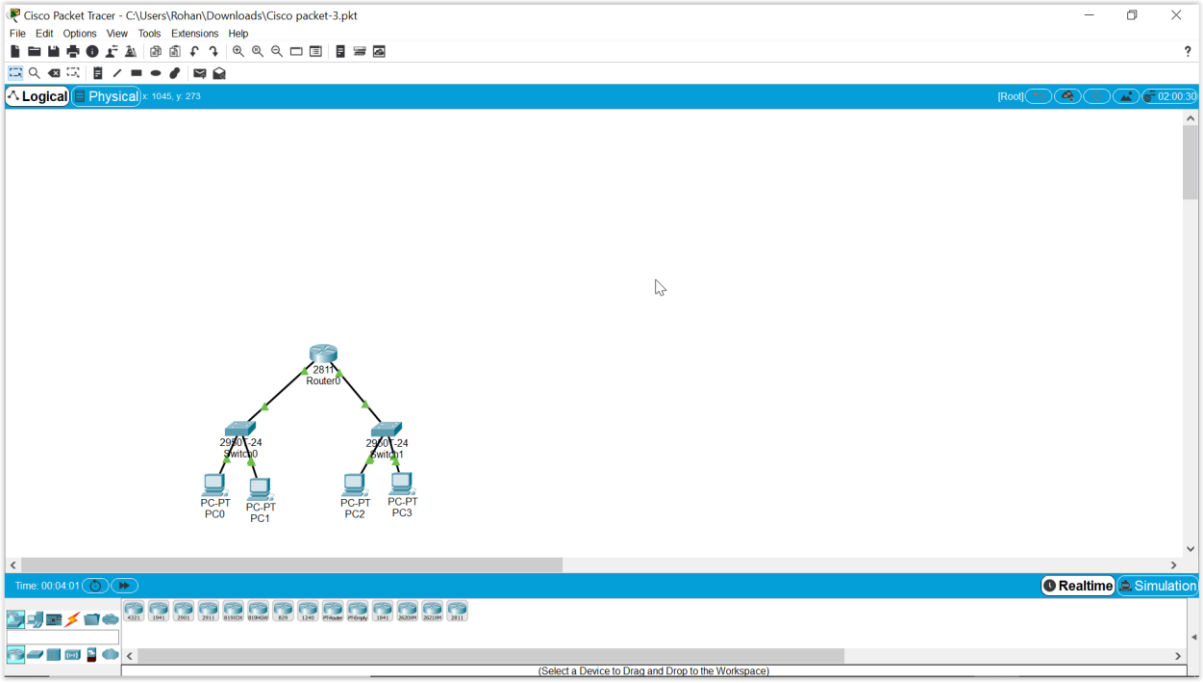
Simulation:


2811
Router0
2811
Router1
2811
Router2
2960-24
Switch0
2960-24
Switch1
2960-24
Switch2
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5

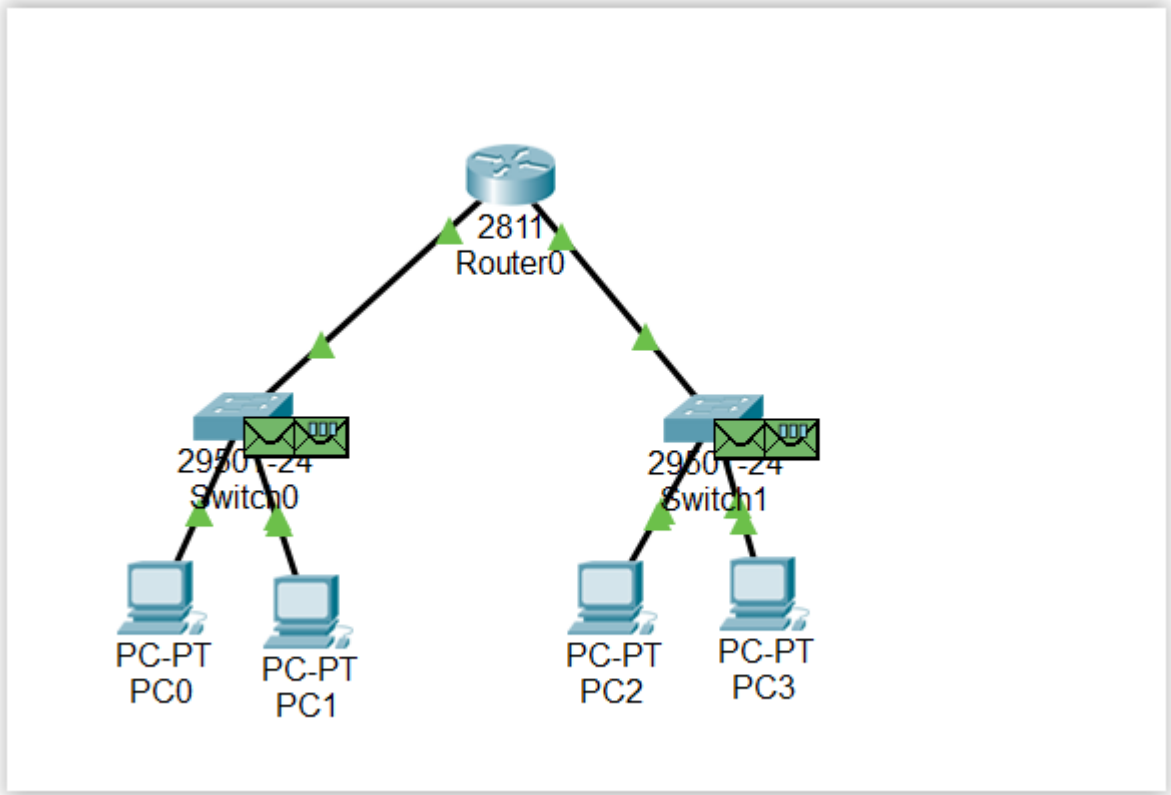

Cisco Packet Tracer - C:\Users\Rohan\Downloads\Cisco packet-2.pkt
File Edit Options View Tools Extensions Help
Logical
Physical
Time: 00:03:09.213
PLAY CONTROLS:
Event List
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)

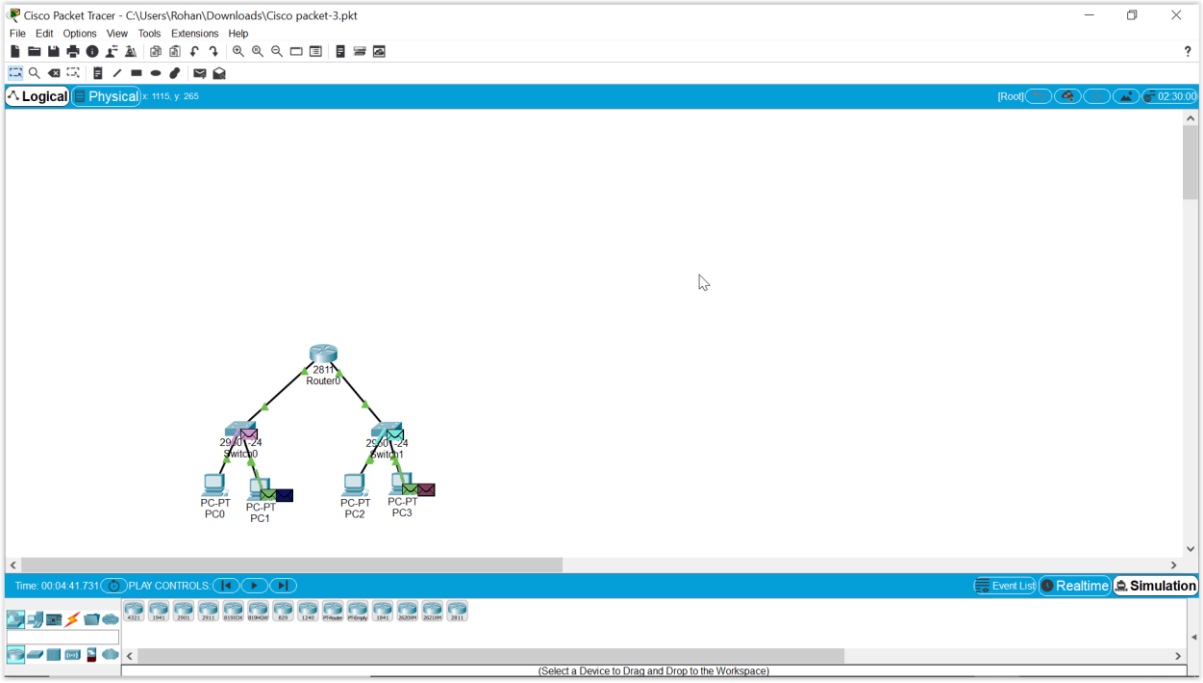
Aim:

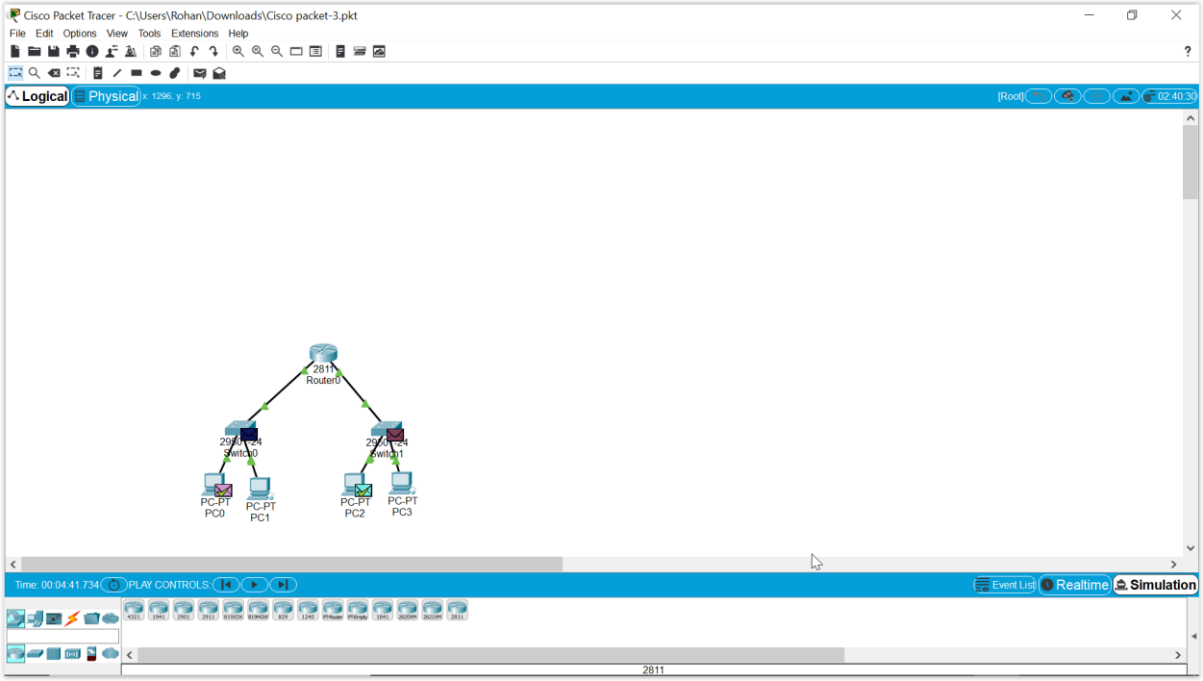
2) To get this network topology:



On Simulation:






Cisco Packet Tracer - C:\Users\Rohan\Downloads\Cisco packet-3.pkt
File Edit Options View Tools Extensions Help
Logical
Physical
x: 1296, y: 715
[Root]
02:40:30
2811
Router0
2960-24
Switch0
2960-24
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
Time: 00:04:41.734
PLAY CONTROLS:
Event List
Realtime
Simulation
2811