



School of Computer Science
UNIVERSITY OF PETROLEUM AND ENERGY
STUDIES
DEHRADUN, UTTARAKHAND

Digital Forensics Lab File

5th Semester

Submitted by:

Khushi Wadhawan
Sap ID: 500093673
Btech CSE CSF
Batch: 2

Submitted to:

Dr. Deepika Koundal

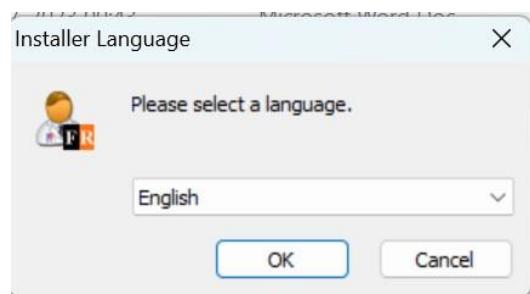
EXPERIMENT 1

Lab Objective: Data Recovery using PC Inspector and other data recovery tools

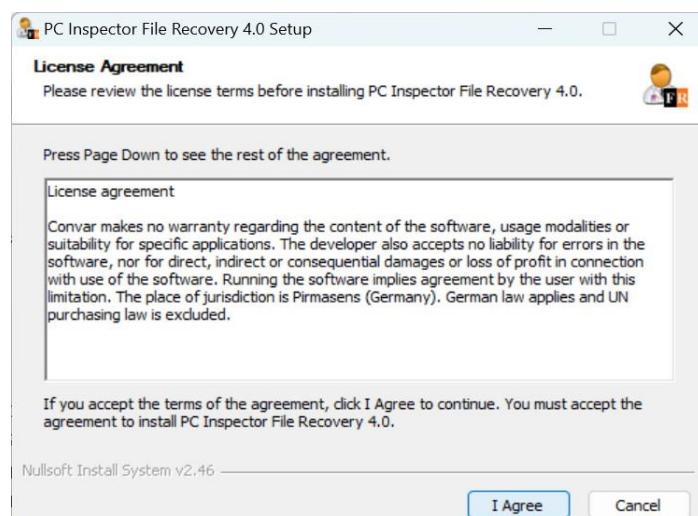
Go to pcinspector.de site and install pc inspector

The screenshot shows a web browser window with the URL pcinspector.de/index-en.html. The page content includes a list of file formats supported by the software, a note about being freeware, and a prominent green 'DOWNLOAD here!' button. The browser's address bar and various tabs are visible at the top.

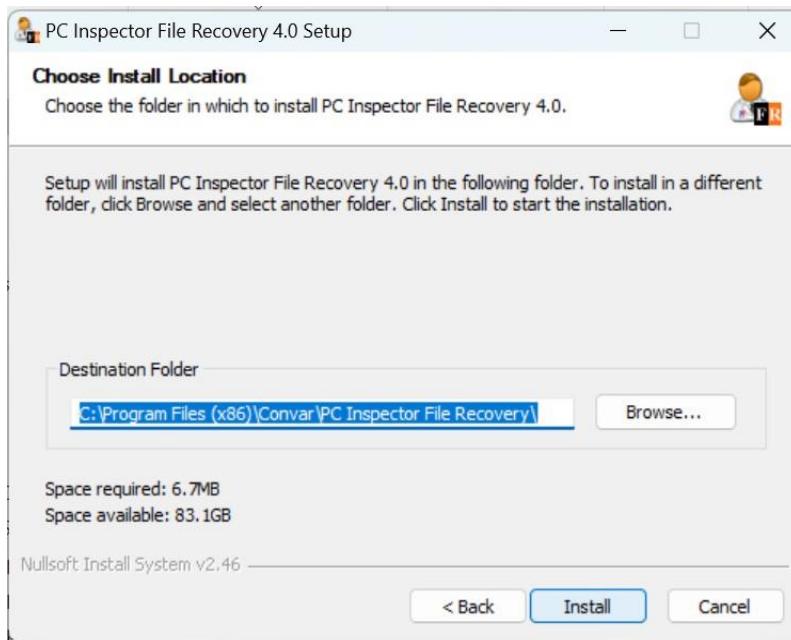
Choose the preferred language



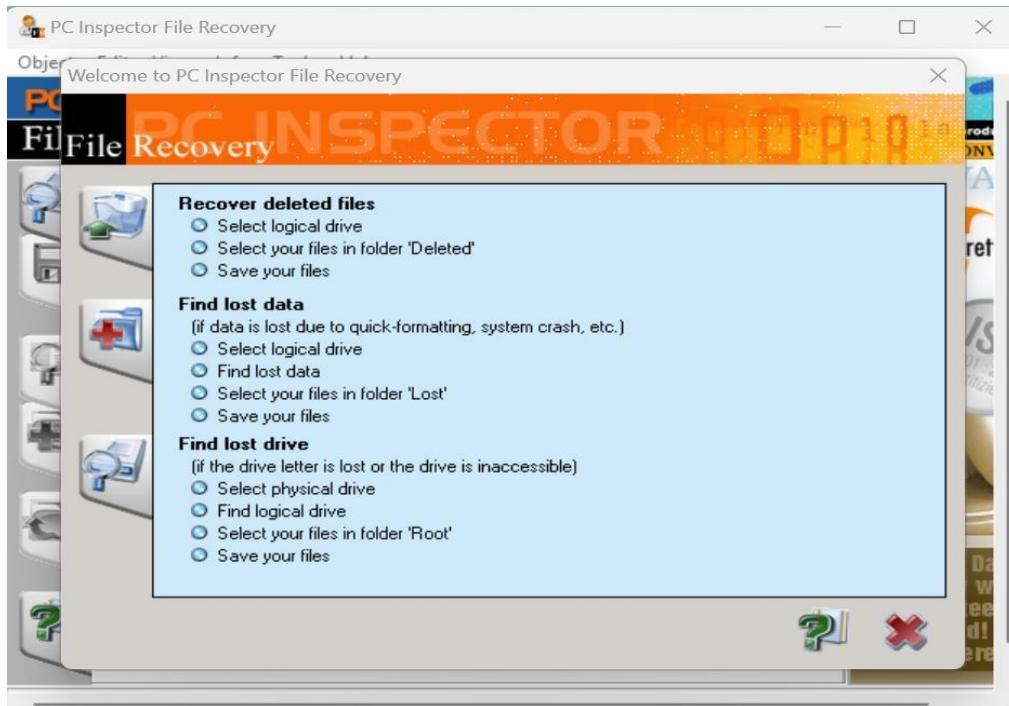
Accept terms and conditions and click on “I Agree”



Choose the location at which we want to install pc inspector

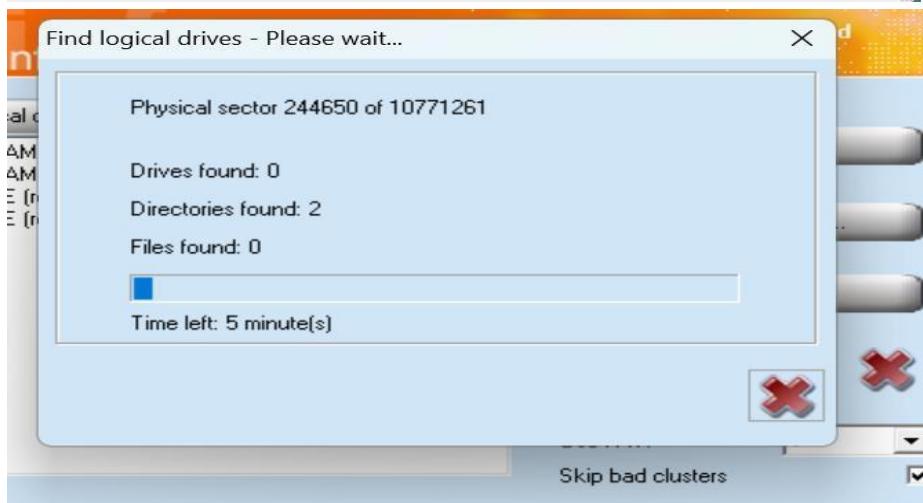
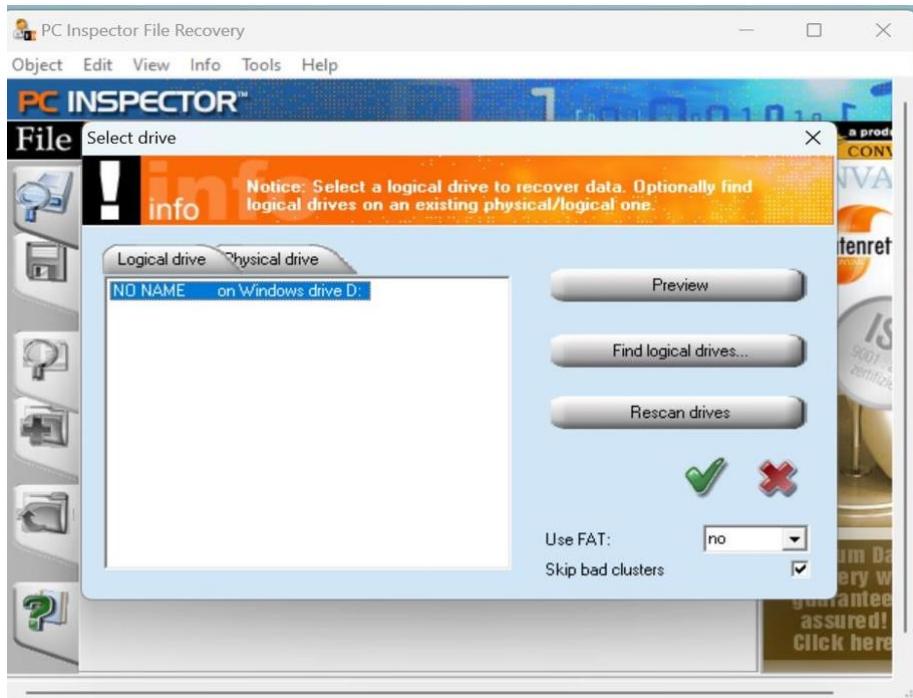


Click on select logical drive

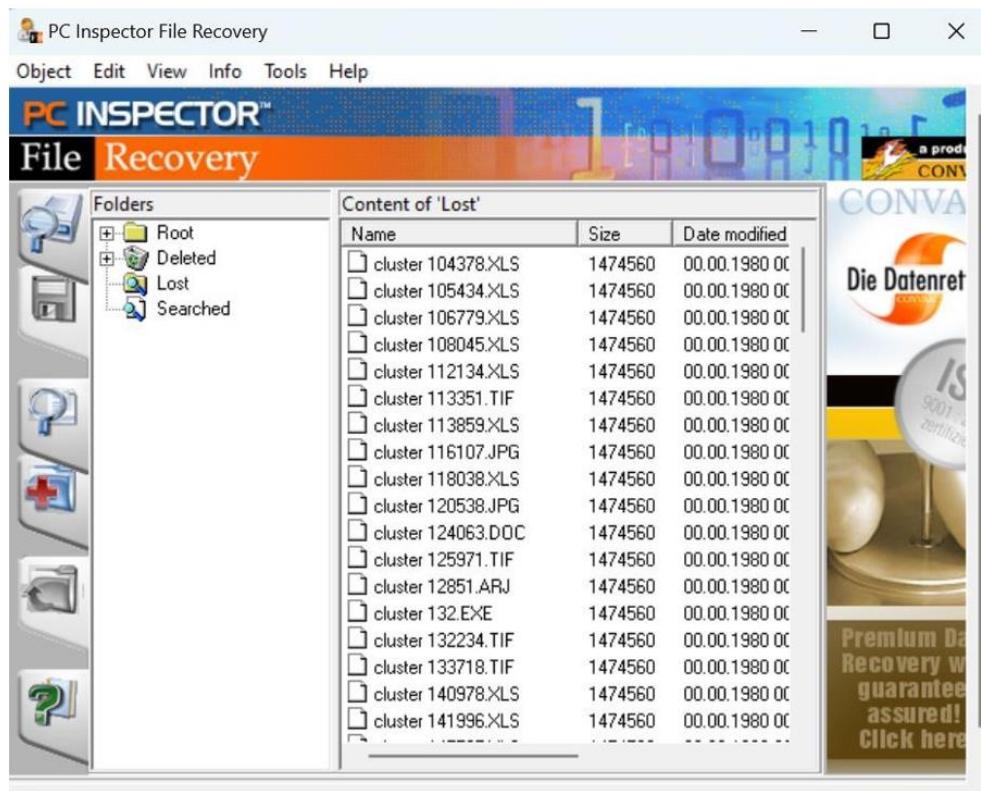


Select your pen drive that will be used to perform the experiment

Click on find logical drives



Recovered files will be displayed

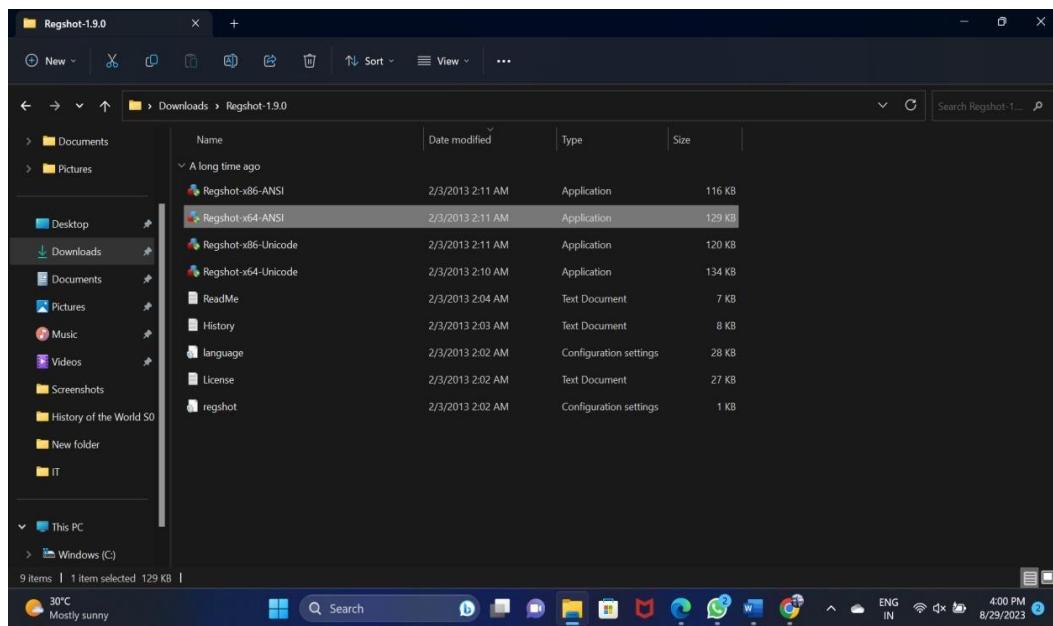
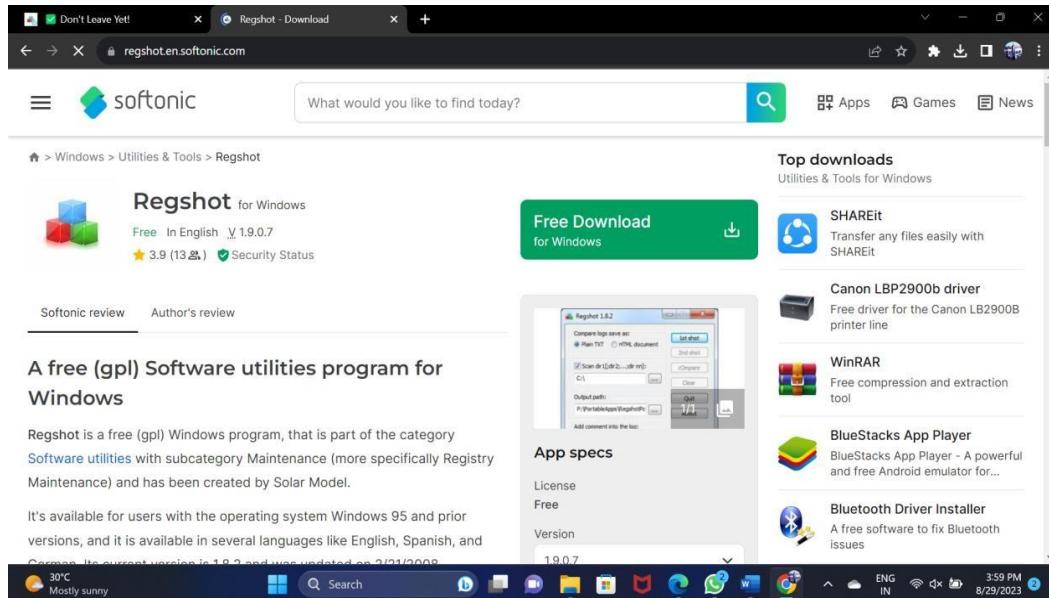


EXPERIMENT 2

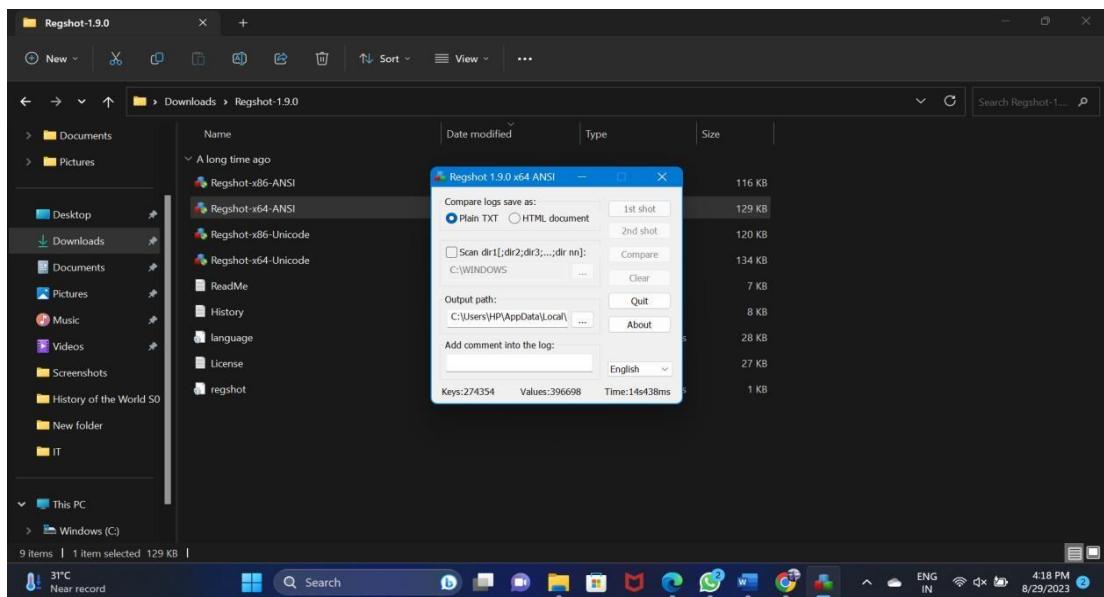
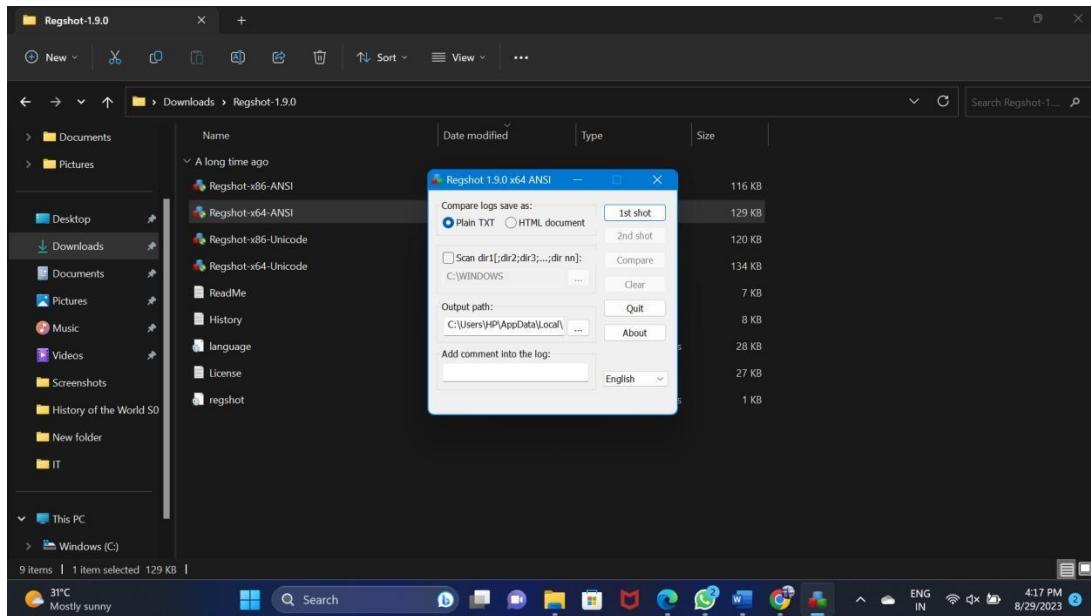
Lab Objective: Identifying changes in registry files using Regshot

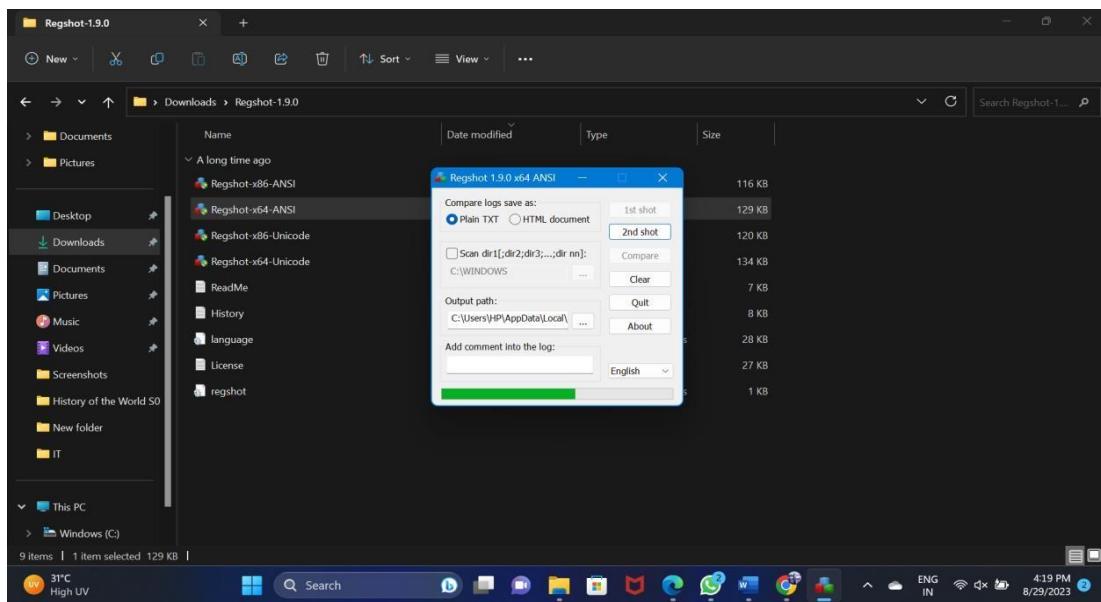
STEPS:

1. Download Regshot from <https://regshot.en.softonic.com/>



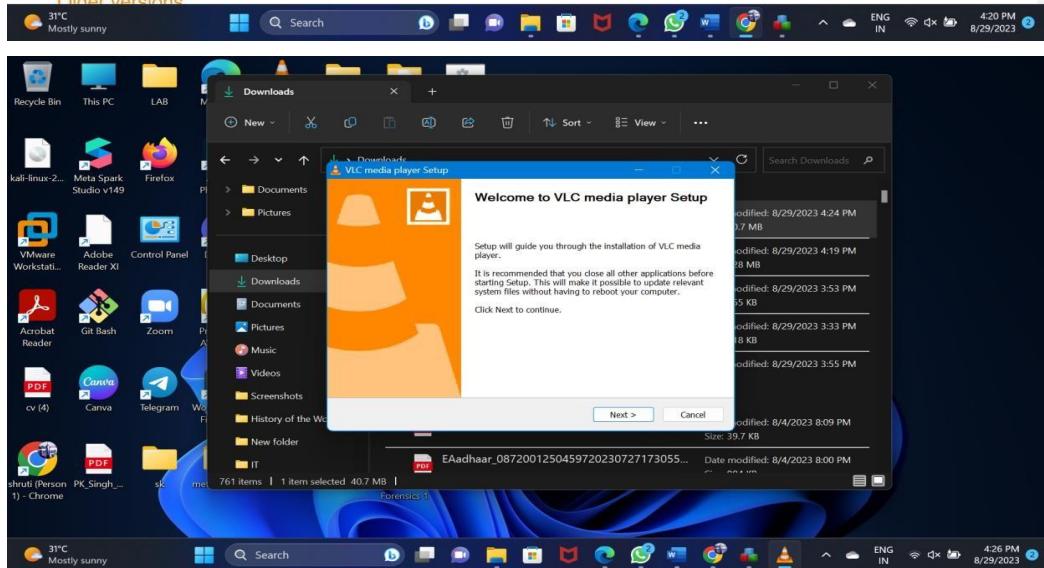
2. Running ANSI executable file from Regshot and taking the 1st shot





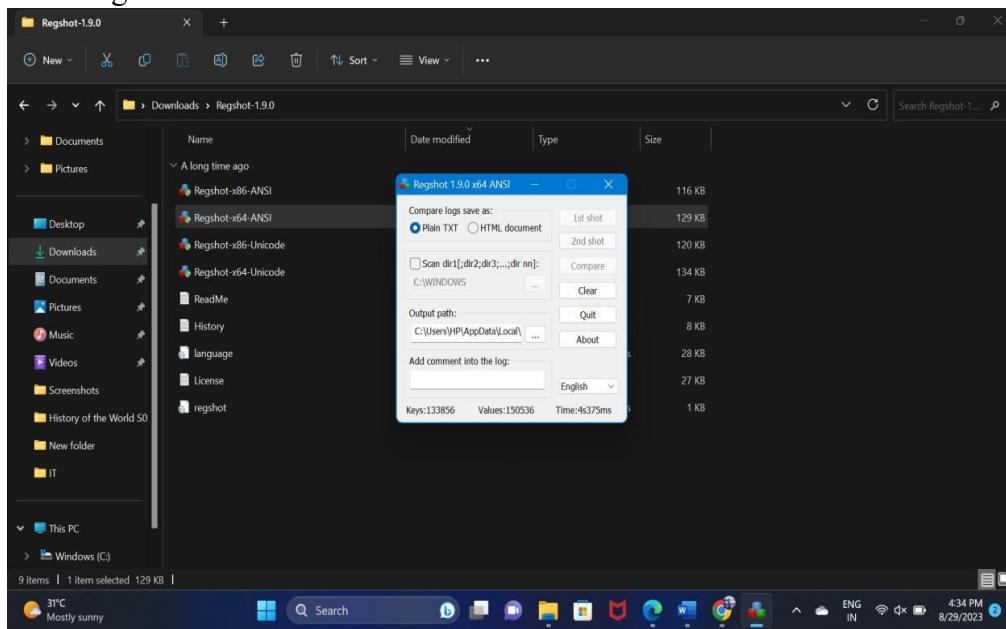
3. Installing VLC to change registry files

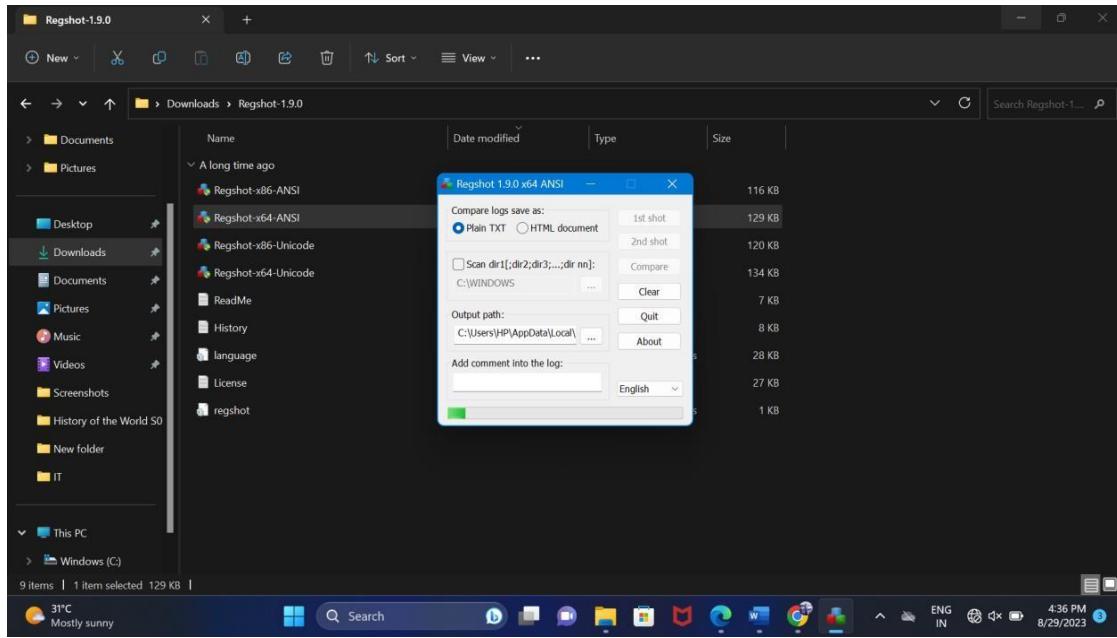
A screenshot of a web browser displaying the official VLC media player download page at videolan.org/vlc/download-windows.html. The page has a header with the VideoLAN organization logo and navigation links for VideoLAN, VLC, Projects, Contribute, and Support. It features a large video thumbnail of a lion from the movie 'Madagascar'. Below the video, there's a prominent orange 'Download VLC' button. To the left of the button, there's a section titled 'Windows requirements' with a note that VLC runs on all versions of Windows from XP SP3 to Windows 11. There's also a 'VLC for Windows 95/98/Me' section with a note about Kernel32.dll. The page footer contains a 'donate' button.





4. Taking the 2nd shot





5. Comparing the two shots

CONCLUSION: Through this experiment, I learnt about the tool REGSHOT, which can be used to identify changes in registry files. This can determine what kind of activities and changes are performed on the system and whether they can be harmful.

EXPERIMENT 3

Lab objective: Sysinternals tool kits to diagnosis, monitoring or analysis of windows machine.

Sysinternals tool kits to diagnosis, monitoring or analysis of windows machine.

Install Sysinternals

The screenshot shows a Microsoft Learn page for the Sysinternals Suite. The URL is learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite. The page title is "Sysinternals Suite". On the left, there's a sidebar with navigation links like Home, Downloads, and Sysinternals Suite (which is highlighted). The main content area has a heading "Sysinternals Suite" and a sub-heading "By Mark Russinovich Updated: July 26, 2023". It lists four download options: "Download Sysinternals Suite" (45.2 MB), "Download Sysinternals Suite for Nano Server" (9.5 MB), "Download Sysinternals Suite for ARM64" (14.3 MB), and "Install Sysinternals Suite from the Microsoft Store". To the right, there are sections for "Additional resources" (Training, Documentation, Sysinternals Utilities, Sysinternals - Sysinternals, Sysinternals Process UI) and "Feedback". A search bar is at the top right.

Exploring Procmon

Procmon is a downloadable utility for Microsoft Windows OS that captures and displays system and network activity. This includes file system activity, registry key activity, network, and threat activities.

Process Monitor - Sysinternals: www.sysinternals.com

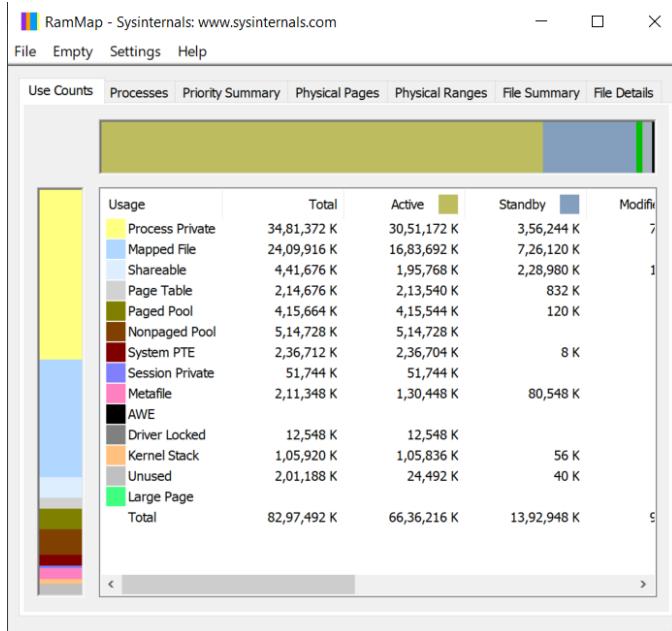
File Edit Event Filter Tools Options Help

Time o.	Process Name	PID	Operation	Path	Result	Detail
15:34:39.	lsass.exe	996	ReadFile	C:\Windows\System32\lsass.dll	SUCCESS	Offset: 1607168, Le...
15:34:39.	lsass.exe	996	ReadFile	C:\Windows\System32\lsass.dll	SUCCESS	Offset: 1590784, Le...
15:34:39.	lsass.exe	996	ReadFile	C:\Windows\System32\lsass.dll	SUCCESS	Offset: 1506304, Le...
15:34:39.	MsMpEng.exe	5564	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset: 15695872, L...
15:34:39.	MsMpEng.exe	5564	ReadFile	C:\Windows\System32\lsass.dll	SUCCESS	Offset: 1578496, Le...
15:34:39.	MsMpEng.exe	5564	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset: 15675392, L...
15:34:39.	MsMpEng.exe	5564	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset: 16793600, L...
15:34:39.	lsass.exe	996	ReadFile	C:\Windows\System32\lsass.dll	SUCCESS	Offset: 1489900, Le...
15:34:39.	MsMpEng.exe	5564	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset: 15794176, L...
15:34:39.	lsass.exe	996	QueryNameInfo	C:\Users\pavne\AppData\Local\Temp\...	SUCCESS	Name: \Users\pav...
15:34:39.	lsass.exe	996	QueryNameInfo	C:\Users\pavne\AppData\Local\Temp\...	SUCCESS	Name: \Users\pav...
15:34:39.	Explorer EXE	10040	RegQueryKey	HKEY\Software\Classes	SUCCESS	Query: Name
15:34:39.	Explorer EXE	10040	RegQueryKey	HKEY\Software\Classes	SUCCESS	Query: HandleTag...
15:34:39.	Explorer EXE	10040	RegQueryKey	HKEY\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
15:34:39.	Explorer EXE	10040	RegOpenKey	HKEY\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
15:34:39.	MsMpEng.exe	5564	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset: 1577792, L...
15:34:39.	Explorer EXE	10040	RegQueryKey	HKEY\Software\Classes	BUFFER TOO SM...	Query: Name, Len...
15:34:39.	Explorer EXE	10040	RegQueryKey	HKEY\Software\Classes	SUCCESS	Query: Name
15:34:39.	Explorer EXE	10040	RegOpenKey	HKEY\Software\Microsoft\AppMode...	NAME NOT FOUND	Desired Access: R...
15:34:39.	Explorer EXE	10040	RegQueryKey	HKEY\Software\Classes	SUCCESS	Query: Name
15:34:39.	Explorer EXE	10040	RegQueryKey	HKEY\Software\Classes	SUCCESS	Query: HandleTag...
15:34:39.	Explorer EXE	10040	RegQueryKey	HKEY\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
15:34:39.	Explorer EXE	10040	RegOpenKey	HKEY\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
15:34:39.	Explorer EXE	10040	RegQueryKey	HKEY\Software\Classes	BUFFER TOO SM...	Query: Name, Len...
15:34:39.	Explorer EXE	10040	RegQueryKey	HKEY\Software\Classes	SUCCESS	Query: Name
15:34:39.	Explorer EXE	10040	RegOpenKey	HKEY\Software\Microsoft\AppMode...	NAME NOT FOUND	Desired Access: R...
15:34:39.	MsMpEng.exe	5564	ReadFile	C:\ProgramData\Microsoft\Windows Def...	SUCCESS	Offset: 16908288, L...
15:34:39.	Explorer EXE	10040	CreateFile	C:\Users\pavne\AppData\Local\Temp\...	SUCCESS	Desired Access: R...
15:34:39.	Explorer EXE	10040	QueryBasicInfor	C:\Users\pavne\AppData\Local\Temp\...	SUCCESS	CreationTime: 05-0...

Showing 141265 of 161525 events (87%) Backed by virtual memory

Exploring Rammap

This tool provides us with details regarding how windows assign physical memory, how much data is cached in RAM, kernel, and device drivers' uses of RAM.



RamMap - Sysinternals: www.sysinternals.com

File Empty Settings Help

Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details

Process	Session	PID	Private	Standby	Modifier
System	-1	4	0 K	0 K	0 I
Registry	-1	124	12,636 K	0 K	0 I
Creative Cloud	1	14980	11,568 K	0 K	4 I
FMAPP.exe	1	16312	0 K	0 K	0 I
RiotClientServ	1	17420	4,428 K	0 K	16 I
smss.exe	-1	552	104 K	0 K	0 I
dllhost.exe	0	7784	720 K	0 K	0 I
chrome.exe	1	17524	2,38,964 K	0 K	0 I
chrome.exe	1	14888	38,876 K	12 K	0 I
webwallpaper...	1	10260	3,776 K	0 K	0 I
csrss.exe	0	808	872 K	0 K	0 I
TextInputHost.	1	9708	3,904 K	0 K	1,464 I
wininit.exe	0	900	16 K	0 K	8 I
cssrs.exe	1	912	1,480 K	0 K	0 I
services.exe	0	976	4,988 K	0 K	0 I
lsass.exe	0	996	6,616 K	0 K	24 I
fontdrvhost.ex	0	480	136 K	0 K	0 I
svchost.exe	0	568	9,248 K	0 K	16 I
WUDFHost.exe	0	1076	3,484 K	0 K	0 I
svchost.exe	0	1180	2,192 K	0 K	4 I
svchost.exe	0	1132	9,336 K	0 K	0 C I

RamMap - Sysinternals: www.sysinternals.com

File Empty Settings Help

Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details

Priority	Standby	Repurposed
0	2,61,332 K	96,41,828 K
1	18,092 K	53,69,988 K
2	60,428 K	36,82,324 K
3	0 K	1,300 K
4	81,192 K	54,47,372 K
5	7,80,628 K	1,27,31,996 K
6	54,096 K	32,608 K
7	1,36,744 K	0 K
Total	13,92,512 K	3,69,07,416 K

RamMap - Sysinternals: www.sysinternals.com

File Empty Settings Help

Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details

Path	Size	PhysicalAddress	List
C:\users\pavne\appdata\local\microsoft\windows\usrclass.dll	8,308 K		
C:\program files\google\chrome\application\116.0.5845.141\chromedriver.exe	1,12,71...		
C:\programdata\microsoft\windows\apprepository\staterespository.dll	940 K		
C:\windows\system32\webplatstorageserver.dll	776 K		
C:\windows\prefetch\wwwahost.exe-07457cc0e.pf	112 K		
C:\windows\system32\dbgeng.dll	1,544 K		
C:\users\pavne\appdata\local\discord\app-1.0.9016\discord.exe	57,600 K		
D:\program files (x86)\epic games\launcherengine\binaries\win64\epicgames.exe	12,224 K		
C:\windows\system32\config\software	1,03,60...		
C:\users\pavne\appdata\local\google\chrome\user data\default\index.html	2,104 K		
C:\users\pavne\ntuser.dat	11,848 K		
C:\windows\system32\msvcr7.dll	1,244 K		
C:\windows\fonts\seguisemj.ttf	316 K		
C:\windows\winsxs\amd64_microsoft-windows-servicingstack\1_0_2100_1\servicing.dll	128 K		
D:\users\pavne\desktop\steamapps\common\wallpaper_eng\WallpaperEng.exe	51,248 K		
C:\windows\serviceprofiles\localservice\appdata\local\fontcache\FontCache.dll	16,088 K		
C:\users\pavne\onedrive\desktop\sysinternalssuite\procmon.exe	8,252 K		
C:\windows\syswow64\tquery.dll	968 K		
C:\windows\system32\windows.staterepositoryps.dll	1,188 K		
C:\windows\syswow64\d3d12core.dll	704 K		
C:\programdata\microsoft\windows\systemdata\s-1-5-21-138\WindowsUpdate.dll	812 K		
C:\windows\system32\driverstore\filerepository\nvlti.inf_amd64\NVLTI.inf	1,312 K		
C:\windows\system32\en-us\kernelbase.dll.mui	1,276 K		
C:\programdata\microsoft\search\data\applications\windows\WindowsSearch.dll	11,544 K		
C:\program files (x86)\common files\steam\steamservice.dll	1,288 K		

Exploring VMmap

It displays the processes committed to virtual memory types as well as the amount of physical memory assigned by the OS to VM types. It also shows summary information and a detailed process memory map.

VMMap - Sysinternals: www.sysinternals.com

File Edit View Tools Options Help

Select or Launch Process

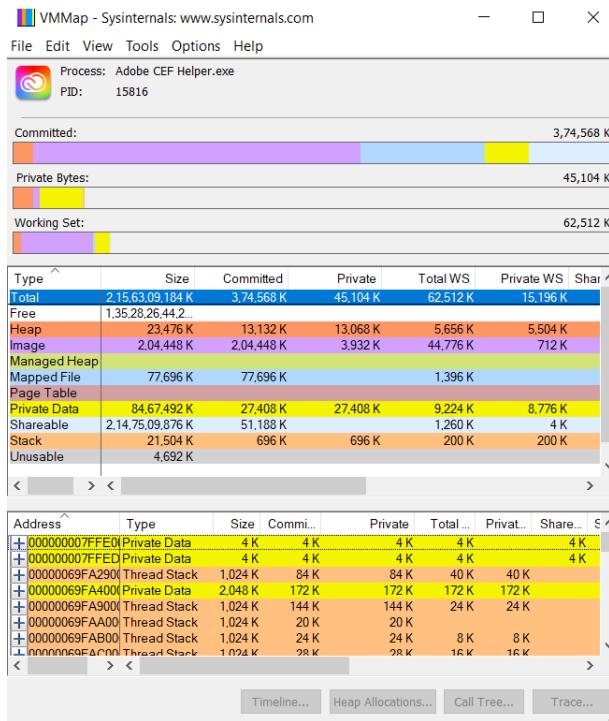
View a running process Launch and trace a new process

Name	PID	User	Private Bytes
Adobe CEF Helper....	9480	LAPTOP-S20IS77A\pa...	23,43
Adobe CEF Helper....	15816	LAPTOP-S20IS77A\pa...	47,44
Adobe CEF Helper....	15684	LAPTOP-S20IS77A\pa...	45,84
Adobe Desktop Ser...	2880	LAPTOP-S20IS77A\pa...	87,65
AdobeIPCBroker.exe	16656	LAPTOP-S20IS77A\pa...	5,90
browserhost.exe	21704	LAPTOP-S20IS77A\pa...	6,32
CCLibrary.exe	11952	LAPTOP-S20IS77A\pa...	63
CCXProcess.exe	16052	LAPTOP-S20IS77A\pa...	63
chrome.exe	2128	LAPTOP-S20IS77A\pa...	1,82,00
chrome.exe	23068	LAPTOP-S20IS77A\pa...	6,85
chrome.exe	20804	LAPTOP-S20IS77A\pa...	4,55,76
chrome.exe	8772	LAPTOP-S20IS77A\pa...	25,00
chrome.exe	22480	LAPTOP-S20IS77A\pa...	14,80
chrome.exe	3272	LAPTOP-S20IS77A\pa...	23,75
chrome.exe	1888	LAPTOP-S20IS77A\pa...	24,32
chrome.exe	3424	LAPTOP-S20IS77A\pa...	36,76
chrome.exe	22616	LAPTOP-S20IS77A\pa...	58,89

Refresh Show All Processes

OK Cancel

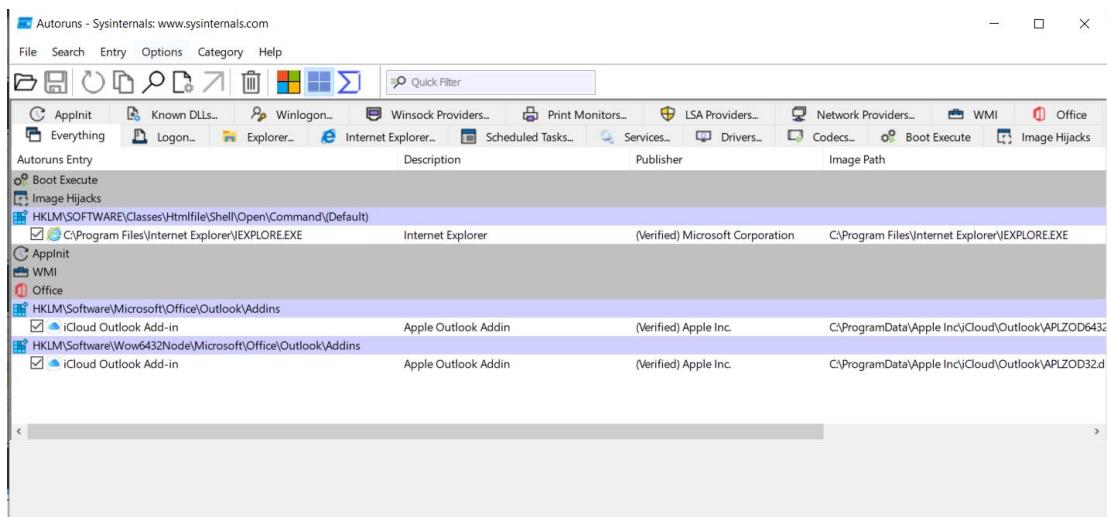
Timeline... Heap Allocations... Call Tree... Trace...



Exploring Autoruns

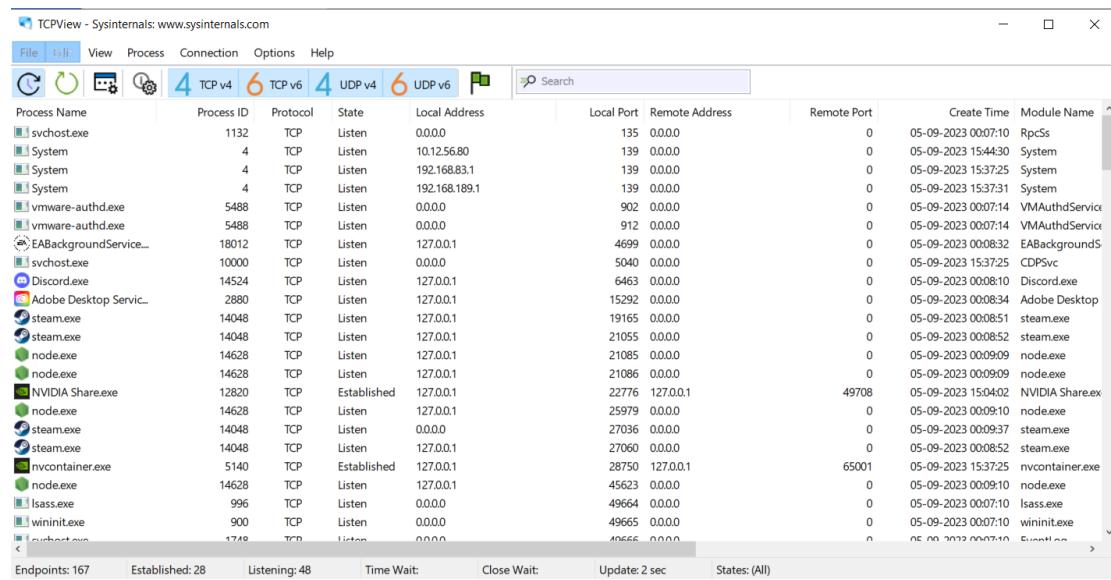
It shows which programs have permission to run during the system bootup or login. It shows which programs have auto run enabled and it also shows us a full list of registries and file system location available for auto-startup configuration.

It also has a virus-total feature which helps us flag out any malicious configuration.



Exploring TCP view

It provides us with a detailed listing of all TCP and UDP endpoints on our machine. These include local and remote connections as well as TCP connection state.



The screenshot shows the TCPView application interface. At the top, there's a menu bar with File, Edit, View, Process, Connection, Options, and Help. Below the menu is a toolbar with icons for File, Edit, View, Process, Connection, Options, Help, and a search bar. The main window displays a table of network endpoints. The columns are: Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, Create Time, and Module Name. The table lists numerous entries, including svchost.exe, System, vmware-authd.exe, EABackgroundService, svchost.exe, Discord.exe, Adobe Desktop Servic..., steam.exe, steam.exe, node.exe, NVIDIA Share.exe, node.exe, steam.exe, steam.exe, nvcontainer.exe, node.exe, lsass.exe, and wininit.exe. The table shows various connection states like Listen, Established, and Time Wait. The 'Create Time' column indicates the date and time when each connection was established. The 'Module Name' column shows the executable file for each connection.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1132	TCP	Listen	0.0.0.0	135	0.0.0.0	0	05-09-2023 00:07:10	RpcSs
System	4	TCP	Listen	10.12.56.80	139	0.0.0.0	0	05-09-2023 15:43:30	System
System	4	TCP	Listen	192.168.83.1	139	0.0.0.0	0	05-09-2023 15:37:25	System
System	4	TCP	Listen	192.168.189.1	139	0.0.0.0	0	05-09-2023 15:37:31	System
vmware-authd.exe	5488	TCP	Listen	0.0.0.0	902	0.0.0.0	0	05-09-2023 00:07:14	VMAuthdService
vmware-authd.exe	5488	TCP	Listen	0.0.0.0	912	0.0.0.0	0	05-09-2023 00:07:14	VMAuthdService
EABackgroundService...	18012	TCP	Listen	127.0.0.1	4699	0.0.0.0	0	05-09-2023 00:08:32	EABackgroundS
svchost.exe	10000	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	05-09-2023 15:37:25	CDPSvc
Discord.exe	14524	TCP	Listen	127.0.0.1	6463	0.0.0.0	0	05-09-2023 00:08:10	Discord.exe
Adobe Desktop Servic...	2880	TCP	Listen	127.0.0.1	15292	0.0.0.0	0	05-09-2023 00:08:34	Adobe Desktop
steam.exe	14048	TCP	Listen	127.0.0.1	19165	0.0.0.0	0	05-09-2023 00:08:51	steam.exe
steam.exe	14048	TCP	Listen	127.0.0.1	21055	0.0.0.0	0	05-09-2023 00:08:52	steam.exe
node.exe	14628	TCP	Listen	127.0.0.1	21085	0.0.0.0	0	05-09-2023 00:09:09	node.exe
node.exe	14628	TCP	Listen	127.0.0.1	21086	0.0.0.0	0	05-09-2023 00:09:09	node.exe
NVIDIA Share.exe	12820	TCP	Established	127.0.0.1	22776	127.0.0.1	49708	05-09-2023 15:04:02	NVIDIA Share.ex
node.exe	14628	TCP	Listen	127.0.0.1	25979	0.0.0.0	0	05-09-2023 00:09:10	node.exe
steam.exe	14048	TCP	Listen	0.0.0.0	27036	0.0.0.0	0	05-09-2023 00:09:37	steam.exe
steam.exe	14048	TCP	Listen	127.0.0.1	27060	0.0.0.0	0	05-09-2023 00:08:52	steam.exe
nvcontainer.exe	5140	TCP	Established	127.0.0.1	28750	127.0.0.1	65001	05-09-2023 15:37:25	nvcontainer.exe
node.exe	14628	TCP	Listen	127.0.0.1	45623	0.0.0.0	0	05-09-2023 00:09:10	node.exe
lsass.exe	996	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	05-09-2023 00:07:10	lsass.exe
wininit.exe	900	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	05-09-2023 00:07:10	wininit.exe
curlhost.exe	1749	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	05-09-2023 00:07:10	curlhost.exe

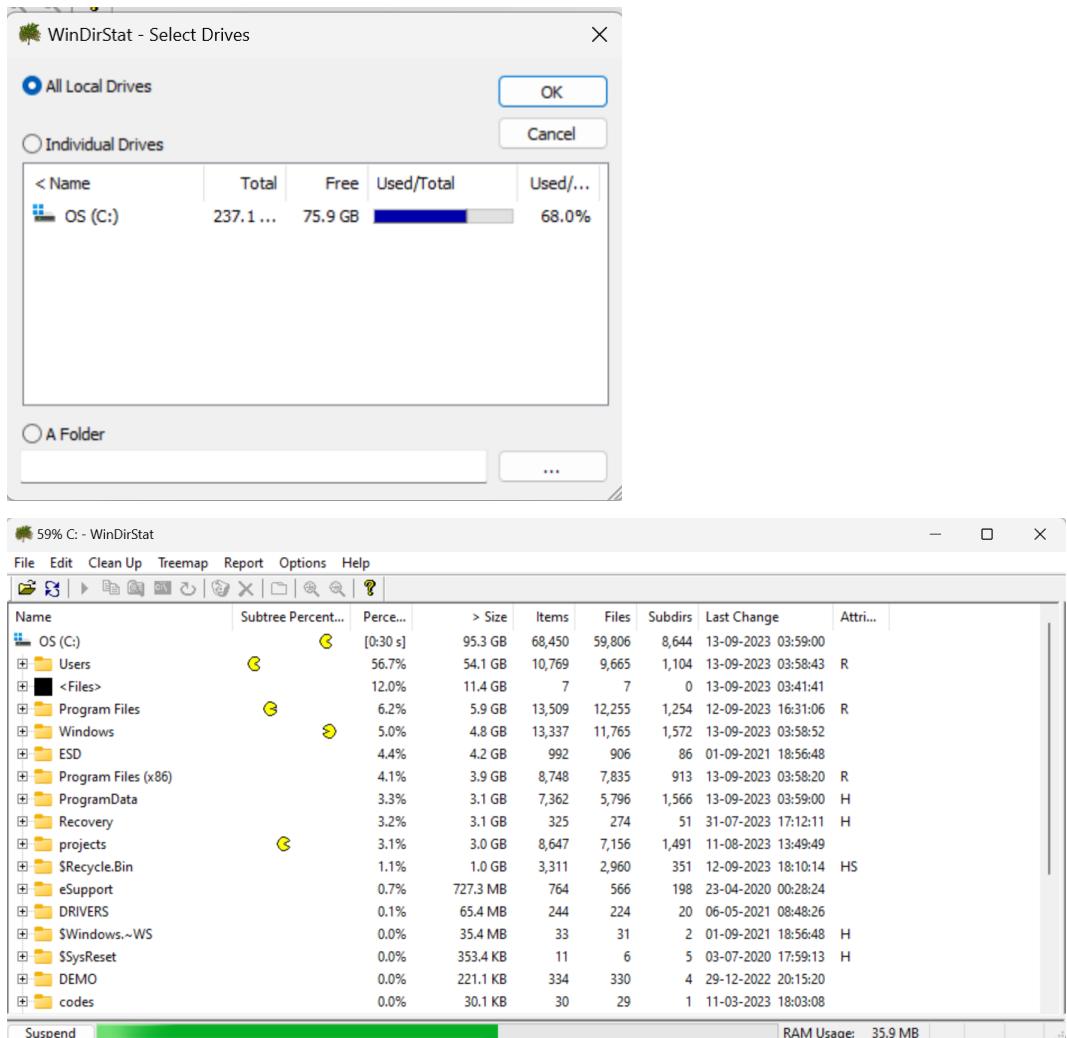
EXPERIMENT 4

Lab Objectives: windows forensics using WinDirStat/ Kdirstst and PsTools.

Install WinDirStat:

The screenshot shows the SourceForge project page for WinDirStat. The URL in the address bar is sourceforge.net/projects/windirstat/. The page features the SourceForge logo at the top left. A navigation bar includes links for New Tab, HP Connected, WhatsApp, YouTube, Python Tutorial for..., Downloads, and E-Way Bill System. The main content area displays the project's name, "WinDirStat: Windows Directory Statistics", and a brief description: "A disk usage statistics viewer and cleanup tool for Windows". It credits "Brought to you by: assarbad, frankbrandt". Below this, it shows a 5-star rating of 161 reviews, 23,812 weekly downloads, and a last update date of 2023-02-14. There are buttons for "Download", "Get Updates", and "Share This". A "Windows" tab is selected, with other tabs for "Summary", "Files", "Reviews", "Support", "Mailing Lists", "News", "Donate", "Mercurial", and "Git Clone".

The screenshot shows the "WinDirStat 1.1.2 Setup" window displaying the "License Agreement". The title bar says "WinDirStat 1.1.2 Setup". The main content area contains the text of the GNU General Public License v2. It states: "This program is distributed under the terms of the GPL v2. GNU GENERAL PUBLIC LICENSE Version 2, June 1991. Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed." Below this, a note says: "If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinDirStat 1.1.2." There is a checkbox labeled "I accept the terms in the License Agreement". At the bottom right are "Next >" and "Cancel" buttons.



Plist



Sysinternals - www.sysinternals.com

Process information for LAPTOP-8GR4A1LO:

Name	Pid	Pri	Thd	Hnd	Priv	CPU Time	Elapsed Time
Idle	0	0	16	0	60	34:32:05.718	22:00:50.656
System	4	8	276	5188	56	0:05:23.437	22:00:50.656
Registry	140	8	4	0	9240	0:00:01.031	22:00:52.449
smss	528	11	2	58	1108	0:00:00.500	22:00:50.631
csrss	864	13	12	762	2184	0:00:02.328	22:00:48.235
wininit	996	13	2	148	1588	0:00:00.046	22:00:47.602
services	1072	9	8	759	5816	0:00:11.453	22:00:47.516
lsass	1096	9	11	1792	9952	0:00:15.078	22:00:47.469
svchost	1228	8	28	1529	14332	0:00:21.046	22:00:47.264
fontdrvhost	1264	8	5	40	2408	0:00:00.312	22:00:47.248
svchost	1368	8	11	1430	10216	0:00:34.593	22:00:47.193
svchost	1420	8	7	323	3092	0:00:02.140	22:00:47.158
svchost	1576	8	4	257	3016	0:00:01.234	22:00:46.983
WUDFHost	1600	8	8	284	4428	0:00:00.937	22:00:46.971
svchost	1608	8	2	311	2112	0:00:00.109	22:00:46.970
svchost	1684	8	7	158	7572	0:00:05.359	22:00:46.937
svchost	1748	8	23	1859	8584	0:00:17.296	22:00:46.919
svchost	1856	8	7	454	19188	0:00:00.906	22:00:46.852
atiesrx	1868	8	4	198	1524	0:00:00.015	22:00:46.851
svchost	1952	8	11	323	3936	0:00:31.703	22:00:46.826
svchost	1120	8	6	421	6504	0:00:03.015	22:00:46.743
svchost	1724	8	10	355	2684	0:00:00.046	22:00:46.716
svchost	2228	8	2	196	2224	0:00:00.343	22:00:46.608
svchost	2240	8	5	238	3892	0:00:18.031	22:00:46.606
svchost	2260	8	5	231	2644	0:00:31.390	22:00:46.602
svchost	2272	8	3	246	1252	0:00:00.171	22:00:46.602
svchost	2280	8	4	178	1900	0:00:00.234	22:00:46.602
Memory Compression	2424	8	70	0	1136	0:00:35.875	22:00:46.571
svchost	2472	8	2	177	1852	0:00:00.328	22:00:46.568
svchost	2480	8	8	278	3164	0:00:04.453	22:00:46.568
svchost	2576	8	5	194	2188	0:00:00.593	22:00:46.549
svchost	2584	8	5	175	1816	0:00:03.468	22:00:46.548
svchost	2724	8	5	326	17412	0:00:28.281	22:00:46.386
svchost	2748	8	11	411	3808	0:00:01.484	22:00:46.203
svchost	2776	8	3	160	1480	0:00:00.109	22:00:46.185

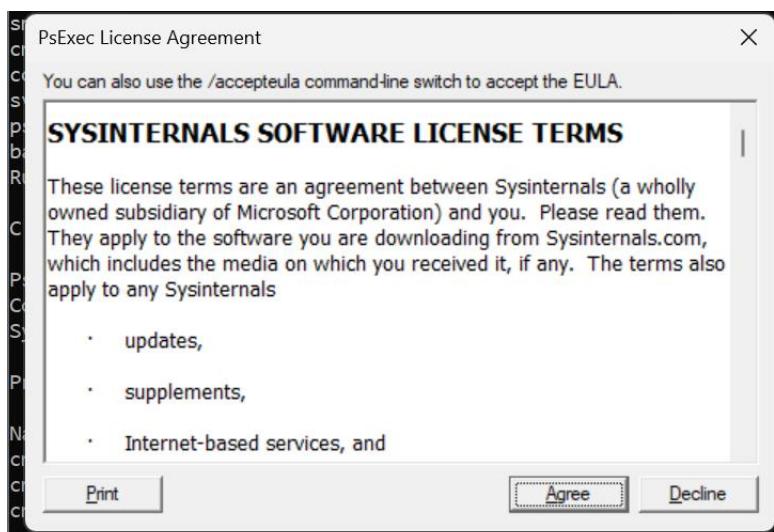
PsList v1.41 - Process information lister

Copyright (C) 2000-2023 Mark Russinovich

Sysinternals - www.sysinternals.com

Process memory detail for LAPTOP-8GR4A1LO:

Name	Pid	VM	WS	Priv	Priv	Pk	Faults	NonP	Page
cmd	12392	2151729656	3928	1900	3132	1294	4	32	
cmd	3672	2151729656	4160	1968	3120	1263	4	32	
cmd	11724	2151739196	5844	2356	5132	2834	6	51	



```
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.

Usage: psexec [\computer[,computer2[,...] | @file]][-u user [-p psswd]][-n s][-r se
rvicename][-h][-1][-s|-e][-x][-i [session]][-c [-f|-v]][-w directory][-d][-<priority
>][-g n][-a n,n,...][-verbose] cmd [arguments]
      -a          Separate processors on which the application can run with
                  commas where 1 is the lowest numbered CPU. For example,
                  to run the application on CPU 2 and CPU 4, enter:
                  "-a 2,4"
      -c          Copy the specified program to the remote system for
                  execution. If you omit this option the application
                  must be in the system path on the remote system.
      -d          Don't wait for process to terminate (non-interactive).
      -e          Does not load the specified account's profile.
      -f          Copy the specified program even if the file already
                  exists on the remote system.
      -g          Set the primary thread's processor group to the one specified
                  (Only for systems with more than 64 processors).
      -i          Run the program so that it interacts with the desktop of the
                  specified session on the remote system. If no session is
                  specified the process runs in the console session.
      -h          If the target system is Vista or higher, has the process
                  run with the account's elevated token, if available.
      -l          Run process as limited user (strips the Administrators group
                  and allows only privileges assigned to the Users group).
                  On Windows Vista the process runs with Low Integrity.
      -n          Specifies timeout in seconds connecting to remote computers.
      -p          Specifies optional password for user name. If you omit this
                  you will be prompted to enter a hidden password.
      -r          Specifies the name of the remote service to create or interact.
                  with.
      -s          Run the remote process in the System account.
```

```
PsKill v1.17 - Terminates processes on local or remote systems
Copyright (C) 1999-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Usage: pskill [-t] [\computer [-u username [-p password]]] <process ID | name>
      -t      Kill the process and its descendants.
      -u      Specifies optional user name for login to
              remote computer.
      -p      Specifies optional password for user name. If you omit this
              you will be prompted to enter a hidden password.
      -nobanner Do not display the startup banner and copyright message.
```

```
PsService v2.26 - Service information and configuration utility
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

SERVICE_NAME: AJRouter
DISPLAY_NAME: AllJoyn Router Service
Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped the AllJoyn clients that do not have their own bundled routers will be unable to run.
    TYPE          : 20 WIN32_SHARE_PROCESS
    STATE         : 1 STOPPED
                  (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 1077 (0x435)
    SERVICE_EXIT_CODE : 0 (0x0)
    CHECKPOINT     : 0x0
    WAIT_HINT      : 0 ms

SERVICE_NAME: ALG
DISPLAY_NAME: Application Layer Gateway Service
Provides support for 3rd party protocol plug-ins for Internet Connection Sharing
    TYPE          : 10 WIN32_OWN_PROCESS
    STATE         : 1 STOPPED
                  (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 1077 (0x435)
    SERVICE_EXIT_CODE : 0 (0x0)
    CHECKPOINT     : 0x0
    WAIT_HINT      : 0 ms

SERVICE_NAME: AMD External Events Utility
DISPLAY_NAME: AMD External Events Utility
    GROUP         : Event log
    TYPE          : 10 WIN32_OWN_PROCESS
    STATE         : 4 RUNNING
                  (STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE : 0 (0x0)
    SERVICE_EXIT_CODE : 0 (0x0)
    CHECKPOINT     : 0x0
    WAIT_HINT      : 0 ms
```

```
PsSuspend v1.08 - Process Suspender
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals

PsSuspend suspends or resumes processes on a local or remote NT system.

Usage: pssuspend [-r] [\RemoteComputer [-u Username [-p Password]]] <process Id or name>
  -r   Resume.
  -u   Specifies optional user name for login to
       remote computer.
  -p   Specifies optional password for user name. If you omit this
       you will be prompted to enter a hidden password.
  -nobanner Do not display the startup banner and copyright message.
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	10.7.14.148:52876	relay-61f2512e:https	ESTABLISHED
TCP	10.7.14.148:52878	20.198.118.190:https	ESTABLISHED
TCP	10.7.14.148:52977	20.187.186.89:https	ESTABLISHED
TCP	10.7.14.148:53575	a104-90-7-81:https	CLOSE_WAIT
TCP	10.7.14.148:53577	a104-90-7-178:https	CLOSE_WAIT
TCP	10.7.14.148:53578	a104-90-7-178:https	CLOSE_WAIT
TCP	10.7.14.148:53579	a104-90-7-83:https	CLOSE_WAIT
TCP	10.7.14.148:53580	a104-90-7-83:https	CLOSE_WAIT
TCP	10.7.14.148:53581	a104-90-7-83:https	CLOSE_WAIT
TCP	10.7.14.148:53582	a104-90-7-83:https	CLOSE_WAIT
TCP	10.7.14.148:53583	a104-90-7-81:https	CLOSE_WAIT
TCP	10.7.14.148:53587	se-in-f188:5228	ESTABLISHED
TCP	10.7.14.148:53592	ec2-3-6-163-125:https	ESTABLISHED
TCP	10.7.14.148:53596	a104-90-7-81:https	LAST_ACK
TCP	10.7.14.148:53599	a104-90-7-123:https	CLOSE_WAIT

Interface: 10.7.14.148 --- 0x2

Internet Address	Physical Address	Type
10.7.1.1	f8-b1-56-33-55-7d	dynamic
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

EXPERIMENT 5

Install FTK Imager

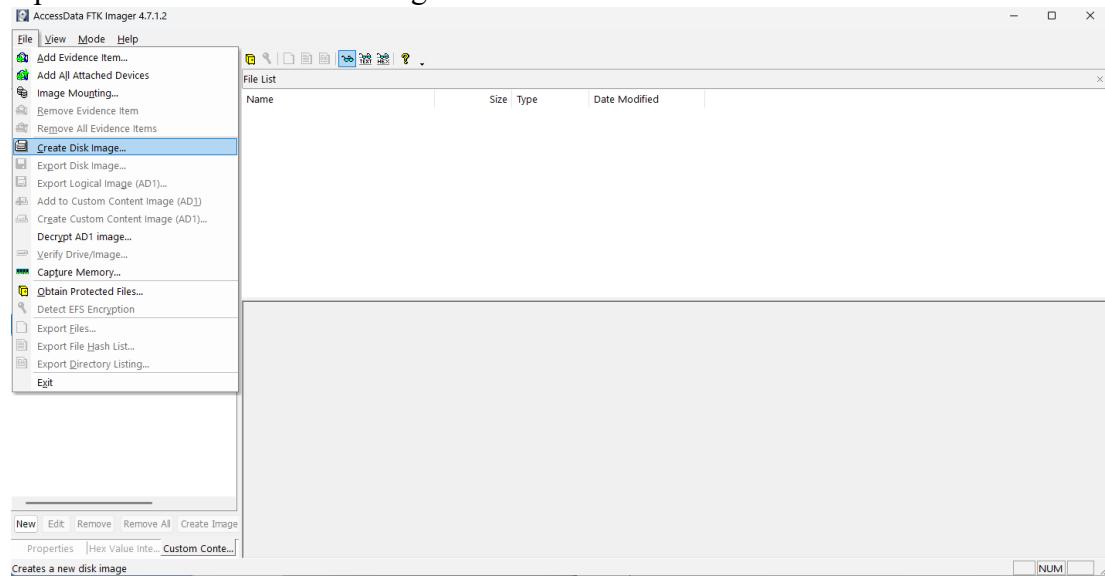
The screenshot shows the exterro.com website with a dark header bar. On the left, there's a logo for "exterro" with the tagline "Legal GRC Software Platform". To the right are navigation links: PRODUCTS, MARKETS, RESOURCES, TRAINING, PARTNERS, ABOUT, LEGAL GRC, STORE, and a "Get Demo" button. A search icon is also present. Below the header, a blue banner features a "Download FTK® Imager Now!" button. The main content area includes a "Get Started with FTK® Imager" section with a "Download FTK® Imager" button and a thumbnail image of a person using a magnifying glass. To the right, a box titled "WHAT CUSTOMERS ARE SAYING" contains a testimonial from "TOM ANGLE" about the software's speed and reliability. Another section below is titled "Do Even More with FTK® Forensic Toolkit".

Installing

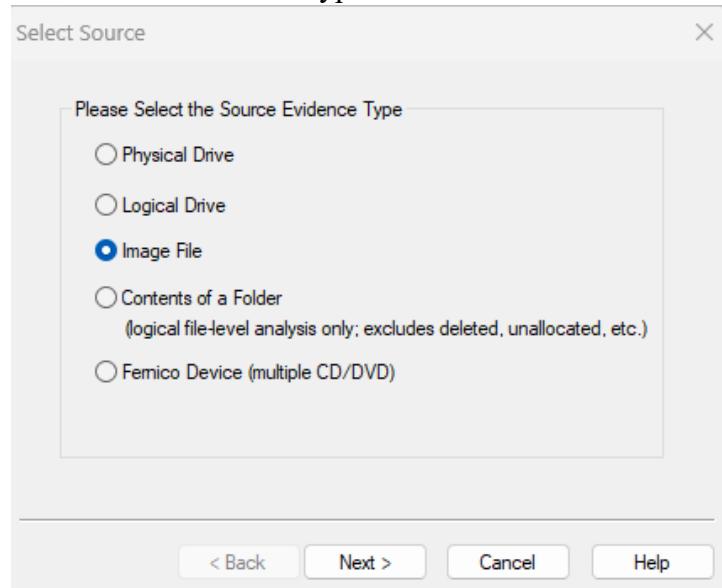
The screenshot shows the "AccessData FTK Imager - InstallShield Wizard" window. It displays a progress bar at the top indicating the setup is preparing the InstallShield Wizard. The main text area says "Extracting: AccessData_FTK_Imager_(x64).msi". Below this, a message states "InstallShield Wizard Completed" and informs the user that the installation was successful. There is a checkbox labeled "Launch AccessData FTK Imager" which is checked. At the bottom, there are buttons for "< Back", "Finish", and "Cancel".

Executing FTK Imager

Open File -> Create Disk Storage



Select source evidence type



Select source type to clone information from

Evidence Item Information

Case Number:	1
Evidence Number:	12
Unique Description:	
Examiner:	
Notes:	

< Back Next > Cancel Help

Select source drive of which you want to clone data from

Select Image Type

Please Select the Destination Image Type

Raw (dd)
 SMART
 E01
 AFF

< Back Next > Cancel Help

Select the type of image in which you want to clone data

Select Image Destination

Image Destination Folder
C:\Users\Sanskrit\Desktop

Image Filename (Excluding Extension)
LAB5

Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 6

Use AD Encryption

< Back Finish Cancel Help

Add a destination folder where you want to store the cloned image and start the process

SIMPLY IMAGE
DATE: 11/01/2024

Creating Image...

Image Source: C:\Users\Sanskrit\Desktop\DIGITAL FORENSIC 1 LAB\DF1 LAB

Destination: C:\Users\Sanskrit\Desktop\LABS

Status: Image created successfully

Progress [Green Bar]

Elapsed time: 0:00:00

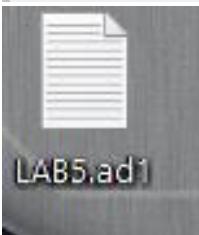
Estimated time left:

[Image Summary...](#) [Close](#)

Drive/Image Verify Results

Name	LAB5.ad1
MD5 Hash	
Computed hash	393c06d0116b4a586cdcc9c9682a7a05
Report Hash	393c06d0116b4a586cdcc9c9682a7a05
Verify result	Match
SHA1 Hash	
Computed hash	c76691e190cc9597845d1f437f3fed42f4e736
Report Hash	c76691e190cc9597845d1f437f3fed42f4e736
Verify result	Match

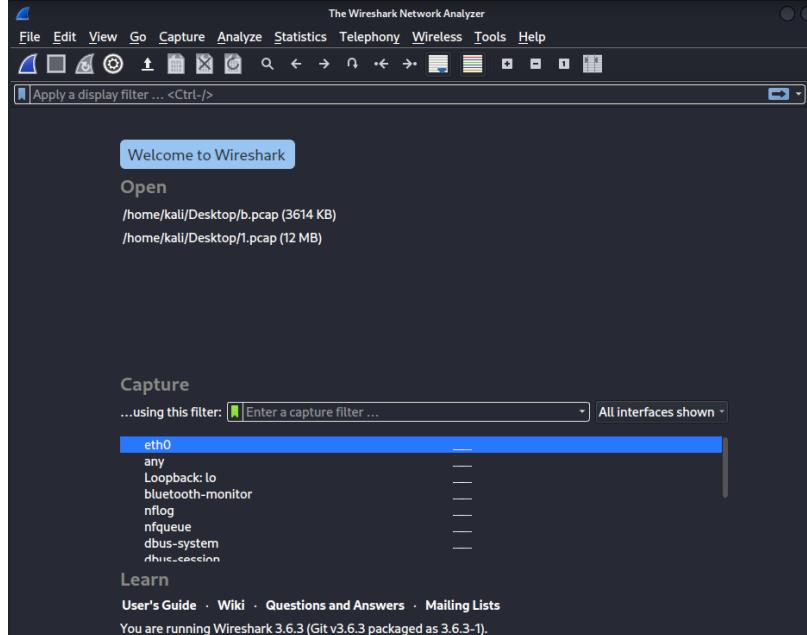
[Close](#)



EXPERIMENT 6

- 1) First, we will open **Wireshark** for tracing the packets in Kali Linux
Click on eth0

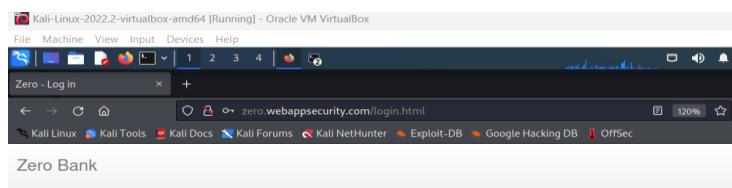
Open **zero.webappsecurity.com** in firefox



2) Capture the packets

Then , we click on eth0 for start tracking the website packets , and at the same time we try to perform sql injection on website **zero.webappsecurity.com** to track the packets of login try attempt also .

We try to perform SQL Injection on the website zero.webappsecurity.com by entering login as **admin' --** and Password as '**or 1=1--**



Log in to ZeroBank

Login

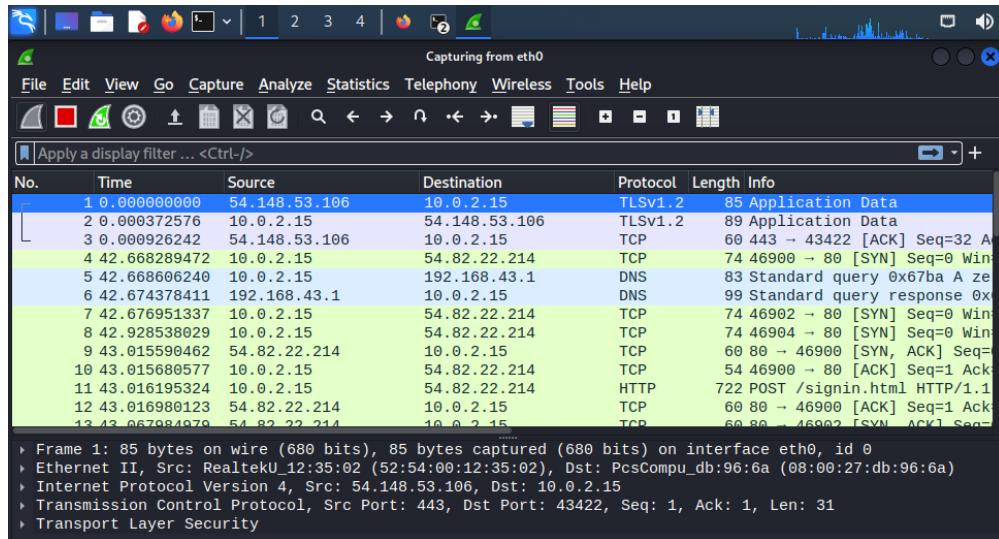
Password

Keep me signed in

This connection is not secure.
Logins entered here could be compromised. [Learn More](#)

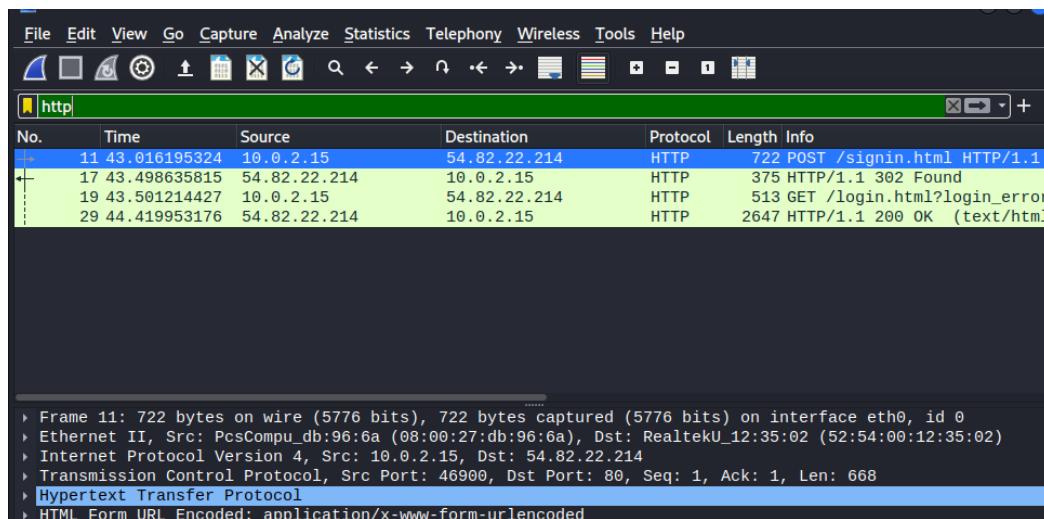
[Forgot your password ?](#)

After trying wireshark packet tracking , we get the packets which are listed below.

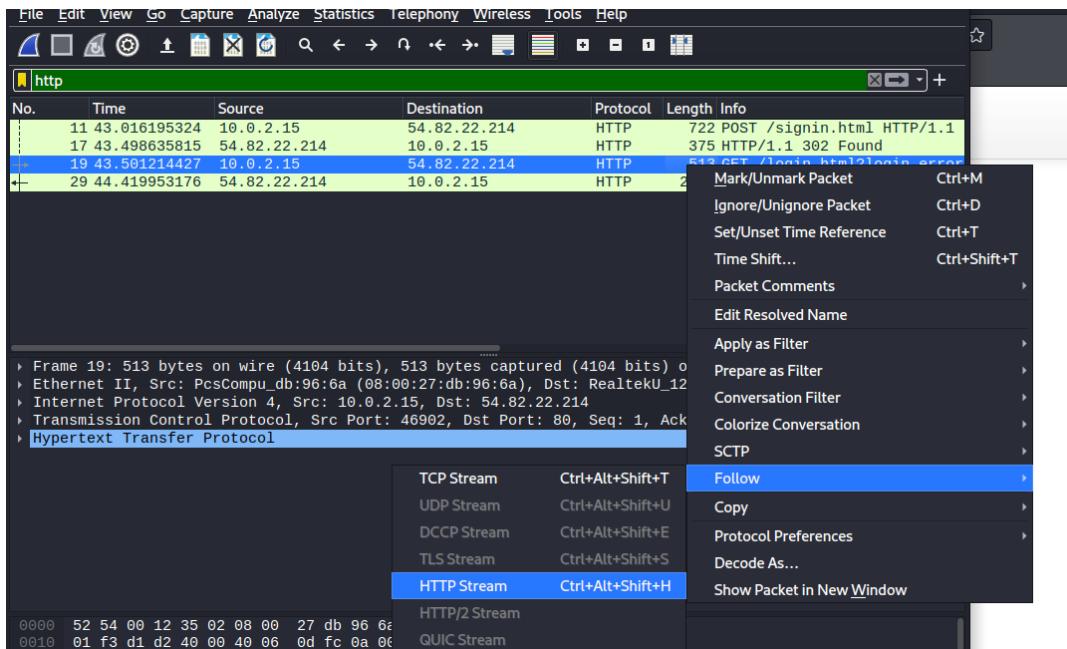


3) Check the login values

But , we want to get the packet trace of just sign in , which we can see in above screenshot
sign in is working on **http** . So we apply a filter of http and as we get what we wanted so we stop the Wireshark by clicking on red button which is shown in the above screenshot.



And then we right click on S.no. 19 which is based on login and then we click on **follow** and then we click on **Http Stream**



We get following detail after doing things .

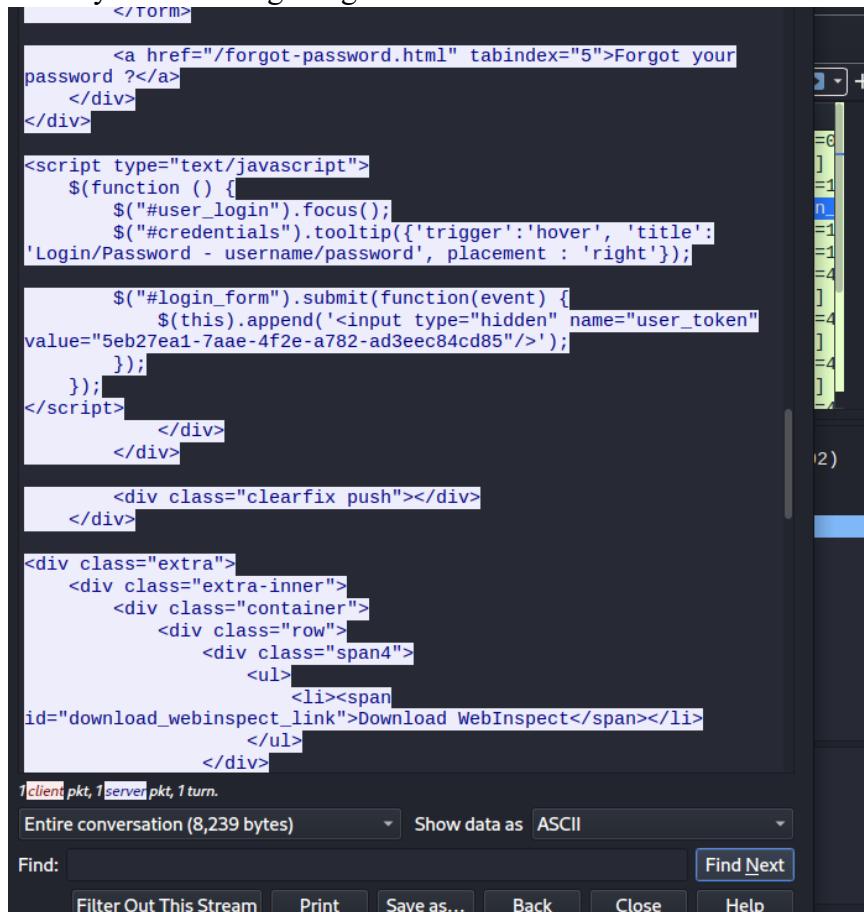
```

GET /login.html?login_error=true HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://zero.webappsecurity.com/login.html?login_error=true
Connection: keep-alive
Cookie: JSESSIONID=ACA35613
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Mon, 05 Dec 2022 07:14:07 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked

```

But as I scroll down to looking if username and passwords are written in Http Stream , I actually found the right login credentials of that website .



The screenshot shows the NetworkMiner tool interface. The main pane displays an HTML file with various script and CSS elements. A specific section of the code is highlighted, showing a JavaScript function that handles a login form submission. The function appends a hidden input field named "user_token" with the value "5eb27ea1-7aae-4f2e-a782-ad3eec84cd85". Below this, there's a link to download WebInspect. At the bottom of the tool, there are buttons for "Find Next" and other options like "Filter Out This Stream", "Print", "Save as...", "Back", "Close", and "Help".

```
</form>
<a href="/forgot-password.html" tabindex="5">Forgot your password ?</a>
</div>
</div>

<script type="text/javascript">
$(function () {
    $("#user_login").focus();
    $("#credentials").tooltip({'trigger':'hover', 'title':'Login/Password - username/password', placement : 'right'});
}

    ("#login_form").submit(function(event) {
        $(this).append('<input type="hidden" name="user_token" value="5eb27ea1-7aae-4f2e-a782-ad3eec84cd85"/>');
    });
})
</script>
</div>
</div>

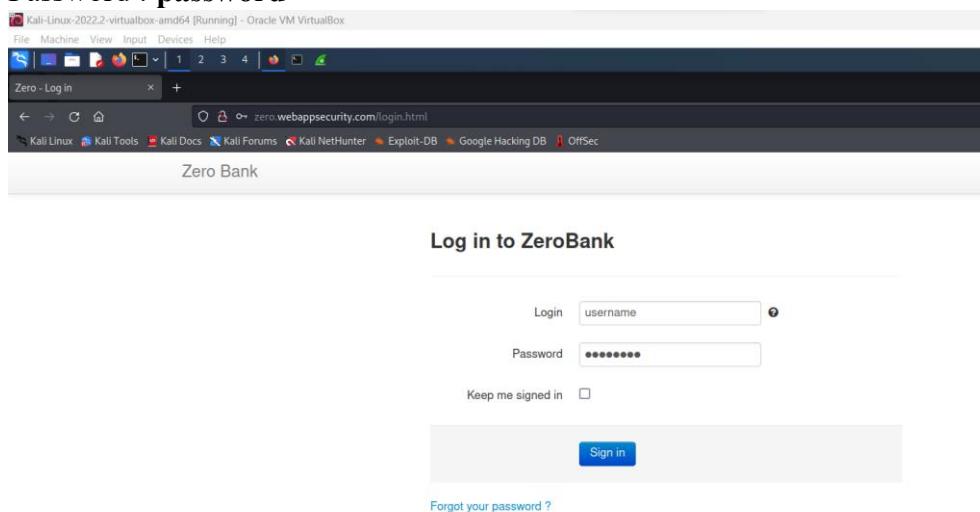
<div class="clearfix push"></div>
</div>

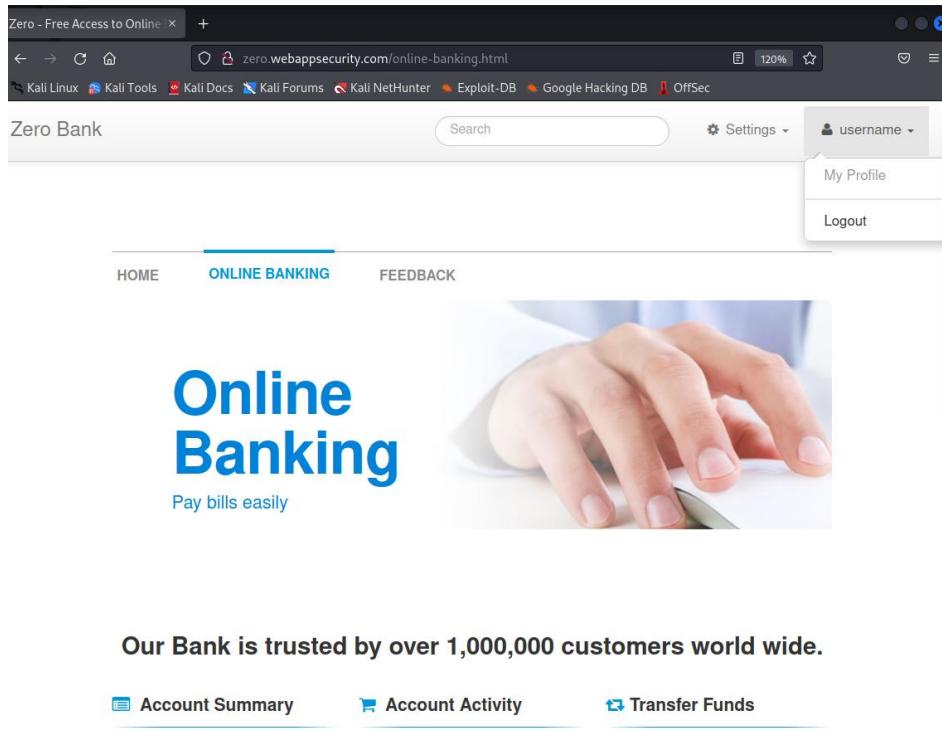
<div class="extra">
<div class="extra-inner">
<div class="container">
<div class="row">
<div class="span4">
<ul>
<li><span id="download_webinspect_link">Download WebInspect</span></li>
</ul>
</div>
</div>
</div>
</div>
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (8,239 bytes) Show data as ASCII
Find: Find Next
Filter Out This Stream Print Save as... Back Close Help
```

I tried entering the username and password to website and it worked .

Login : **username**

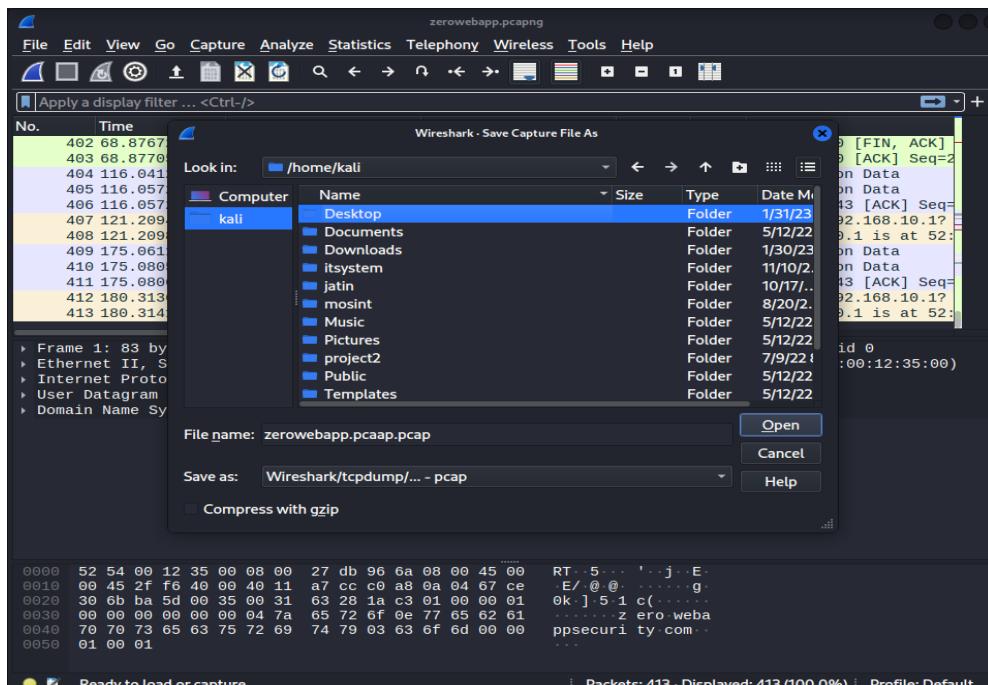
Password : **password**





4) Use A-packets

We click on red Button stop , and then save with file name as testfire.pcap



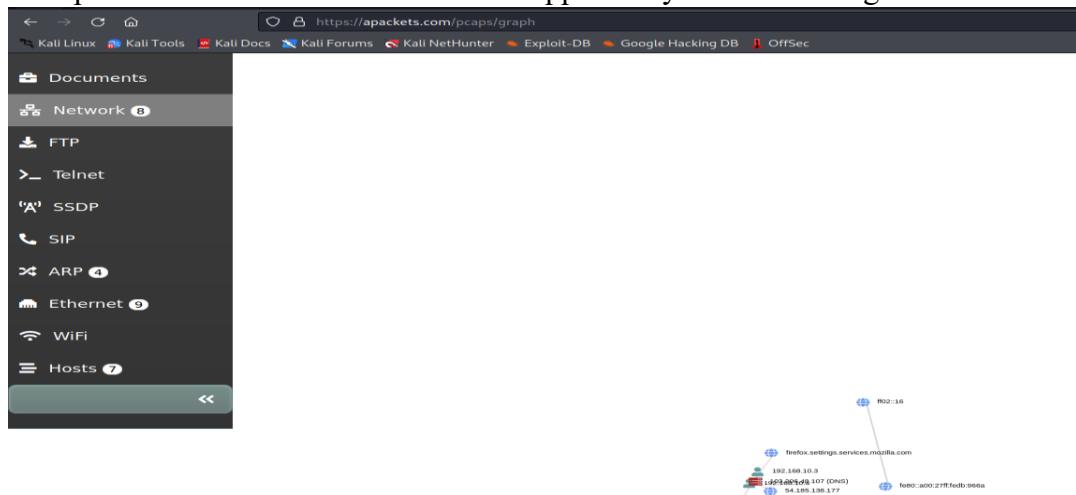
Now , we go to apackets.com and upload that file .

The screenshot shows the apackets.com upload interface. At the top, there's a header with links to Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the header, a large button says "Upload pcap or pcapng file". A sub-instruction below the button reads "to analyze network structure, HTTP headers and data, FTP, Telnet, WiFi, ARP, SSDP and other". On the left, there's a section for dragging files or selecting them from a device. On the right, a box titled "PUBLIC UPLOAD!" informs users that their files and analysis reports will be visible to anyone after processing, with a "Choose Plan" button. A green progress bar at the bottom indicates "Processing zerowebapp.pcap completed. view report".

And here we go , after viewing reports , we can find lot of information such as Found Credentials , DNS Queries , Network Route and much more.

The screenshot shows the apackets.com analysis interface for the file "zerowebapp.pcap". The left sidebar has a tree view with categories like Pcaps List, Overview, Credentials, DNS, HTTP Headers, Connections, Open ports, Pictures, HTTP, SMB, Servers, Documents, Network, FTP, Telnet, SSDP, SIP, ARP, Ethernet, and WiFi. The main area is titled "zerowebapp.pcap Overview" and contains a grid of 14 modules: Found credentials, DNS Queries, HTTP Communication, SMB Sniffer, ARP, Network Map, Open Ports, Images, Telnet, and FTP. Below this grid are two rows of four modules each: SSDP announces, Connections, DNS, DHCP and LDAP Servers, Ethernet Devices, WiFi, SIP, and Documents. Each module has a small icon and a brief description.

We open the Network Route of zero.webappsecurity.com which is given below.



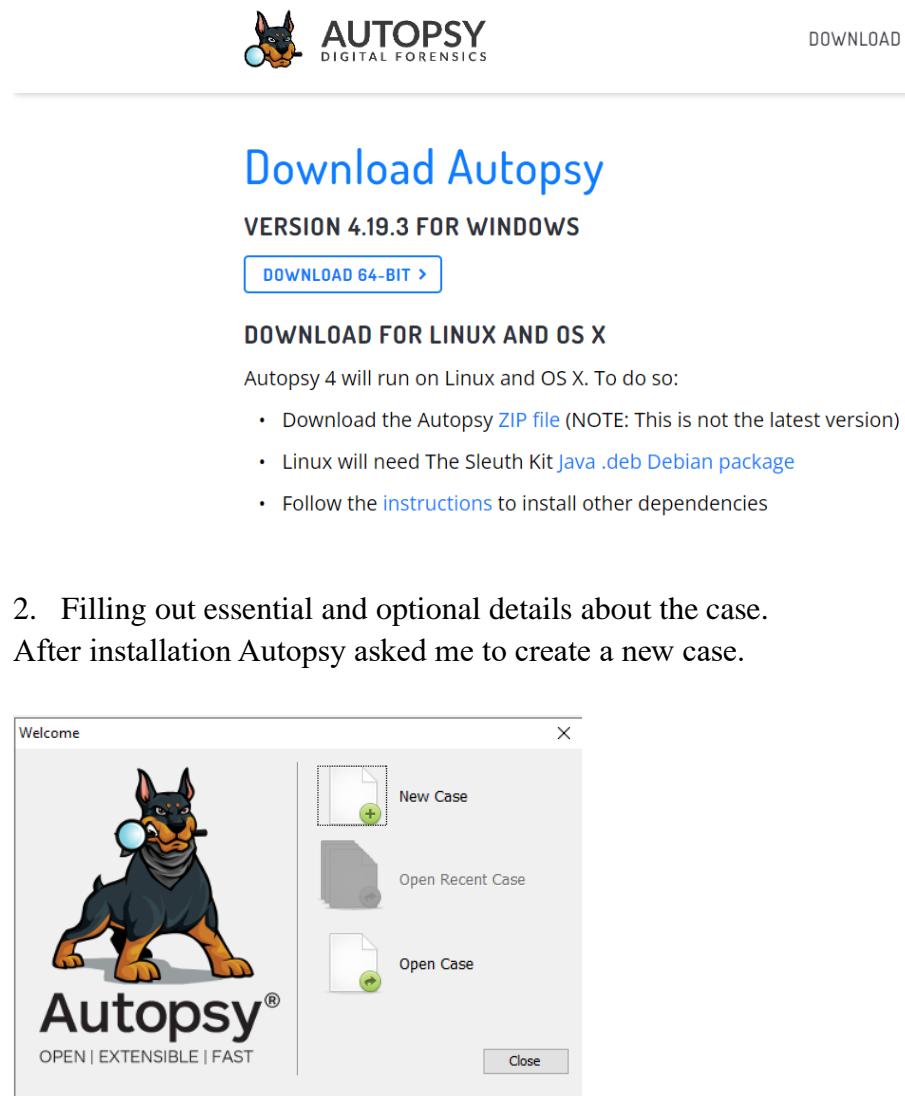
EXPERIMENT 7

Lab Objective: Data Acquisition using Autopsy

Steps:

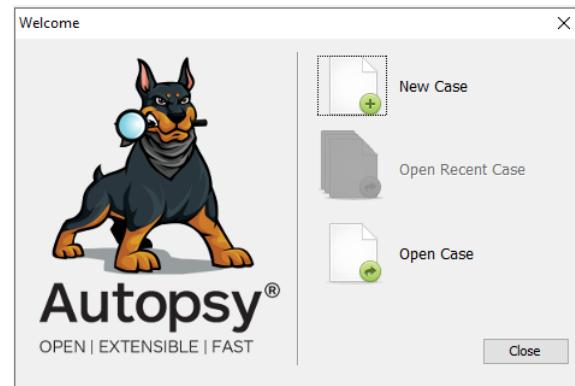
1. Download and install Autopsy.

Downloading of Autopsy was done from the official website of Autopsy.



The screenshot shows the official Autopsy website's download section. At the top, there is a logo featuring a cartoon dog wearing a mask and the word "AUTOPSY" with "DIGITAL FORENSICS" below it. To the right of the logo is a "DOWNLOAD" button. Below the logo, the text "Download Autopsy" is displayed in blue, followed by "VERSION 4.19.3 FOR WINDOWS". A blue "DOWNLOAD 64-BIT >" button is centered below this text. Further down, the section "DOWNLOAD FOR LINUX AND OS X" is shown, with instructions for running Autopsy on Linux and OS X. It includes a bulleted list of steps: "Download the Autopsy ZIP file (NOTE: This is not the latest version)", "Linux will need The Sleuth Kit Java .deb Debian package", and "Follow the instructions to install other dependencies".

2. Filling out essential and optional details about the case.
After installation Autopsy asked me to create a new case.



The screenshot shows the Autopsy welcome screen. On the left, there is a large logo of a Doberman Pinscher with the word "Autopsy" in a stylized font below it, with the tagline "OPEN | EXTENSIBLE | FAST" underneath. On the right, there are three main options: "New Case" (represented by a document icon with a plus sign), "Open Recent Case" (represented by a stack of documents icon), and "Open Case" (represented by a document icon with a circular arrow). At the bottom right of the screen is a "Close" button.

After creating a new case Autopsy asked me for the details related to the case.

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

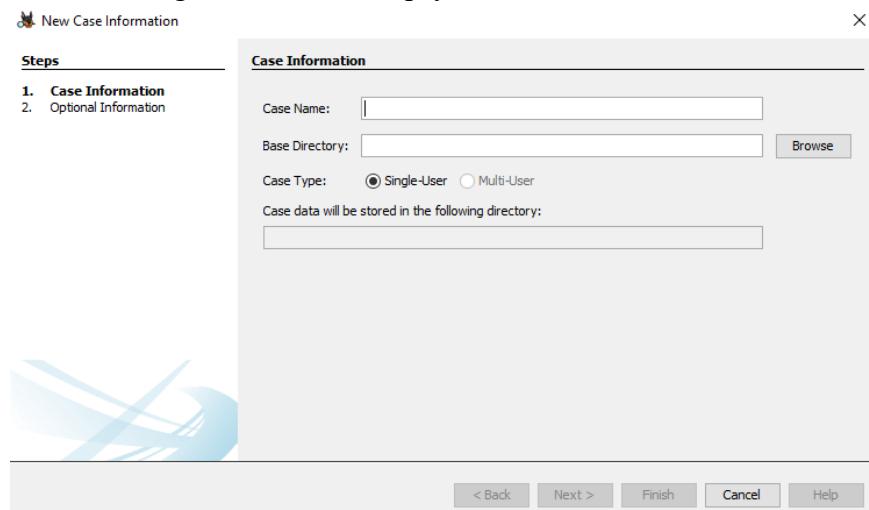
Case Name:

Base Directory:

Case Type: Single-User Multi-User

Case data will be stored in the following directory:

< Back Help



New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number:

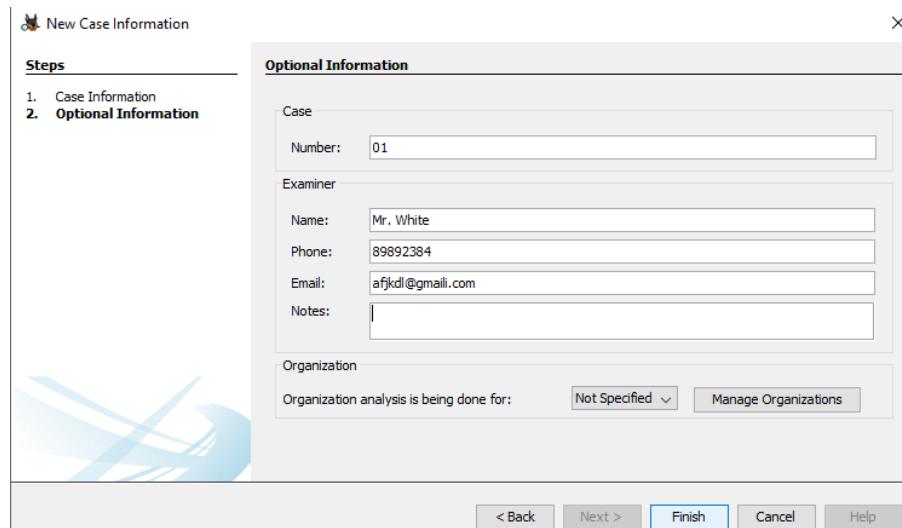
Examiner

Name:
Phone:
Email:
Notes:

Organization

Organization analysis is being done for:

< Back Help

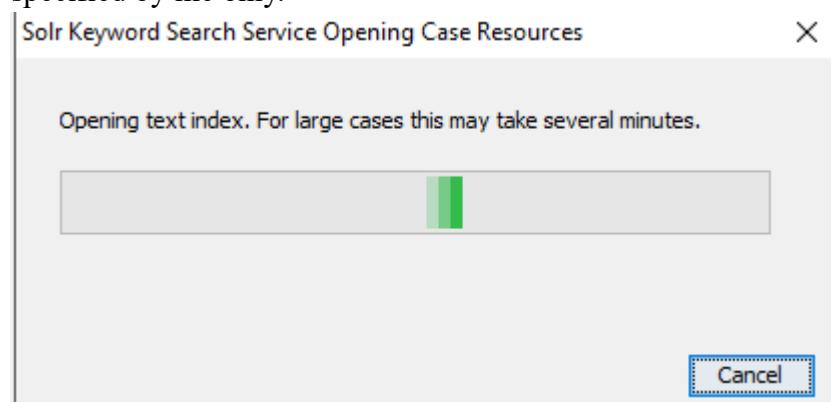


After filling essential and optional information. Autopsy created a database in the folder specified by me only.

Solr Keyword Search Service Opening Case Resources

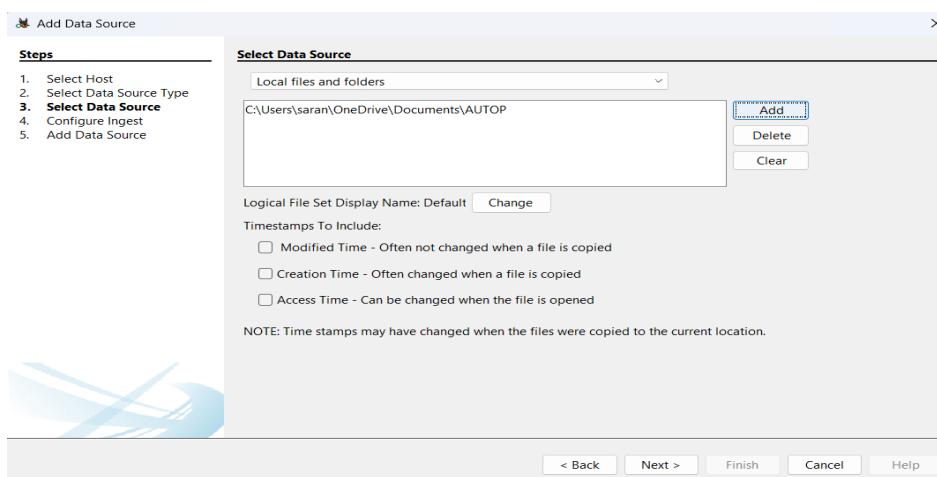
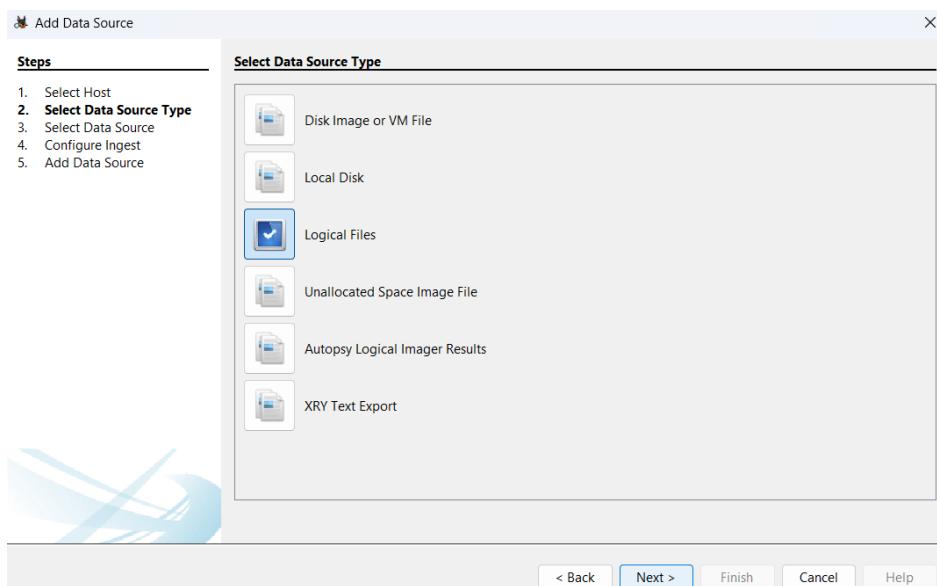
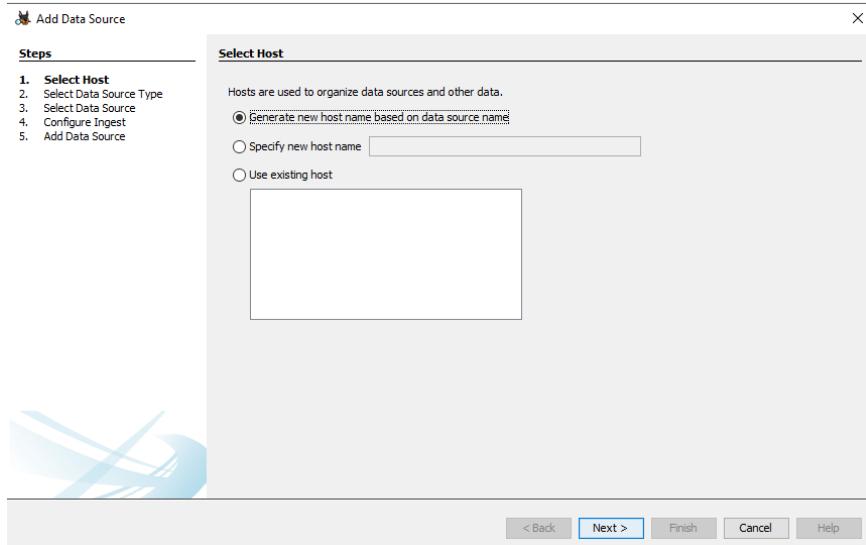
Opening text index. For large cases this may take several minutes.

Cancel

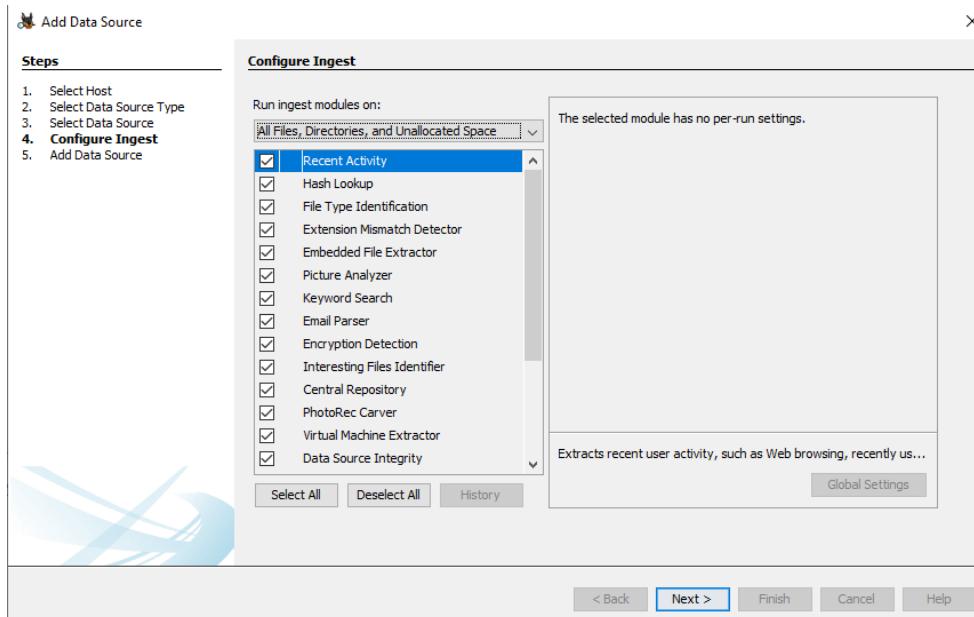


3. Selecting the evidence disk and starting the analysis.

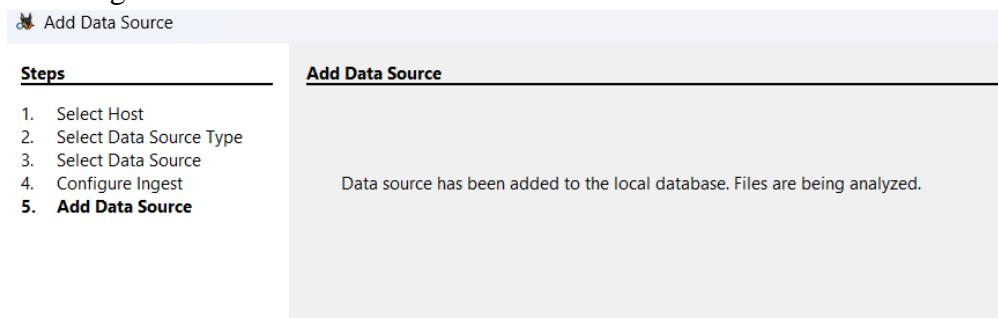
Now, I needed to selected a file or drive as my evidence on which I need to perform.



Autopsy can also apply filters. To search for a specific file.



Scanning started.



After scanning Autopsy was able to find file with extensions.

a) .jpg , .png

The screenshot shows the main Autopsy interface. The left sidebar includes 'Data Sources', 'File Views', 'File Types' (with 'By Extension' expanded to show 'Images (29)', 'Videos (0)', 'Audio (0)', 'Archives (0)', 'Text (0)', 'Documents (0)', 'Executable (0)', 'By File Type' (with 'Deleted Files (0)' expanded to show 'image01.jpg', 'image02.jpg', etc.), 'MB File Size (0)', 'Data Artifacts (0)', 'Analysis Results (0)', 'OS Accents (0)', 'Tags (0)', and 'Score (0)'). The central area shows a table of file analysis results with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, FlagDir, and Flag. There are 29 results. Below the table is a detailed view of a file's metadata, showing sections like 'Hex', 'Text', 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. The 'File Metadata' tab is active, displaying a large amount of technical data.

b) OFFICE

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meti)
Experiment 3.docx	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	678304	Allocated	Allocated
Experiment 4.docx	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1089015	Allocated	Allocated
LAB 1-- DCCN.docx	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	678284	Allocated	Allocated

c) PDF

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meti)
12th board result PDF.pdf	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	244133	Allocated	Allocated
lab2.pdf	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	312153	Allocated	Allocated

d) .exe

Name	S	C	O	Modified Time	Change Time	Access Time
t32.exe	0	2022-08-27 14:34:16 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
h64.exe	0	2022-08-27 14:34:16 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
w32.exe	0	2022-08-27 14:34:16 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
w64.exe	0	2022-08-27 14:34:16 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
d32.exe	1	2022-08-27 14:34:14 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
d64.exe	0	2022-08-27 14:34:14 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
d1.exe	1	2022-08-27 14:34:14 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
g1a-32.exe	1	2022-08-27 14:34:14 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
g1i-64.exe	0	2022-08-27 14:34:14 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
g1i.exe	1	2022-08-27 14:34:14 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
estimator_dclpt_converter.exe	0	2022-08-27 14:43:06 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
Favr.exe	0	2022-08-27 14:41:34 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
google-oauthlib-tool.exe	0	2022-08-27 14:41:36 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
import_pb_to_tensorboard.exe	0	2022-08-27 14:45:00 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
markdown_py.exe	0	2022-08-27 14:41:34 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
ntk.exe	0	2022-08-27 14:45:06 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
normalizer.exe	0	2022-08-27 14:41:12 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
pip.exe	1	2022-08-27 14:34:22 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
pip3.9.exe	1	2022-08-27 14:34:22 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
pip3.exe	1	2022-08-27 14:34:22 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		
nvraa-decrypt.exe	0	2022-08-27 14:41:14 IST	0000-00-00 00:00:00	2022-08-29 00:00:00 IST		

e) File Size

The screenshot shows the Autopsy Forensic Browser interface. On the left, there's a tree view of file types: File Types (By Extension: Images (29), Videos (0), Audio (0), Archives (0), Databases (0); By MIME Type: application, image; Deleted Files: File System (0), All (0)); MB File Size: MB 50 - 200MB (0), MB 200MB - 1GB (0), MB 1GB+ (0)). The right pane is titled 'File size' and contains tabs for Table, Thumbnail, and Summary. Under 'Size Range', it lists 'MB 50 - 200MB (0)', 'MB 200MB - 1GB (0)', and 'MB 1GB+ (0)'.

4. Final Report

Final report can be generated in HTML form.

The screenshot shows the Autopsy interface with a 'Generate Report' button highlighted. A modal dialog box titled 'Report Generation Progress...' shows a green progress bar at 100% completion. The message 'HTML Report : C:\Users\saran\CRIMES\Reports\CRIMES HTML Report 10-18-2023-13-42-15\report.html' is displayed, followed by 'Complete'. There are 'Cancel' and 'Close' buttons at the bottom.

The screenshot shows the generated 'Autopsy Forensic Report' in HTML format. The top bar includes 'Import favorites' and 'rewardsss'. The main content is divided into sections: 'Report Navigation' (Case Summary, Metadata (5), Tagged Files (0), Tagged Images (0), Tagged Results (0)), 'Autopsy Forensic Report' (Case: CRIMES, Case Number: 01, Number of data sources in case: 1, Examiner: Mr.White), 'Image Information:' (LogicalFileSet1), and 'Software Information:' (Autopsy Version: 4.21.0, various other modules listed). The page footer says 'HTML Report Generated on 2023/10/18 13:42:15'.

EXPERIMENT 8

Lab Objective: Exploration of Digital Forensics Tools in Kali Linux

1.BULK WALK

```
[root@kali]~[/home/crimsonwings]
# binwalk -e --run-as=root TL-WR710N_V2.1_150507.zip

DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----      -----
0            0x0      Zip archive data, at least v2.0 to extract, compressed size: 3802215, uncompressed size: 8258048, name: w
(150507).bin    0x3A04B2      Zip archive data, at least v2.0 to extract, compressed size: 242353, uncompressed size: 259952, name: How
Router.pdf     0x3DB8AC      End of Zip archive, footer length: 22
```

```
[root@kali]~[/home/crimsonwings/_TL-WR710N_V2.1_150507.zip.extracted]
# ls
0.zip 'How to upgrade TP-LINK Wireless N Router.pdf' 'wr710nv2_fs_uk_8M_3_16_12_up_boot(150507).bin'
```

```
[root@kali]~[/home/crimsonwings]
# wget http://digitalcorpora.org/downloads/bulk_extractor/
--2022-11-03 11:45:27--  http://digitalcorpora.org/downloads/bulk_extractor/
Resolving digitalcorpora.org (digitalcorpora.org) ... 173.236.181.133
Connecting to digitalcorpora.org (digitalcorpora.org)|173.236.181.133|:80 ... connected.
HTTP request sent, awaiting response ... 302 Found
Location: https://digitalcorpora.org/downloads/bulk_extractor/ [following]
--2022-11-03 11:45:29--  https://digitalcorpora.org/downloads/bulk_extractor/
Connecting to digitalcorpora.org (digitalcorpora.org)|173.236.181.133|:443 ... connected.
HTTP request sent, awaiting response ... 302 Found
Location: http://downloads.digitalcorpora.org/downloads/bulk_extractor/ [following]
--2022-11-03 11:45:31--  http://downloads.digitalcorpora.org/downloads/bulk_extractor/
Resolving downloads.digitalcorpora.org (downloads.digitalcorpora.org) ... 173.236.181.133
Connecting to downloads.digitalcorpora.org (downloads.digitalcorpora.org)|173.236.181.133|:80 ... connected.
HTTP request sent, awaiting response ... 301 Moved Permanently
Location: https://downloads.digitalcorpora.org/downloads/bulk_extractor/ [following]
--2022-11-03 11:45:33--  https://downloads.digitalcorpora.org/downloads/bulk_extractor/
Connecting to downloads.digitalcorpora.org (downloads.digitalcorpora.org)|173.236.181.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 11453 (11K) [text/html]
Saving to: 'index.html'

index.html          100%[=====]
```

2. BULK EXTRACTOR

```
[root@kali]~[/home/crimsonwings]
# bulk_extractor -o bulk-out/ index.html
bulk_extractor version: 2.0.0
Input file: "index.html"
Output directory: "bulk-out/"
Disk Size: 11453
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml_carved msxml net ntfsindx
winlnk winpPrefetch zip accts email gps
Threads: 4
going multi-threaded ... ( 4 )
bulk_extractor      Thu Nov  3 11:52:22 2022

available_memory: 7340679168
bytes_queued: 0
depth0_bytes_queued: 0
depth0_sbufs_queued: 0
elapsed_time: 0:00:00
estimated_date_completion: 2022-11-03 11:52:21
estimated_time_remaining: n/a
fraction_read: 0.000000 %
max_offset: 0
sbufs_created: 0
sbufs_queued: 0
sbufs_remaining: 0
tasks_queued: 0
thread_count: 4
>.....
```

```

└─(root㉿kali)-[~/home/kali/_TL-WR710N_V2.1_150507.zip.extracted]
# wget http://downloads.digitalcorpora.org/downloads/bulk_extractor
--2022-11-03 02:27:48-- http://downloads.digitalcorpora.org/downloads/bulk_extractor
Resolving downloads.digitalcorpora.org (downloads.digitalcorpora.org) ... 173.236.181.133
Connecting to downloads.digitalcorpora.org (downloads.digitalcorpora.org)|173.236.181.133|:80 ...
HTTP request sent, awaiting response ... 301 Moved Permanently
Location: https://downloads.digitalcorpora.org/downloads/bulk_extractor [following]
--2022-11-03 02:27:50-- https://downloads.digitalcorpora.org/downloads/bulk_extractor
Connecting to downloads.digitalcorpora.org (downloads.digitalcorpora.org)|173.236.181.133|:443 ...
HTTP request sent, awaiting response ... 200 OK
Length: 11453 (11K) [text/html]
Saving to: 'bulk_extractor'

bulk_extractor          100%[=====] 11.18K --.-KB/s   in 0s

2022-11-03 02:27:52 (48.6 MB/s) - 'bulk_extractor' saved [11453/11453]

```

3. P0f

```

└─(root㉿kali)-[~/home/crimsonwings]
# apt install p0f
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  p0f
0 upgraded, 1 newly installed, 0 to remove and 228 not upgraded.
Need to get 81.0 kB of archives.
After this operation, 224 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 p0f amd64 3.09b-1
Fetched 81.0 kB in 3s (25.4 kB/s)
Selecting previously unselected package p0f.
(Reading database ... 311160 files and directories currently installed.)
Preparing to unpack .../archives/p0f_3.09b-3_amd64.deb ...
Unpacking p0f (3.09b-3) ...
Setting up p0f (3.09b-3) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.3.1) ...

```

```

-[ 192.168.209.128/49846 → 195.42.179.202/443 (syn) ]-
client    = 192.168.209.128/49846
os        = Linux 2.2.x-3.x
dist      = 0
params   = generic
raw_sig   = 4:64+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df,id+:0
`-- System

-[ 192.168.209.128/49846 → 195.42.179.202/443 (mtu) ]-
client    = 192.168.209.128/49846
link      = Ethernet or modem
raw_mtu   = 1500
`-- 

-[ 192.168.209.128/49846 → 195.42.179.202/443 (syn+ack) ]-
server    = 195.42.179.202/443
os        = ???
dist      = 0
params   = none
raw_sig   = 4:128+0:0:1460:mss*44,0:mss::0
`-- 

-[ 192.168.209.128/49846 → 195.42.179.202/443 (mtu) ]-
server    = 195.42.179.202/443
link      = Ethernet or modem
raw_mtu   = 1500
`-- 

```

```
[root@kali]~]# p0f -i eth0 -p -o p0f.log
— p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> —

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[-] PROGRAM ABORT : 'p0f.log' is being used by another process.
```

4. BINWALK

Binwalk is a tool for searching a given binary image for embedded files and executable code. Specifically, it is designed for identifying files and code embedded inside of firmware images.

```
[kali㉿kali]~]# sudo wget https://static.tp-link.com/res/down/soft/TL-WR710N_V2.1_150507.zip
[sudo] password for kali:
--2022-11-03 02:10:02-- https://static.tp-link.com/res/down/soft/TL-WR710N_V2.1_150507.zip
Resolving static.tp-link.com (static.tp-link.com) ... 108.158.221.35, 108.158.221.38, 108.158.221.59, ...
Connecting to static.tp-link.com (static.tp-link.com)|108.158.221.35|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 4044994 (3.9M) [application/x-zip-compressed]
Saving to: 'TL-WR710N_V2.1_150507.zip'

TL-WR710N_V2.1_150507.zip      100%[=====] 3.86M 3.41MB/s   in 1.1s
2022-11-03 02:10:03 (3.41 MB/s) - 'TL-WR710N_V2.1_150507.zip' saved [4044994/4044994]
```

```
[root@kali]~]# binwalk -e --run-as=root TL-WR710N_V2.1_150507.zip
DECIMAL      HEXADECIMAL      DESCRIPTION
_____
0            0x0      Zip archive data, at least v2.0 to extract, compressed size: 3802215, uncompressed size: 82580
48, name: wr710nv2_fs_uk_8M_3_16_12_up_boot(150507).bin
3802290      0x3A04B2      Zip archive data, at least v2.0 to extract, compressed size: 242353, uncompressed size: 259952
, name: How to upgrade TP-LINK Wireless N Router.pdf
4044972      0x3DB8AC      End of Zip archive, footer length: 22
```

```
[root@kali]~]# cd _TL-WR710N_V2.1_150507.zip.extracted
[root@kali]~/_TL-WR710N_V2.1_150507.zip.extracted]# ls
0.zip  'How to upgrade TP-LINK Wireless N Router.pdf'  'wr710nv2_fs_uk_8M_3_16_12_up_boot(150507).bin'
[root@kali]~/_TL-WR710N_V2.1_150507.zip.extracted]#
```

EXPERIMENT 9

Lab Objective : Email Forensics

New post in iseetea [Inbox](#)

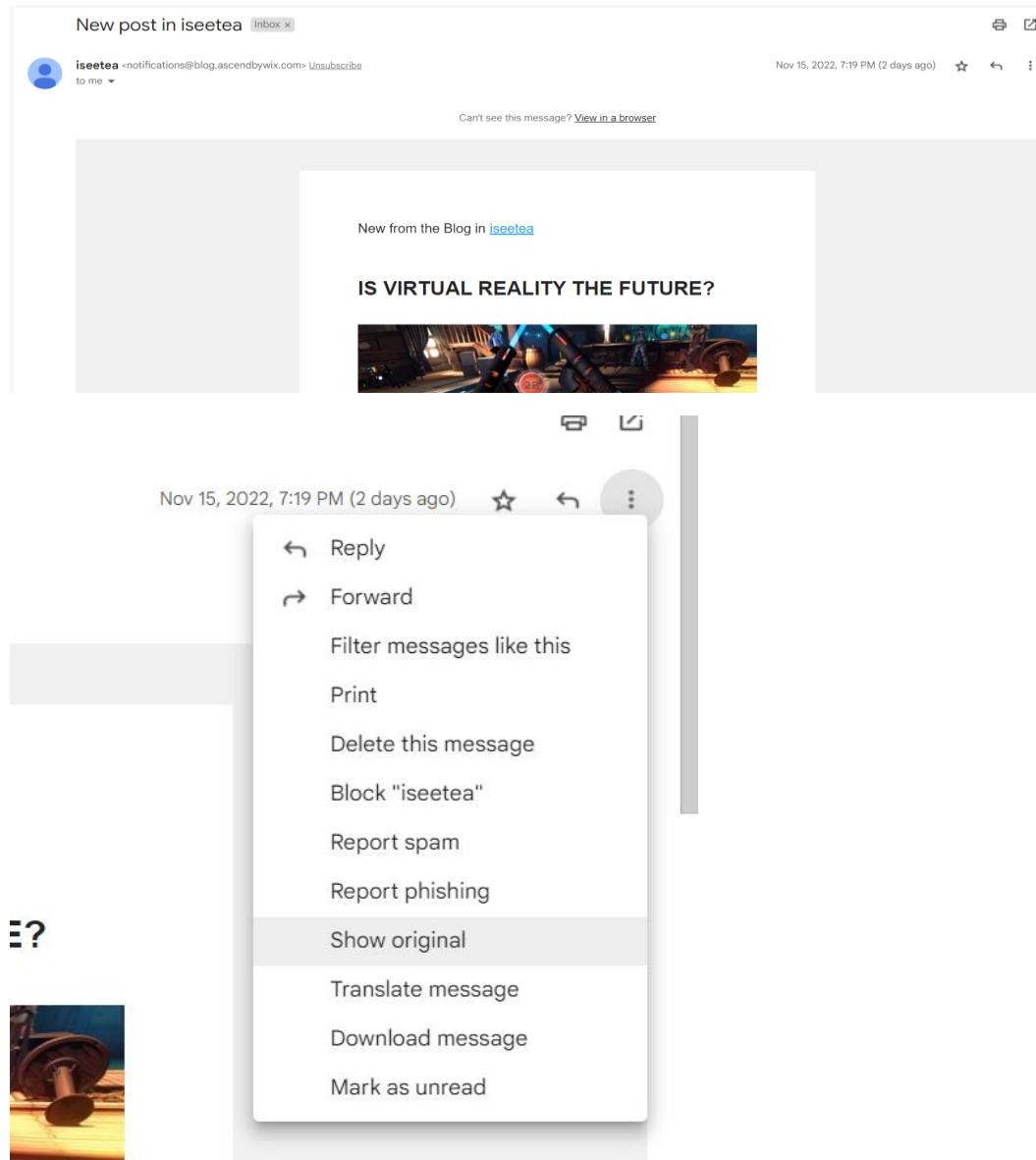
iseetea <notifications@blog.ascendbywix.com> [Unsubscribe](#)
to me ▾

Nov 15, 2022, 7:19 PM (2 days ago) [View in a browser](#)

Can't see this message? [View in a browser](#)

New from the Blog in [iseetea](#)

IS VIRTUAL REALITY THE FUTURE?



Nov 15, 2022, 7:19 PM (2 days ago)

Reply

Forward

Filter messages like this

Print

Delete this message

Block "iseetea"

Report spam

Report phishing

Show original

Translate message

Download message

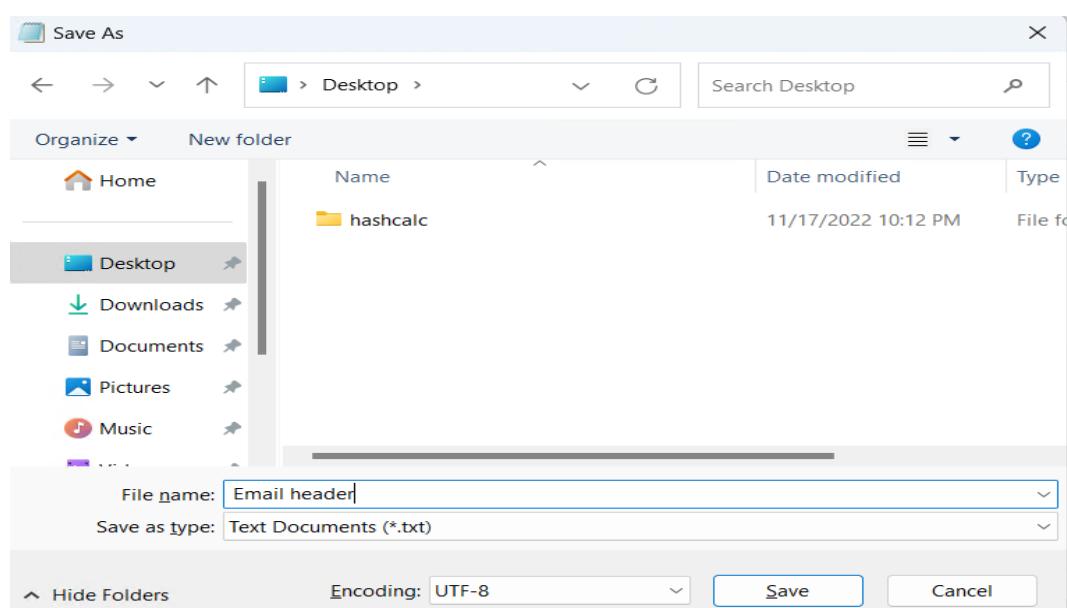
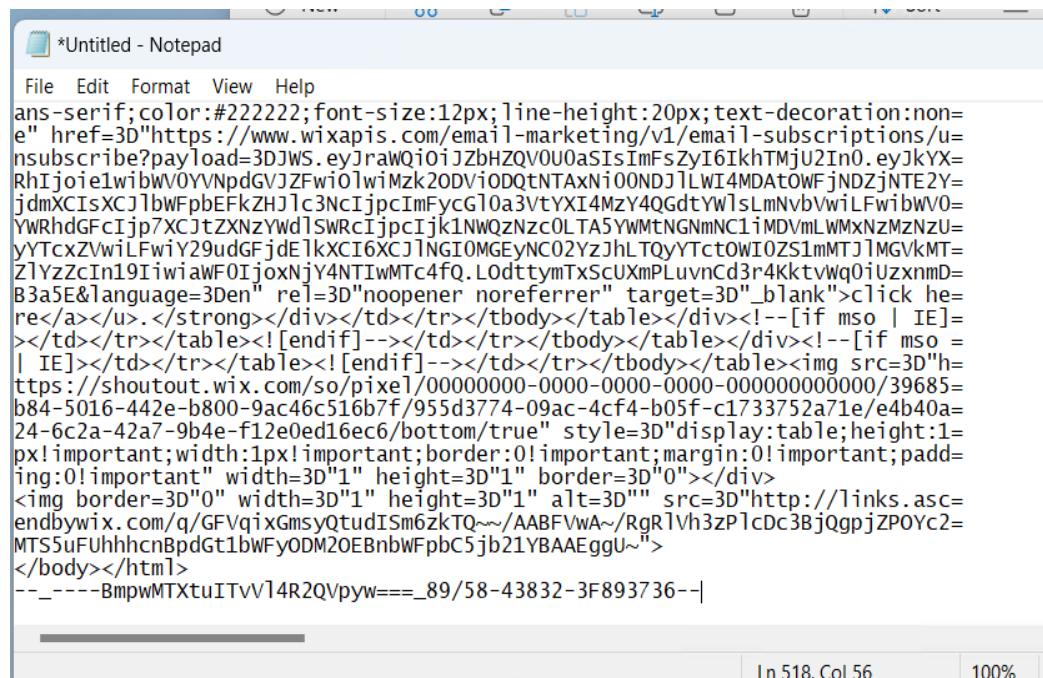
Mark as unread

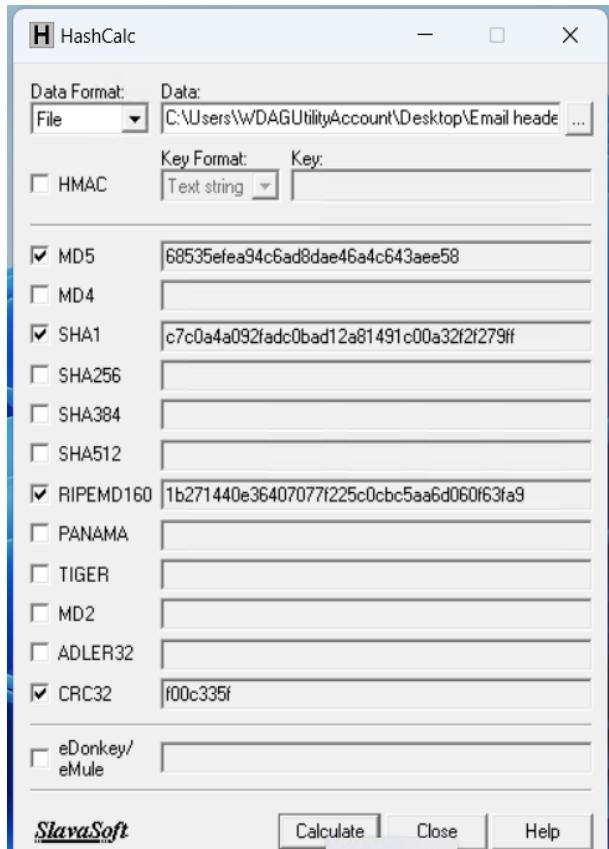
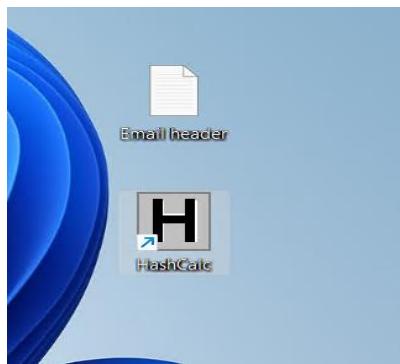
Original Message

Message ID	<B9.58.43832.3F893736@jk.mta1vrest.cc.prd.sparkpost>
Created at:	Tue, Nov 15, 2022 at 7:19 PM (Delivered after 0 seconds)
From:	iseetea <notifications@blog.ascendbywix.com>
To:	Arpit Kumar <arpitkumar8368@gmail.com>
Subject:	New post in iseetea
SPF:	PASS with IP 156.70.25.18 Learn more
DKIM:	'PASS' with domain blog.ascendbywix.com Learn more
DMARC:	'PASS' Learn more

[Download Original](#) [Copy to clipboard](#)

Delivered-To: arpitkumar836@gmail.com
 Received: by 2002:a9d:7c97::0:0:0:0 with SMTP id q23csp3667979otn;
 Tue, 15 Nov 2022 05:49:39 -0800 (PST)
 X-Google-Smtp-Source: AA0mqFsjlgn9bcyQfpGrSzLrxXfVHvTGBbRBPBzIOaUp0cLteWCKxVytRf3rwOELkpxAQF5wTNZ
 X-Received: by 2002:a17:902:74cc:bo:17c:5b01:f227 with SMTP id f12-20020a17090274cc00b0017c5b01f227mr420338plt.3.1668520179464;
 Tue, 15 Nov 2022 05:49:39 -0800 (PST)
 ARC-Seal: i=1; a=rsa-sha256; t=1668520179; cv=none;
 d=google.com; s=arc-20160816;
 b=nxQ0MKBrp+2gPjd4zRcQj3U3wZcTHbcor3K+sjx/VK/r900ytWk82J3MBegwsc+c
 vr0UTKNUktKjm1wMhmtzn0/h1n1n2EwK+Z60xIwNqzwrhagBGDwfsxh4keAUMAl
 jn2pwePckfUEbd+F4c43+cmu2iqoPyNdr+FCNrca4as9/i1GPijBz#m0g2KOQCAC0f+F
 B1Lts5quSz91M9K1xKxDT5469BHiZ7VC/8R3diHVZ7KVYzGtf1ovhb1AQXBnpvlgFmT
 hb/xF1yhega7o1oGDMzCx5rHCH80naIOHtqOPWoAIhvaqjPPbkirkpTau7rx4Fw5Q8p8
 RR6w==
 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
 h=feedback-id:precedence:from:list-unsubscribe:subject:mime-version
 :date:message-id:to:dkim-signature:
 bh-9ifx51xe/xhTWeosutVh3vvB2zIBGDdhCg3DDK-AY=;
 b=niPFUH0z3+C+kda{jIUZnYQK5DbfwA7DwXzPBwDxw2Cydspyzs2jL0Hju49JW3
 Lb469Ygv2hg4czM5N0M1D/LcsLodhM5cBQVnuhhsC2pZG2BgPTdEWIDooIfk13bJ
 fzsfxcMDTUKBBF/UzvToHf12b94lyss+A4qVi bvqjRwe28D4kuFR46fhtRp5PWE98
 oTBzfoetnVawnvpxb0ILpmdxWAkmpig/h3EfvtQocycbzouVpcVEa64KaweySmkQ35C
 qkF1dA34f1Extf6iwaAloABqrrioOv0jMRTDvHs0mz88adT9Hbry60b+t6zRE01E700S
 BgUa=
 ARC-Authentication-Results: i=1; mx.google.com;
 dkim=pass header.i=@blog.ascendbywix.com header.s=schph0420 header.b=nCrsoWU;
 spf=pass (google.com: domain of msprvsi=19318bgewk20-bounces-17751-295429@spmailtechno.com designates 156.70.25.18 as permitted
 smtp.mailfrom="msprvsi=19318bgewk20-bounces-17751-295429@spmailtechno.com";
 dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=@ascendbywix.com
 Return-Path: <msprvsi=19318bgewk20-bounces-17751-295429@spmailtechno.com>
 Received: from mta-70-25-18.wix-shared.com.sparkpostmail.com (mta-70-25-18.wix-shared.com.sparkpostmail.com. [156.70.25.18])
 by mx console.com with ESMTPS id a5-20020a17090274cc00b0017c5b01f227mr420338plt.3.1668520179464;





email header analyzer

X | : More Tools

About 88,10,000 results (0.29 seconds)

<https://mxtoolbox.com> › EmailHeaders :

Email Header Analyzer, RFC822 Parser - MxToolbox

This tool will make email headers human readable by parsing them according to RFC 822.

Email headers are present on every email you receive via the Internet ...

<https://mha.azurewebsites.net> :

Message Header Analyzer

Message Header Analyzer. Insert the message header you would like to analyze+ -. Analyze

MX TOOLBOX®

SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup **Analyze Header**

Email Header Analyzer

Paste Header:

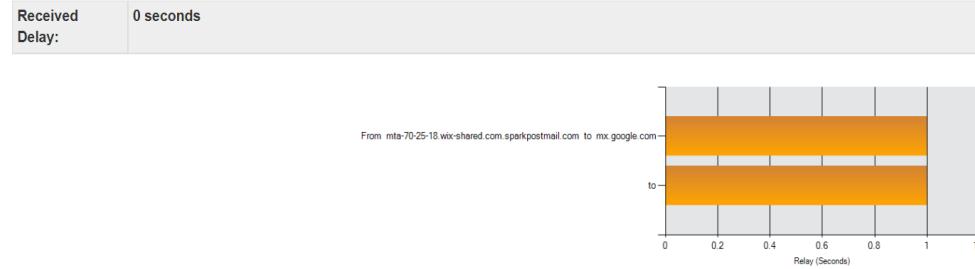
```
<tr></tr></table><td><img alt="Email icon" style="vertical-align: middle;"/> Email Header Analyzer</td></tr></table><img alt="Background image" style="background-size: cover; background-position: center; height: 100%; width: 100%; object-fit: cover; filter: grayscale(1);"/>
```

Analyze Header

Delivery Information

- ⓘ DMARC Compliant
- ⓘ SPF Alignment
- ⓘ SPF Authenticated
- ⓘ DKIM Alignment
- ⓘ DKIM Authenticated

Relay Information



SPF and DKIM Information

dmarc:blog.ascendbywix.com [Show](#) [Solve Email Delivery Problems](#)

DMARC Record for blog.ascendbywix.com

No DMARC Record found for sub-domain.

Organization Domain of this sub-domain is: ascendbywix.com Inbox Receivers will apply ascendbywix.com DMARC record to mail sent from blog.ascendbywix.com

SP Tag '' found: Inbox Receivers will treat all mail sent from blog.ascendbywix.com that fails DMARC as suspicious.

DMARC Record for ascendbywix.com (organizational domain)

v=DMARC1;p=reject;rua=mailto:monitor@wixshoutout.com,mailto:wix@dmarc.postmastery.com,mailto:dmarc_agg@everest.email;ruf=mailto:danny@wixshoutout.com,

◀

spf:spmailtechno.com:156.70.25.18 [Hide](#)

v=spf1 exists:{i}._spf.sparkpostmail.com ~all

Prefix	Type	Value	PrefixDesc	Description
v		spf1		The SPF record version
+	exists	{i}._spf.sparkpostmail.com	Pass	This mechanism is used to construct an arbitrary host name that is used for
~	all		SoftFail	Always matches. It goes at the end of your record.
	From Domain	blog ascendbywix.com		The domain used in the From header field.
	Return Path Domain	spmailtechno.com		The domain used in the Return-Path header field.

Test	Result
SPF Alignment	Domain not found in SPF
SPF Record Published	SPF Record found
SPF Record Deprecated	No deprecated records found
SPF Multiple Records	Less than two records found
SPF Contains characters after ALL	No items after 'ALL'.
SPF Syntax Check	The record is valid
SPF Included Lookups	Number of included lookups is OK
SPF Type PTR Check	No type PTR found
DKIM Validations	All checks successful

dkim:blog.ascendbywix.com:scph0420 [Show](#)

Dkim Public Record:

v=DKIM1;k=rsa;h=sha256;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCx0kyVU+mX21Ef3zRnHA3trLgmwUSUXgxenWtNm

◀

Dkim Signature:

v=1; a=rsa-sha256; c=relaxed/relaxed; d=blog.ascendbywix.com; s=scph0420; t=1668520179; i=@blog.ascendbywix.com

◀