



VIT[®]

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Analysis and Audit

Course Code: CSE3501

Slot: L47-48

Faculty: Dr. Anil Kumar K

Assessment: 2

18BCI0247

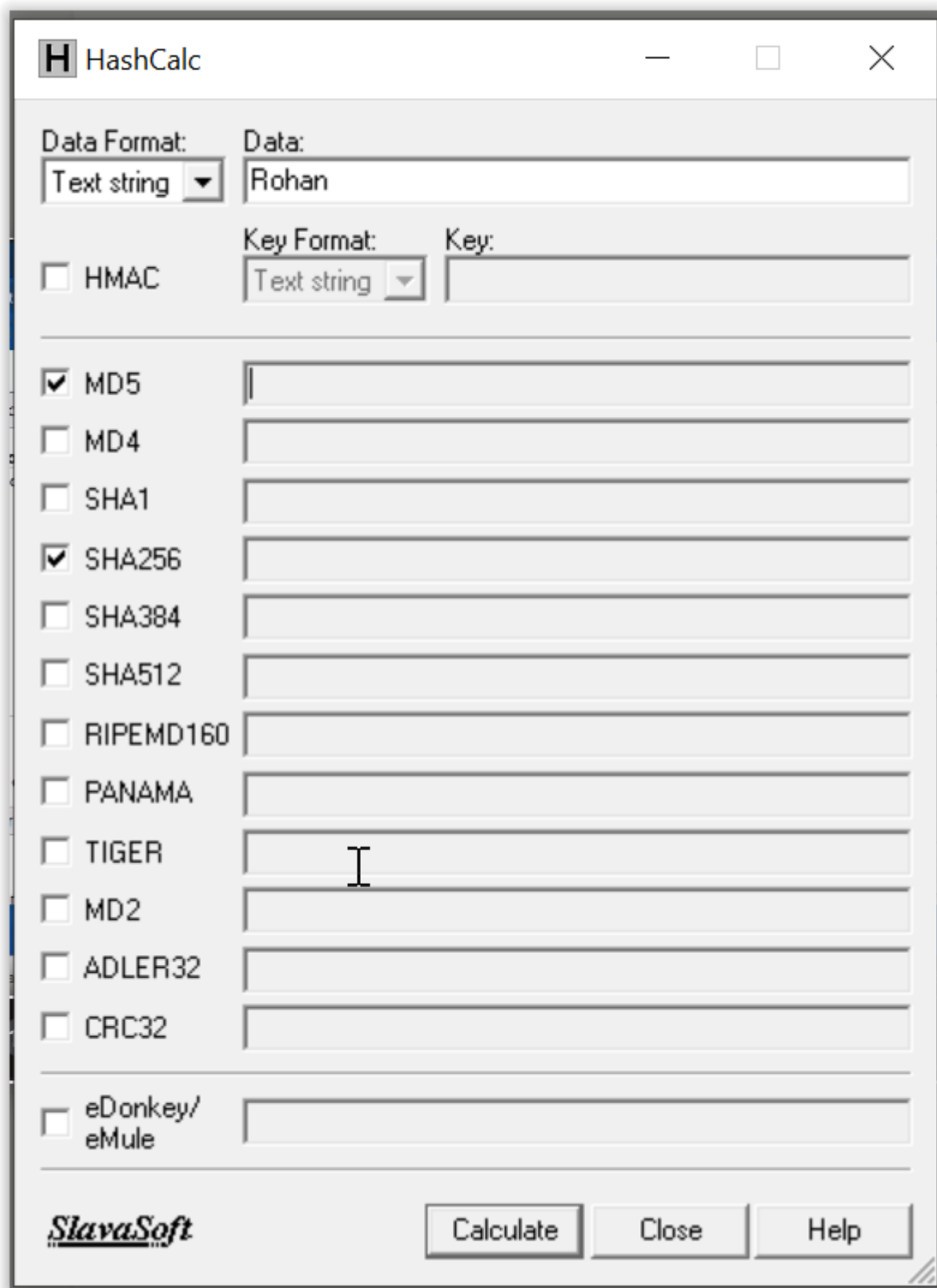
Rohan Allen

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".



The image shows the HashCalc application window. The title bar reads "HashCalc" with a standard Windows window icon. The main interface is divided into several sections. At the top, there is a "Data Format:" dropdown menu set to "Text string" and a "Data:" text box containing the text "Rohan". Below this, there is a section for HMAC with an unchecked checkbox and a "Key Format:" dropdown set to "Text string" next to an empty "Key:" text box. A horizontal line separates this from a list of hash algorithms. The list includes MD5 (checked), MD4, SHA1, SHA256 (checked), SHA384, SHA512, RIPEMD160, PANAMA, TIGER, MD2, ADLER32, and CRC32. Each algorithm has a corresponding empty text box for its output. The TIGER output box has a cursor. At the bottom, there is a section for "eDonkey/eMule" with an unchecked checkbox and an empty text box. The footer contains the "SlavaSoft" logo and three buttons: "Calculate", "Close", and "Help".

Algorithm	Output
<input checked="" type="checkbox"/> MD5	
<input type="checkbox"/> MD4	
<input type="checkbox"/> SHA1	
<input checked="" type="checkbox"/> SHA256	
<input type="checkbox"/> SHA384	
<input type="checkbox"/> SHA512	
<input type="checkbox"/> RIPEMD160	
<input type="checkbox"/> PANAMA	
<input type="checkbox"/> TIGER	
<input type="checkbox"/> MD2	
<input type="checkbox"/> ADLER32	
<input type="checkbox"/> CRC32	
<hr/>	
<input type="checkbox"/> eDonkey/eMule	

SlavaSoft

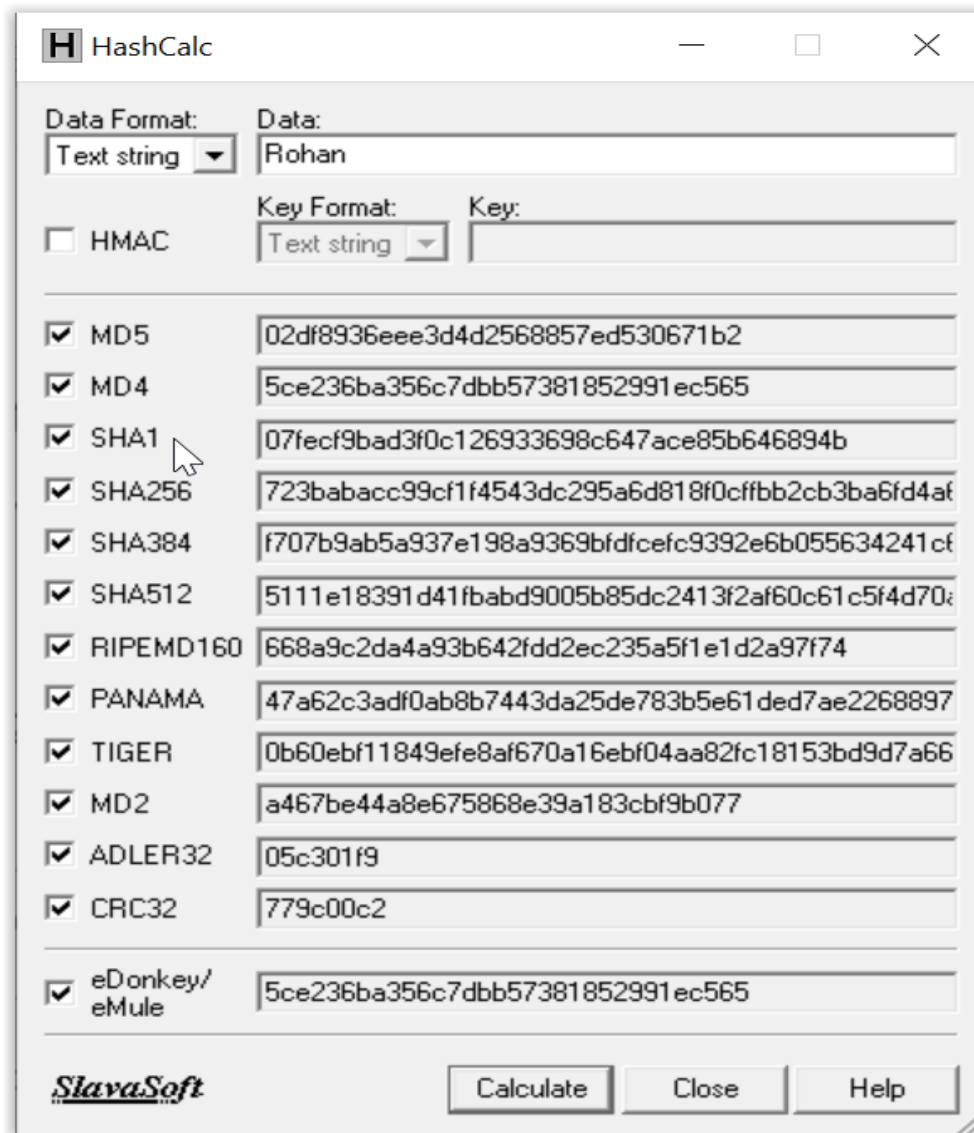
Calculate Close Help

Hash value using MD5 and SHA256 hash algorithm.

The screenshot shows the HashCalc application window. The 'Data Format' is set to 'Text string' and the 'Data' field contains 'Rohan'. The 'Key Format' is also set to 'Text string' and the 'Key' field is empty. The 'HMAC' checkbox is unchecked. The 'MD5' and 'SHA256' checkboxes are checked, and their respective hash values are displayed in the output fields. The 'SHA256' field is highlighted by a mouse cursor. The 'eDonkey/eMule' checkbox is unchecked. The 'SlavaSoft' logo is in the bottom left, and 'Calculate', 'Close', and 'Help' buttons are in the bottom right.

Algorithm	Hash Value
<input checked="" type="checkbox"/> MD5	02df8936eee3d4d2568857ed530671b2
<input type="checkbox"/> MD4	
<input type="checkbox"/> SHA1	
<input checked="" type="checkbox"/> SHA256	723babacc99cf1f4543dc295a6d818f0cffbb2cb3ba6fd4af
<input type="checkbox"/> SHA384	
<input type="checkbox"/> SHA512	
<input type="checkbox"/> RIPEMD160	
<input type="checkbox"/> PANAMA	
<input type="checkbox"/> TIGER	
<input type="checkbox"/> MD2	
<input type="checkbox"/> ADLER32	
<input type="checkbox"/> CRC32	
<input type="checkbox"/> eDonkey/eMule	

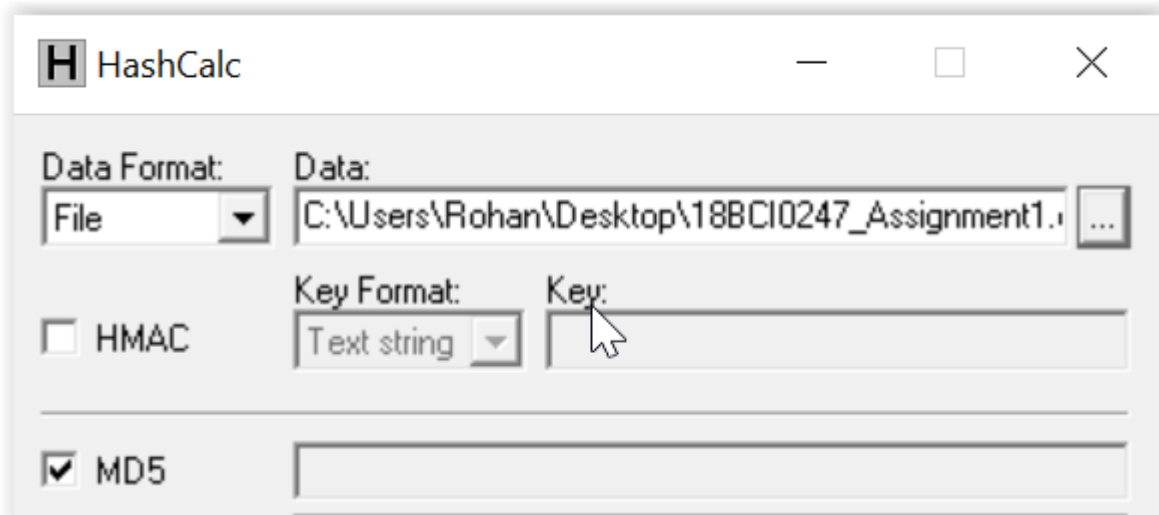
Hash value using all the hash functions available.



The screenshot shows the HashCalc application window. The 'Data' field contains 'Rohan'. The 'Data Format' is set to 'Text string'. The 'Key Format' is also set to 'Text string', and the 'Key' field is empty. The 'HMAC' checkbox is unchecked. A list of hash functions is shown, each with a checked checkbox and a corresponding hash value. The functions include MD5, MD4, SHA1, SHA256, SHA384, SHA512, RIPEMD160, PANAMA, TIGER, MD2, ADLER32, CRC32, and eDonkey/eMule. The 'SlavaSoft' logo is in the bottom left, and 'Calculate', 'Close', and 'Help' buttons are in the bottom right.

Function	Hash Value
<input checked="" type="checkbox"/> MD5	02df8936eee3d4d2568857ed530671b2
<input checked="" type="checkbox"/> MD4	5ce236ba356c7dbb57381852991ec565
<input checked="" type="checkbox"/> SHA1	07fecf9bad3f0c126933698c647ace85b646894b
<input checked="" type="checkbox"/> SHA256	723babacc99cf1f4543dc295a6d818f0cffbb2cb3ba6fd4af
<input checked="" type="checkbox"/> SHA384	f707b9ab5a937e198a9369bdfcfc9392e6b055634241cf
<input checked="" type="checkbox"/> SHA512	5111e18391d41fbabd9005b85dc2413f2af60c61c5f4d70i
<input checked="" type="checkbox"/> RIPEMD160	668a9c2da4a93b642fdd2ec235a5f1e1d2a97f74
<input checked="" type="checkbox"/> PANAMA	47a62c3adf0ab8b7443da25de783b5e61ded7ae2268897
<input checked="" type="checkbox"/> TIGER	0b60ebf11849efe8af670a16ebf04aa82fc18153bd9d7a66
<input checked="" type="checkbox"/> MD2	a467be44a8e675868e39a183cbf9b077
<input checked="" type="checkbox"/> ADLER32	05c301f9
<input checked="" type="checkbox"/> CRC32	779c00c2
<input checked="" type="checkbox"/> eDonkey/ eMule	5ce236ba356c7dbb57381852991ec565

Selecting a file to hash



Hash values of the file.

The screenshot shows the HashCalc application window. At the top, the title bar reads 'HashCalc'. Below the title bar, there are two main sections. The first section is for 'Data Format' and 'Data'. 'Data Format' is set to 'File' (indicated by a dropdown arrow). 'Data' is a text field containing the path 'C:\Users\Rohan\Desktop\18BCI0247_Assignment1.' followed by a browse button '...'. The second section is for 'Key Format' and 'Key'. 'Key Format' is set to 'Text string' (indicated by a dropdown arrow). The 'Key' field is empty. Below these sections, there is a list of hash algorithms, each with a checkbox and a corresponding text field for the hash value. The algorithms and their values are: MD5 (checked), MD4 (checked), SHA1 (checked), SHA256 (checked), SHA384 (checked), SHA512 (checked), RIPEMD160 (checked), PANAMA (checked), TIGER (checked), MD2 (checked), ADLER32 (checked), CRC32 (checked), and eDonkey/eMule (checked). At the bottom of the window, there is a logo for 'SlavaSoft' and three buttons: 'Calculate', 'Close', and 'Help'.

Algorithm	Hash Value
<input checked="" type="checkbox"/> MD5	26e157dab19fd7c9a496f4dbad2bc1bd
<input checked="" type="checkbox"/> MD4	2a76c36a35a41e705ad0bf415b897c8f
<input checked="" type="checkbox"/> SHA1	5d57318f761dd5a725b8e6955290c54e46801528
<input checked="" type="checkbox"/> SHA256	ff1f0d9837bc38ac7d1a160f997b40a74c6b9b26aa7bf5ff3
<input checked="" type="checkbox"/> SHA384	42bf145652f0c30780bd208ca9a4ccdebf36c8eca92cbb7
<input checked="" type="checkbox"/> SHA512	5d450bf291e06f180589a99d40a3c87b60a8d16d92b88d
<input checked="" type="checkbox"/> RIPEMD160	d7b22d9cd31804058d245f559f5ee3f7539b768d
<input checked="" type="checkbox"/> PANAMA	d783f393e6b85c3cd5a30d9c789dcb8f15f6f5e6a9663cf0
<input checked="" type="checkbox"/> TIGER	64c7b041ae4210cfa0cde24bbc95163e186c892e969800
<input checked="" type="checkbox"/> MD2	cd1f5811f17269fd53108e7414f5c250
<input checked="" type="checkbox"/> ADLER32	5be2aa67
<input checked="" type="checkbox"/> CRC32	12e331ba
<input checked="" type="checkbox"/> eDonkey/ eMule	2a76c36a35a41e705ad0bf415b897c8f

SlavaSoft

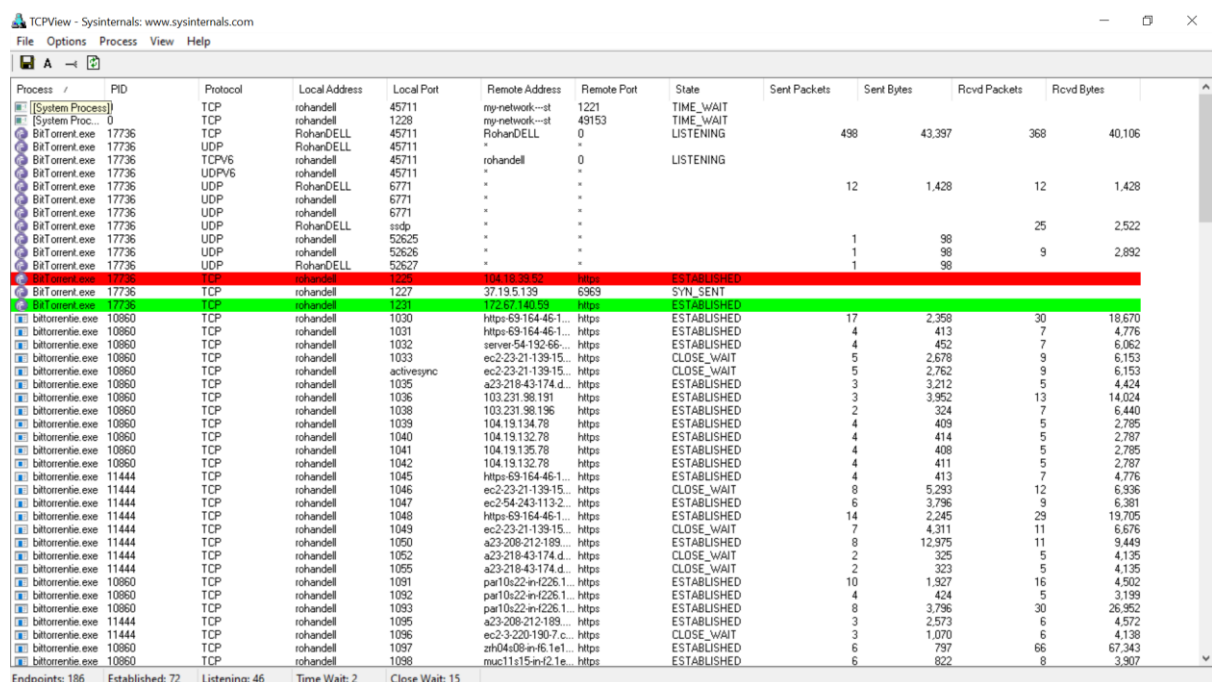
Calculate Close Help

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



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	52625	*	*		1	98	25	2,522
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	104.18.38.52	https	ESTABLISHED				
BitTorrent.exe	17736	TCP	rohandell	1227	37.19.5.139	6969	SYN_SENT				
BitTorrent.exe	17736	TCP	rohandell	1231	172.67.140.95	https	ESTABLISHED				
bit torrent.exe	10860	TCP	rohandell	1030	https-69-164-46-1...	https	ESTABLISHED	17	2,358	30	18,670
bit torrent.exe	10860	TCP	rohandell	1031	https-69-164-46-1...	https	ESTABLISHED	4	413	7	4,776
bit torrent.exe	10860	TCP	rohandell	1032	server-54-192-66...	https	ESTABLISHED	4	452	7	6,062
bit torrent.exe	10860	TCP	rohandell	1033	ec2-23-21-139-15...	https	CLOSE_WAIT	5	2,678	9	6,153
bit torrent.exe	10860	TCP	rohandell	1035	ec2-23-21-139-15...	https	CLOSE_WAIT	5	2,762	9	6,153
bit torrent.exe	10860	TCP	rohandell	1036	a23-218-43-174.d...	https	ESTABLISHED	3	3,212	5	4,424
bit torrent.exe	10860	TCP	rohandell	1036	103.231.98.191	https	ESTABLISHED	3	3,952	13	14,024
bit torrent.exe	10860	TCP	rohandell	1038	103.231.98.196	https	ESTABLISHED	2	324	7	6,440
bit torrent.exe	10860	TCP	rohandell	1039	104.19.134.78	https	ESTABLISHED	4	409	5	2,785
bit torrent.exe	10860	TCP	rohandell	1040	104.19.132.78	https	ESTABLISHED	4	414	5	2,787
bit torrent.exe	10860	TCP	rohandell	1041	104.19.135.78	https	ESTABLISHED	4	408	5	2,785
bit torrent.exe	10860	TCP	rohandell	1042	104.19.132.78	https	ESTABLISHED	4	411	5	2,787
bit torrent.exe	11444	TCP	rohandell	1045	https-69-164-46-1...	https	ESTABLISHED	4	413	7	4,776
bit torrent.exe	11444	TCP	rohandell	1046	ec2-23-21-139-15...	https	CLOSE_WAIT	8	5,293	12	6,936
bit torrent.exe	11444	TCP	rohandell	1047	ec2-54-243-113-2...	https	ESTABLISHED	6	3,796	9	6,381
bit torrent.exe	11444	TCP	rohandell	1048	https-69-164-46-1...	https	ESTABLISHED	14	2,245	29	19,705
bit torrent.exe	11444	TCP	rohandell	1049	ec2-23-21-139-15...	https	CLOSE_WAIT	7	4,311	11	6,676
bit torrent.exe	11444	TCP	rohandell	1050	a23-208-212-189...	https	ESTABLISHED	8	12,975	11	9,449
bit torrent.exe	11444	TCP	rohandell	1052	a23-218-43-174.d...	https	CLOSE_WAIT	2	325	5	4,135
bit torrent.exe	11444	TCP	rohandell	1055	a23-218-43-174.d...	https	CLOSE_WAIT	2	323	5	4,135
bit torrent.exe	10860	TCP	rohandell	1091	par10s22-m4226.1...	https	ESTABLISHED	10	1,927	16	4,502
bit torrent.exe	10860	TCP	rohandell	1092	par10s22-m4226.1...	https	ESTABLISHED	4	424	5	3,199
bit torrent.exe	10860	TCP	rohandell	1093	par10s22-m4226.1...	https	ESTABLISHED	8	3,796	30	26,952
bit torrent.exe	11444	TCP	rohandell	1095	a23-208-212-189...	https	ESTABLISHED	3	2,573	6	4,572
bit torrent.exe	11444	TCP	rohandell	1096	ec2-3-220-190-7.c...	https	CLOSE_WAIT	3	1,070	6	4,138
bit torrent.exe	10860	TCP	rohandell	1097	zrh04s06-m46.1e1...	https	ESTABLISHED	6	797	66	67,343
bit torrent.exe	10860	TCP	rohandell	1098	muc11s15-m2.1e...	https	ESTABLISHED	6	822	8	3,907

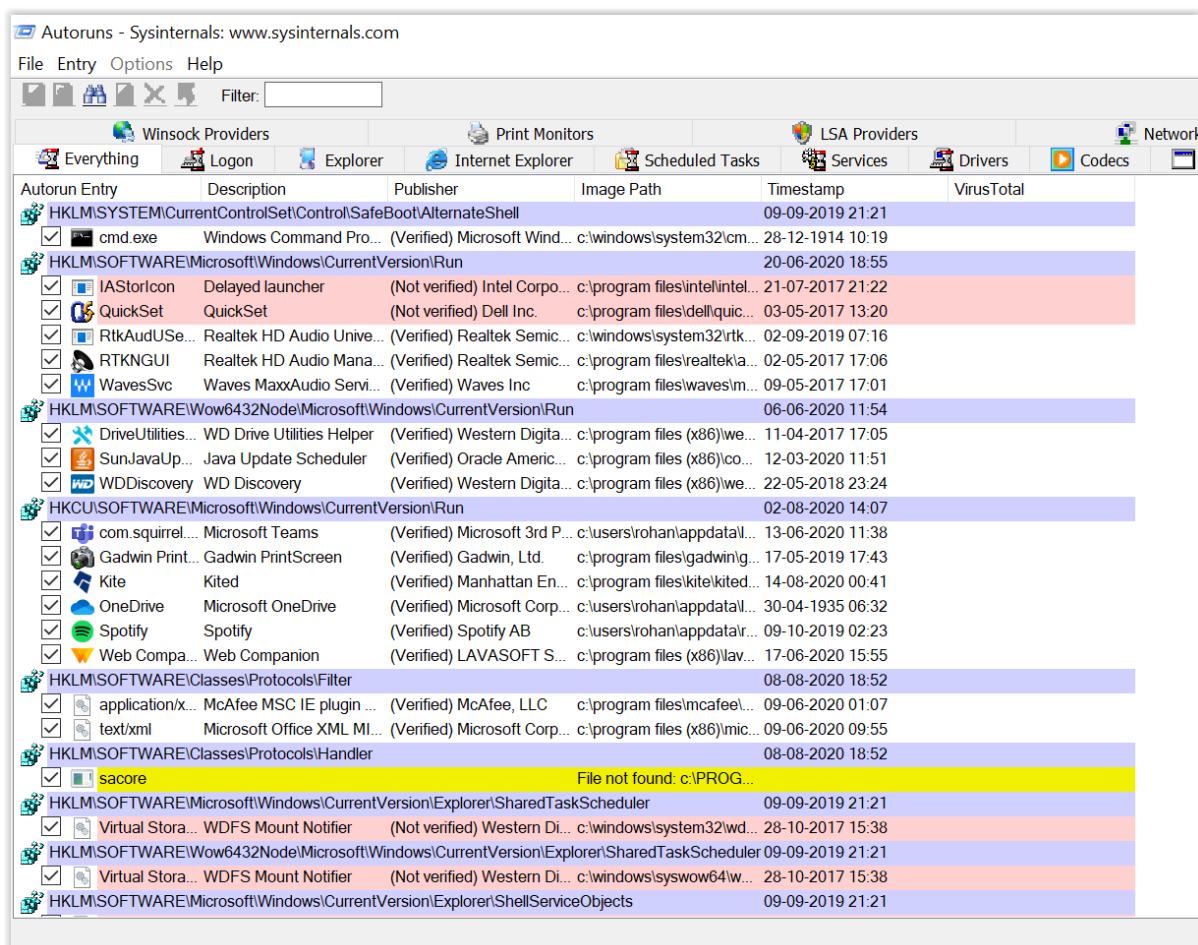
Endpoints: 186 Established: 72 Listening: 46 Time Wait: 2 Close Wait: 15

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
dashHost.exe	3676	UDP	RohandELL	ws-discovery	*	*					
dashHost.exe	3676	UDP	RohandELL	ws-discovery	*	*					
dashHost.exe	3676	UDP	RohandELL	55767	*	*					
dashHost.exe	3676	UDPv6	[0.0.0.0.0.0.0.0]	3702	*	*					
dashHost.exe	3676	UDPv6	[0.0.0.0.0.0.0.0]	3702	*	*					
dashHost.exe	3676	UDPv6	[0.0.0.0.0.0.0.0]	55768	*	*					
explorer.exe	9360	TCP	RohandELL	52391	localhost	50039	ESTABLISHED				
fh_service.exe	13360	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	48664	RohandELL	0	LISTENING				
lsass.exe	956	TCPv6	[0.0.0.0.0.0.0.0]	48664	[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

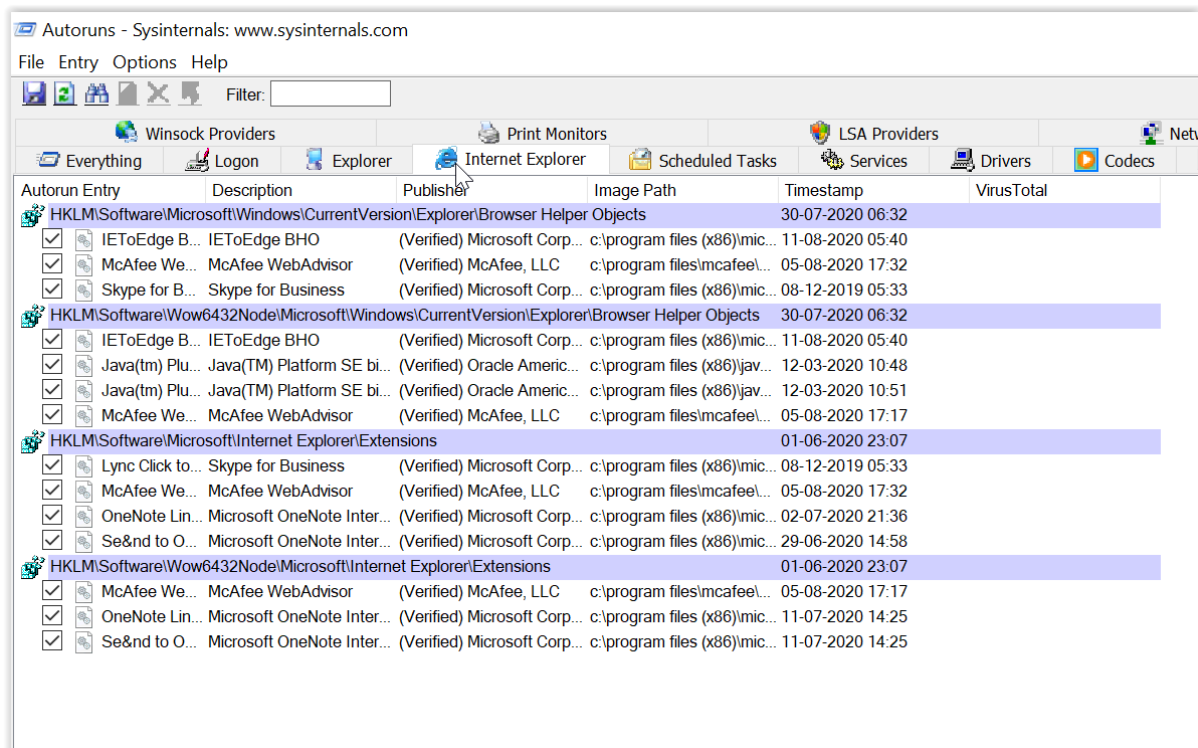
This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer and media players.



The screenshot shows the Autoruns application window with the title bar "Autoruns - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Entry", "Options", and "Help". Below the menu bar is a toolbar with icons for "Winsock Providers", "Print Monitors", "LSA Providers", "Network", "Everything", "Logon", "Explorer", "Internet Explorer", "Scheduled Tasks", "Services", "Drivers", "Codecs", and "Network". The main window displays a table of startup entries with columns: "Autorun Entry", "Description", "Publisher", "Image Path", "Timestamp", and "VirusTotal". The entries are grouped by registry path, such as "HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell", "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "HKLM\SOFTWARE\Classes\Protocols\Filter", and "HKLM\SOFTWARE\Classes\Protocols\Handler". Each entry has a checkbox in the "Autorun Entry" column. The "sacore" entry is highlighted in yellow, and the "File not found: c:\PROG..." entry is highlighted in red.

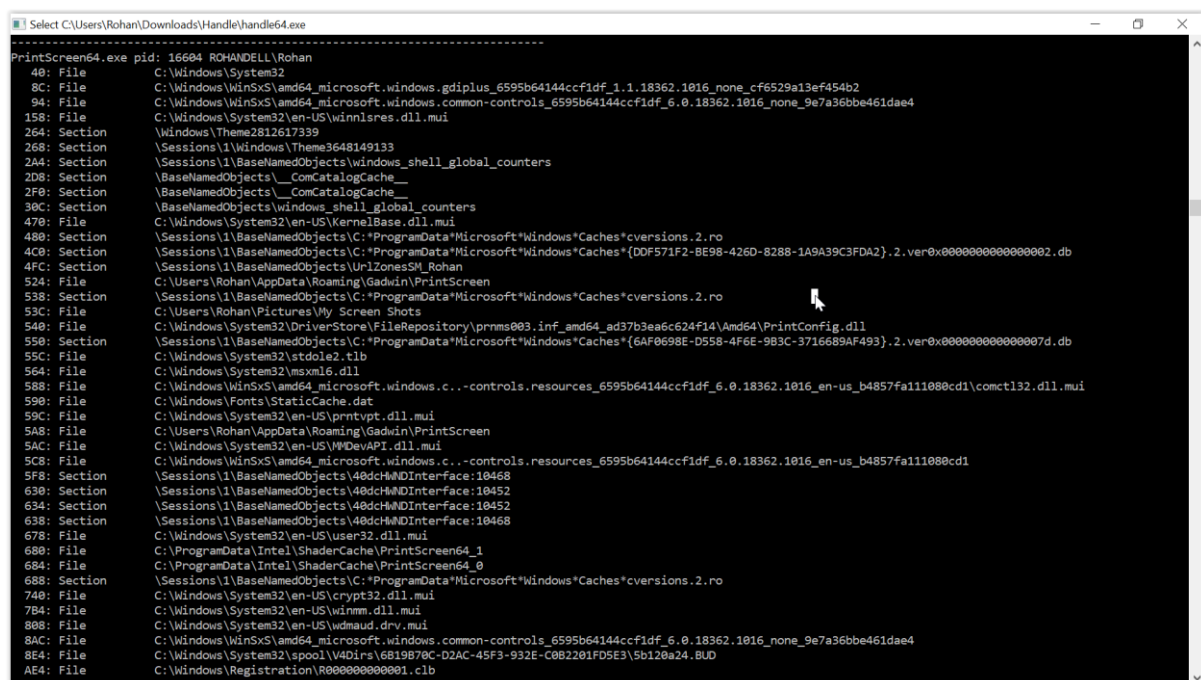
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				09-09-2019 21:21	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Pro...	(Verified) Microsoft Wind...	c:\windows\system32\cm...	28-12-1914 10:19	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				20-06-2020 18:55	
<input checked="" type="checkbox"/> IAStorIcon	Delayed launcher	(Not verified) Intel Corpo...	c:\program files\intel\intel...	21-07-2017 21:22	
<input checked="" type="checkbox"/> QuickSet	QuickSet	(Not verified) Dell Inc.	c:\program files\dell\quic...	03-05-2017 13:20	
<input checked="" type="checkbox"/> RtkAudUse...	Realtek HD Audio Unive...	(Verified) Realtek Semic...	c:\windows\system32\rtk...	02-09-2019 07:16	
<input checked="" type="checkbox"/> RTKNGUI	Realtek HD Audio Mana...	(Verified) Realtek Semic...	c:\program files\realtek\la...	02-05-2017 17:06	
<input checked="" type="checkbox"/> WavesSvc	Waves MaxxAudio Servi...	(Verified) Waves Inc	c:\program files\waves\lm...	09-05-2017 17:01	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				06-06-2020 11:54	
<input checked="" type="checkbox"/> DriveUtilities...	WD Drive Utilities Helper	(Verified) Western Digita...	c:\program files (x86)\we...	11-04-2017 17:05	
<input checked="" type="checkbox"/> SunJavaUp...	Java Update Scheduler	(Verified) Oracle Americ...	c:\program files (x86)\co...	12-03-2020 11:51	
<input checked="" type="checkbox"/> WDDiscovery	WD Discovery	(Verified) Western Digita...	c:\program files (x86)\we...	22-05-2018 23:24	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				02-08-2020 14:07	
<input checked="" type="checkbox"/> com.squirrel...	Microsoft Teams	(Verified) Microsoft 3rd P...	c:\users\rohan\appdata\l...	13-06-2020 11:38	
<input checked="" type="checkbox"/> Gadwin Print...	Gadwin PrintScreen	(Verified) Gadwin, Ltd.	c:\program files\gadwin\g...	17-05-2019 17:43	
<input checked="" type="checkbox"/> Kite	Kited	(Verified) Manhattan En...	c:\program files\kite\kited...	14-08-2020 00:41	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corp...	c:\users\rohan\appdata\l...	30-04-1935 06:32	
<input checked="" type="checkbox"/> Spotify	Spotify	(Verified) Spotify AB	c:\users\rohan\appdata\l...	09-10-2019 02:23	
<input checked="" type="checkbox"/> Web Compa...	Web Companion	(Verified) LAVASOFT S...	c:\program files (x86)\lav...	17-06-2020 15:55	
HKLM\SOFTWARE\Classes\Protocols\Filter				08-08-2020 18:52	
<input checked="" type="checkbox"/> application/x...	McAfee MSC IE plugin ...	(Verified) McAfee, LLC	c:\program files\mcafee\l...	09-06-2020 01:07	
<input checked="" type="checkbox"/> text/xml	Microsoft Office XML MI...	(Verified) Microsoft Corp...	c:\program files (x86)\mic...	09-06-2020 09:55	
HKLM\SOFTWARE\Classes\Protocols\Handler				08-08-2020 18:52	
<input checked="" type="checkbox"/> sacore			File not found: c:\PROG...		
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler				09-09-2019 21:21	
<input checked="" type="checkbox"/> Virtual Stora...	WDFS Mount Notifier	(Not verified) Western Di...	c:\windows\system32\wd...	28-10-2017 15:38	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler				09-09-2019 21:21	
<input checked="" type="checkbox"/> Virtual Stora...	WDFS Mount Notifier	(Not verified) Western Di...	c:\windows\syswow64\w...	28-10-2017 15:38	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects				09-09-2019 21:21	

In Internet Explorer:



Tool 3: Handle for Windows v13.98

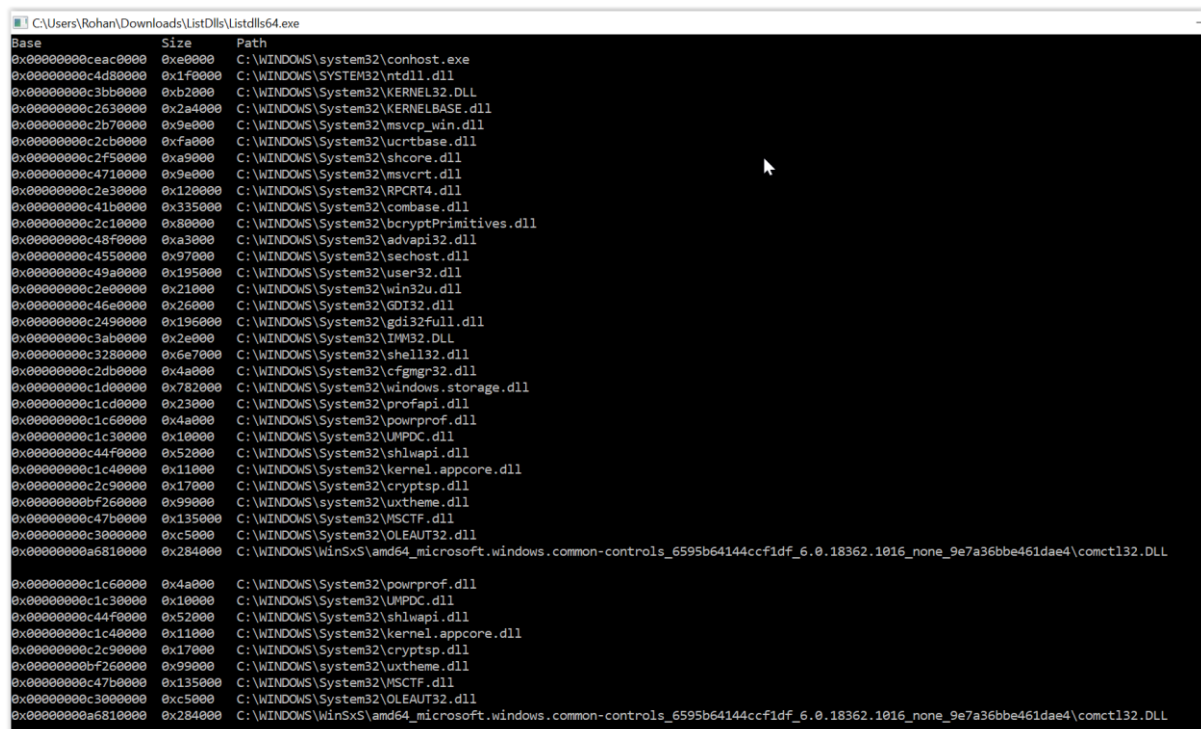
Ever wondered which program has a particular file or directory open? Now you can find out. *Handle* is a utility that displays information about open handles for any process in the system. You can use it to see the programs that have a file open, or to see the object types and names of all the handles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



```
Select C:\Users\Rohan\Downloads\Handle\handle64.exe
-----
PrintScreen64.exe pid: 16684 ROHANDELL\Rohan
40: File C:\Windows\System32
80: File C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.18362.1016_none_cf6529a13ef454b2
94: File C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.18362.1016_none_9e7a36bbe461dae4
158: File C:\Windows\System32\en-US\winl1sres.dll.mui
264: Section \Sessions\1\Windows\Theme2012617339
268: Section \Sessions\1\Windows\Theme3648149133
2A4: Section \Sessions\1\BaseNamedObjects\windows_shell_global_counters
2D8: Section \BaseNamedObjects\ComCatalogCache_
2F0: Section \BaseNamedObjects\ComCatalogCache_
30C: Section \BaseNamedObjects\windows_shell_global_counters
470: File C:\Windows\System32\en-US\KernelBase.dll.mui
480: Section \Sessions\1\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*cversions.2.ro
4C0: Section \Sessions\1\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000002.db
4FC: Section \Sessions\1\BaseNamedObjects\UnlZonesSM_Rohan
524: File C:\Users\Rohan\AppData\Roaming\Gadwin\PrintScreen
538: Section \Sessions\1\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*cversions.2.ro
53C: File C:\Users\Rohan\Pictures\My Screen Shots
540: File C:\Windows\System32\DriverStore\FileRepository\prnms003.inf_amd64_ad37b3ea6c624f14\Amd64\PrintConfig.dll
550: Section \Sessions\1\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x000000000000007d.db
55C: File C:\Windows\System32\lstolx2.tlb
564: File C:\Windows\System32\msxml6.dll
588: File C:\Windows\WinSxS\amd64_microsoft.windows.common-controls.resources_6595b64144ccf1df_6.0.18362.1016_en-us_b4857fa111080cd1\comctl32.dll.mui
590: File C:\Windows\Fonts\StaticCache.dat
59C: File C:\Windows\System32\en-US\prntvpt.dll.mui
5A8: File C:\Users\Rohan\AppData\Roaming\Gadwin\PrintScreen
5AC: File C:\Windows\System32\en-US\MMDevAPI.dll.mui
5C8: File C:\Windows\WinSxS\amd64_microsoft.windows.common-controls.resources_6595b64144ccf1df_6.0.18362.1016_en-us_b4857fa111080cd1
5F8: Section \Sessions\1\BaseNamedObjects\40dchWNDInterface:10468
630: Section \Sessions\1\BaseNamedObjects\40dchWNDInterface:10452
634: Section \Sessions\1\BaseNamedObjects\40dchWNDInterface:10452
638: Section \Sessions\1\BaseNamedObjects\40dchWNDInterface:10468
678: File C:\Windows\System32\en-US\user32.dll.mui
680: File C:\ProgramData\Intel\ShaderCache\PrintScreen64_1
684: File C:\ProgramData\Intel\ShaderCache\PrintScreen64_0
688: Section \Sessions\1\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*cversions.2.ro
740: File C:\Windows\System32\en-US\crypt32.dll.mui
784: File C:\Windows\System32\en-US\winmm.dll.mui
808: File C:\Windows\System32\en-US\wdmaud.drv.mui
8AC: File C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.18362.1016_none_9e7a36bbe461dae4
8E4: File C:\Windows\System32\spool\V4Dirs\6819B70C-D2AC-45F3-932E-C0B2201FD5E3\Sb120a24.BUD
AE4: File C:\Windows\Registration\R000000000001.c1b
```

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.

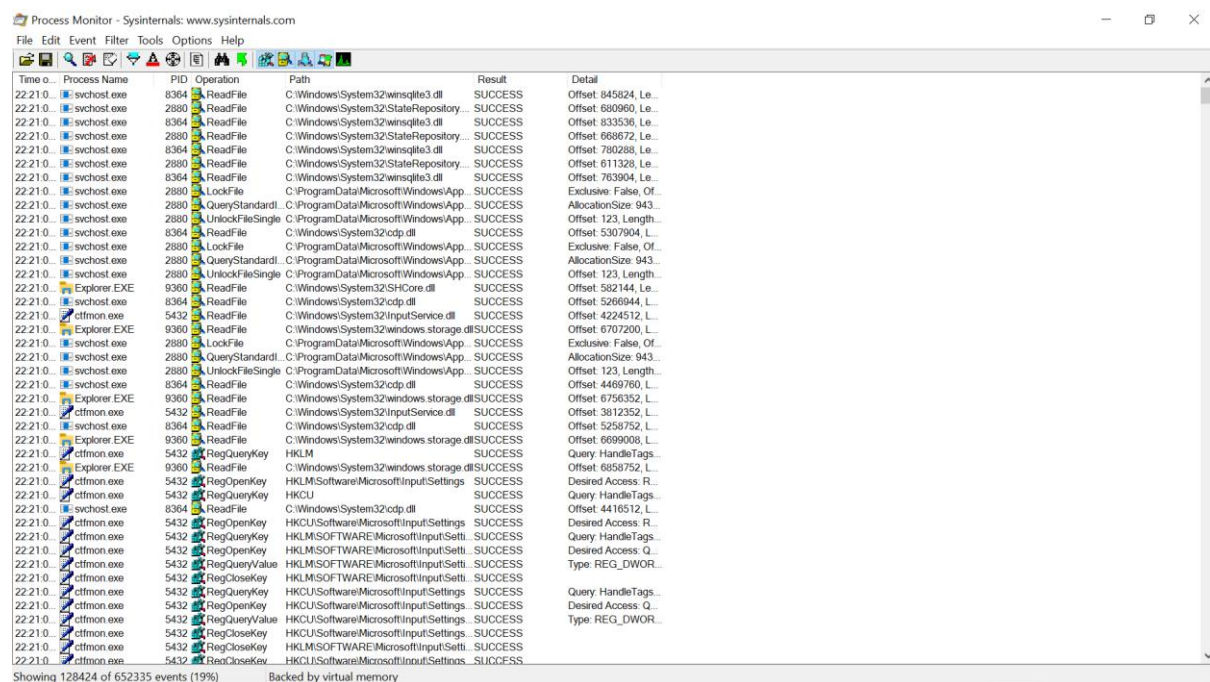


```
C:\Users\Rohan\Downloads\ListDLLs\Listdlls64.exe
Base      Size      Path
0x00000000caac0000 0xe0000 C:\WINDOWS\system32\conhost.exe
0x00000000c4d80000 0x1f0000 C:\WINDOWS\SYSTEM32\ntdll.dll
0x00000000c3bb0000 0xb2000 C:\WINDOWS\System32\KERNEL32.DLL
0x00000000c2630000 0x2a4000 C:\WINDOWS\System32\KERNELBASE.dll
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\x-wwww-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\x-wwww-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.

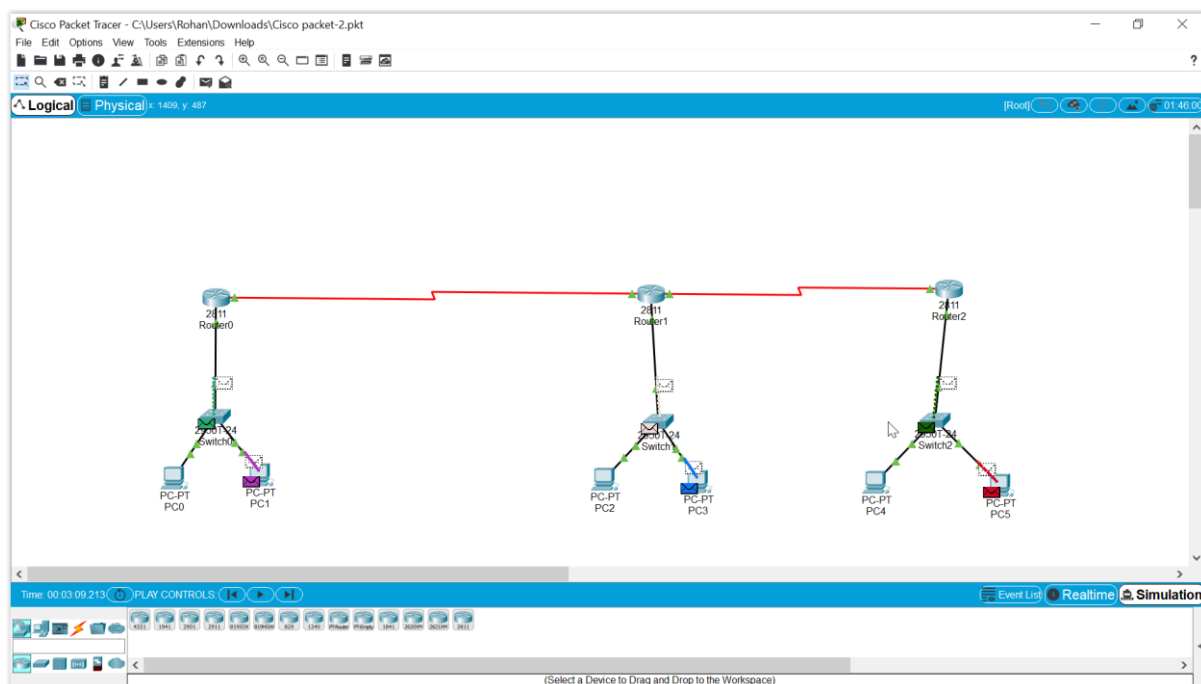
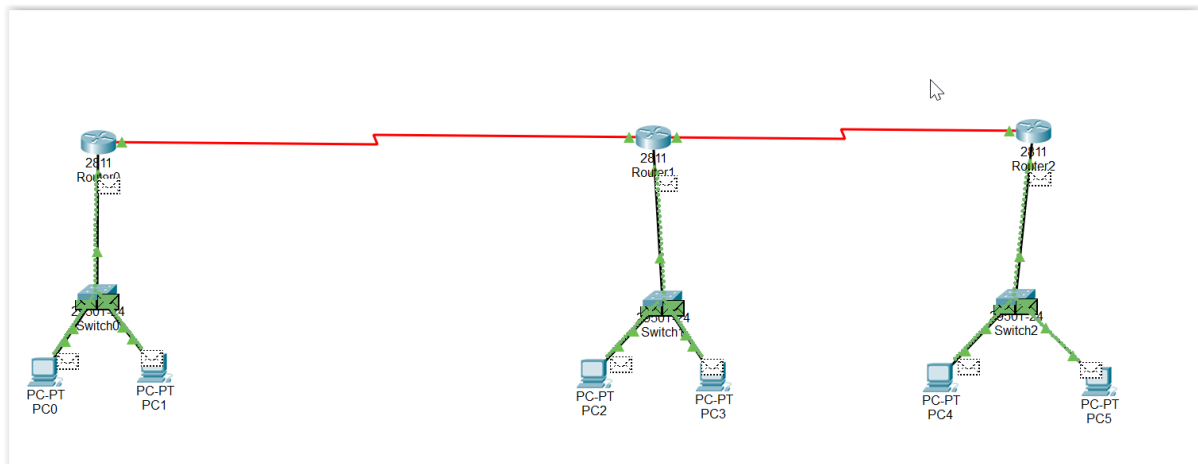
Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

Aim:

- 1) To get this network topology:

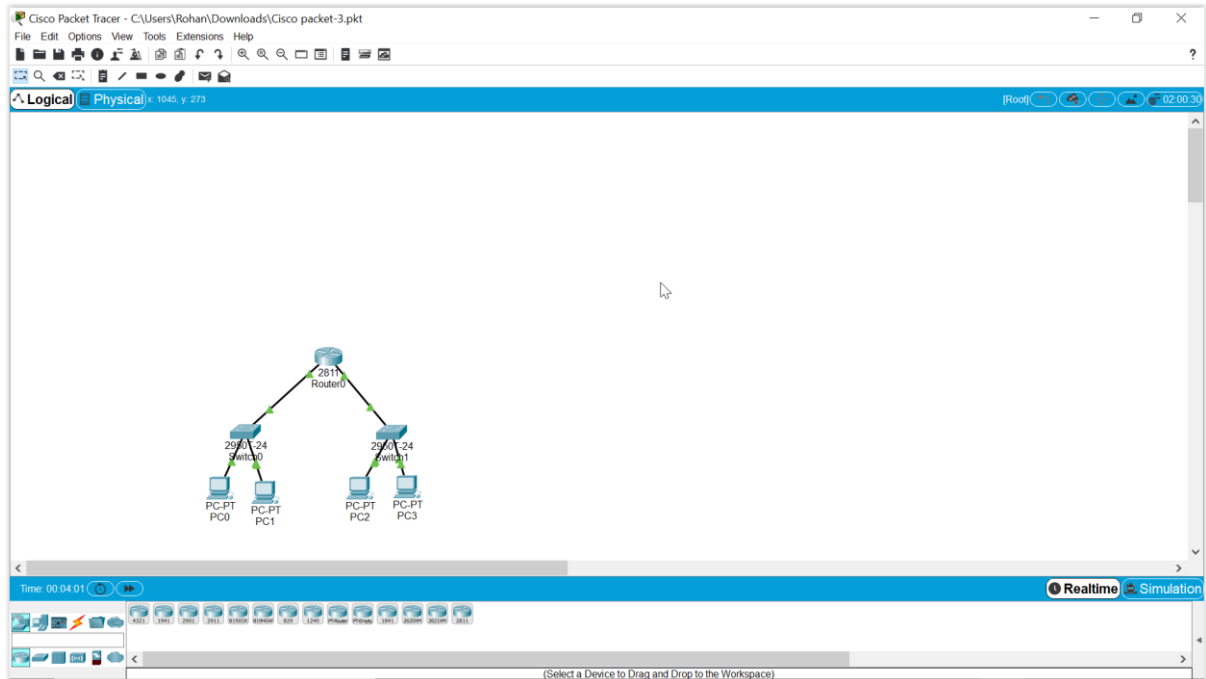


Simulation:



Aim:

2) To get this network topology:



On Simulation:

