NAME: SUYASH SHINDE

ROLL NO: D2223034

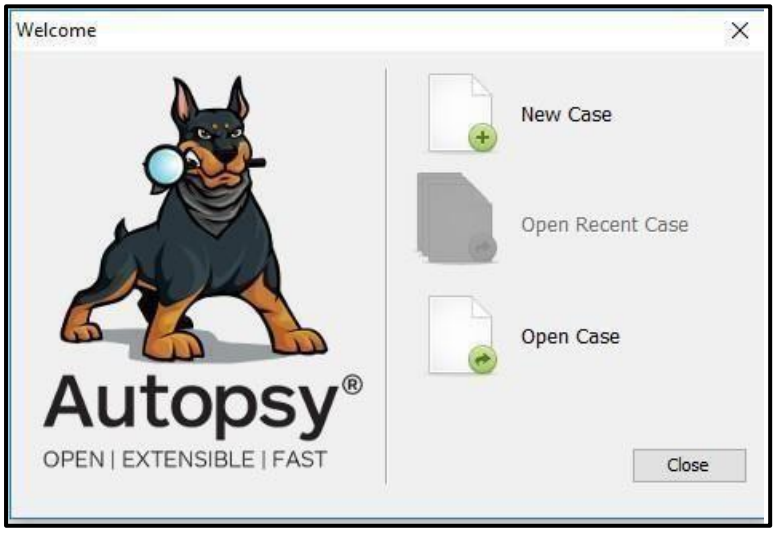
CLASS: CSF 2

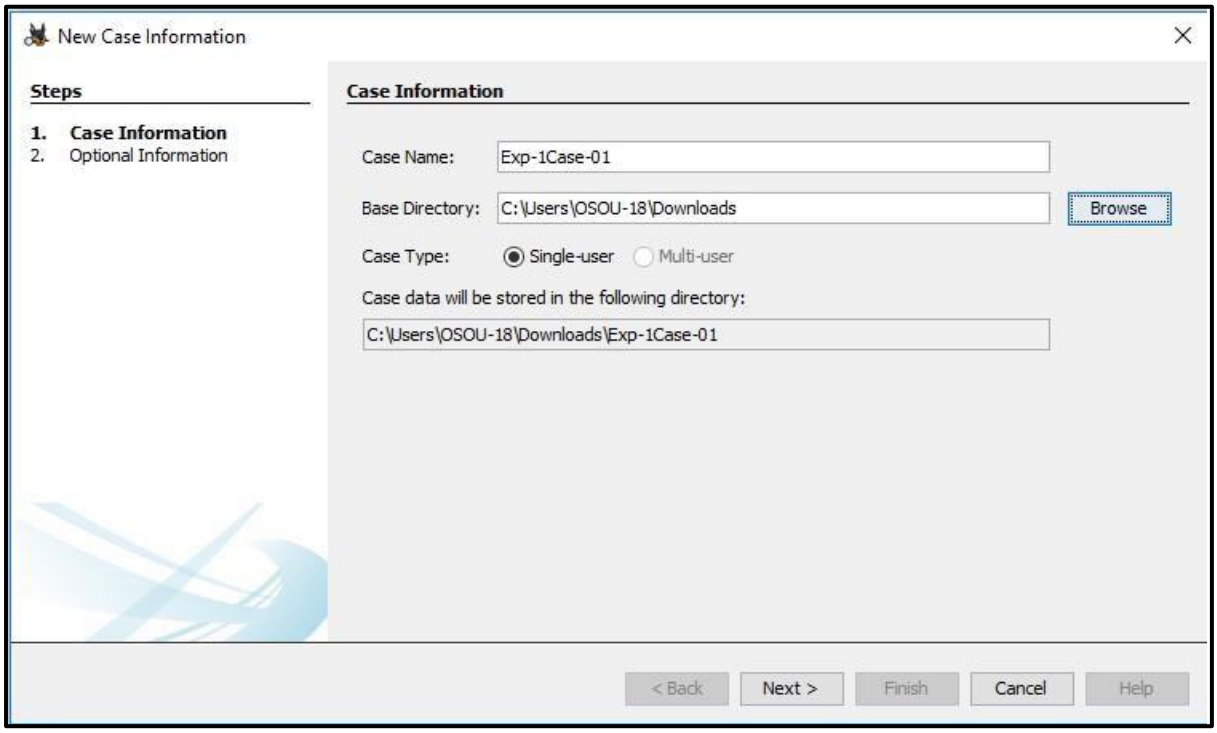
SUBJECT: CFEL

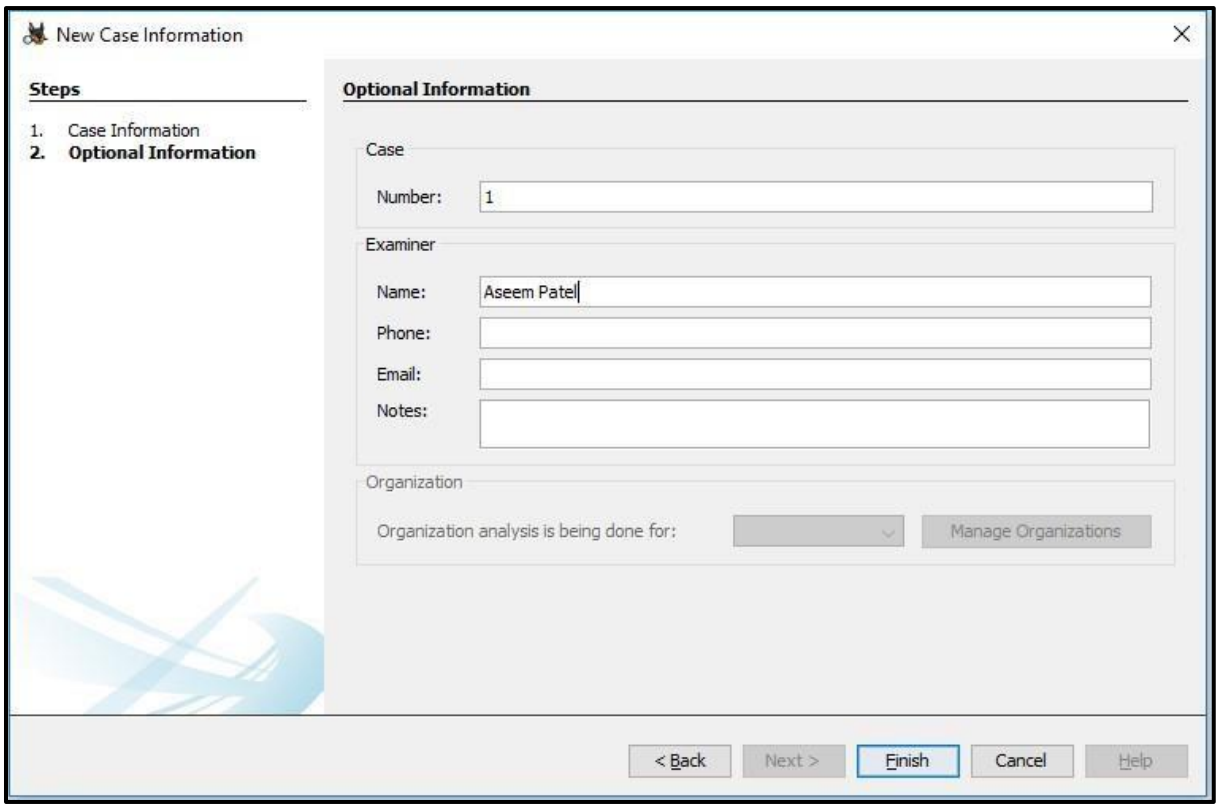
EXPERIMENT 1

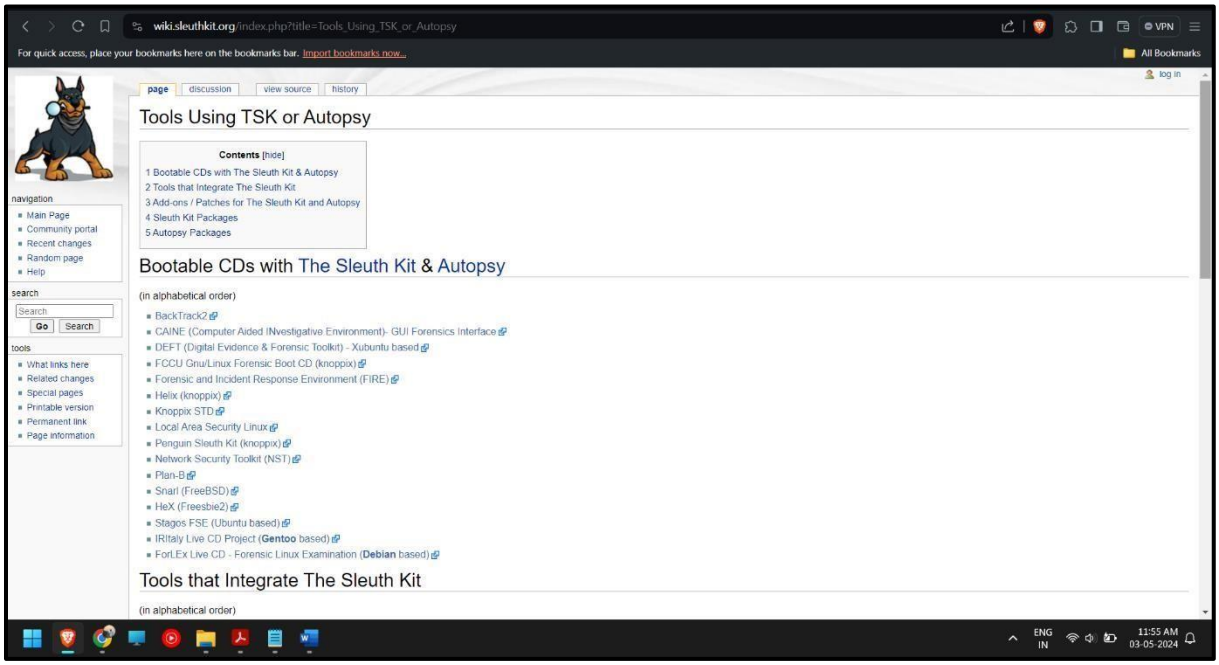
Aim: Study of Computer Forensics and different tools used for forensic investigation.

SCREENSHOTS:






New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 1
Examiner
Name: Aseem Patel
Phone:
Email:
Notes:
Organization
Organization analysis is being done for:
Manage Organizations
< Back
Next >
Finish
Cancel
Help


wiki.sleuthkit.org/index.php?title=Tools_Using_TSK_or_Autopsy
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
All Bookmarks
page
discussion
view source
history
Tools Using TSK or Autopsy
Contents [hide]
1 Bootable CDs with The Sleuth Kit & Autopsy
2 Tools that Integrate The Sleuth Kit
3 Add-ons / Patches for The Sleuth Kit and Autopsy
4 Sleuth Kit Packages
5 Autopsy Packages
Bootable CDs with The Sleuth Kit & Autopsy
(in alphabetical order)
BackTrack2
CAINE (Computer Aided INvestigative Environment)- GUI Forensics Interface
DEFT (Digital Evidence & Forensic Toolkit) - Xubuntu based
FCCU Gnu/Linux Forensic Boot CD (knoppix)
Forensic and Incident Response Environment (FIRE)
Helix (knoppix)
Knoppix STD
Local Area Security Linux
Penguin Sleuth Kit (knoppix)
Network Security Toolkit (NST)
Plan-B
Snarl (FreeBSD)
HeX (Freesbie2)
Stagos FSE (Ubuntu based)
IRItaly Live CD Project (Gentoo based)
ForLEx Live CD - Forensic Linux Examination (Debian based)
Tools that Integrate The Sleuth Kit
(in alphabetical order)
navigation
Main Page
Community portal
Recent changes
Random page
Help
search
Go
Search
tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information
ENG
IN
11:55 AM
03-05-2024

NAME: SUYASH SHINDE

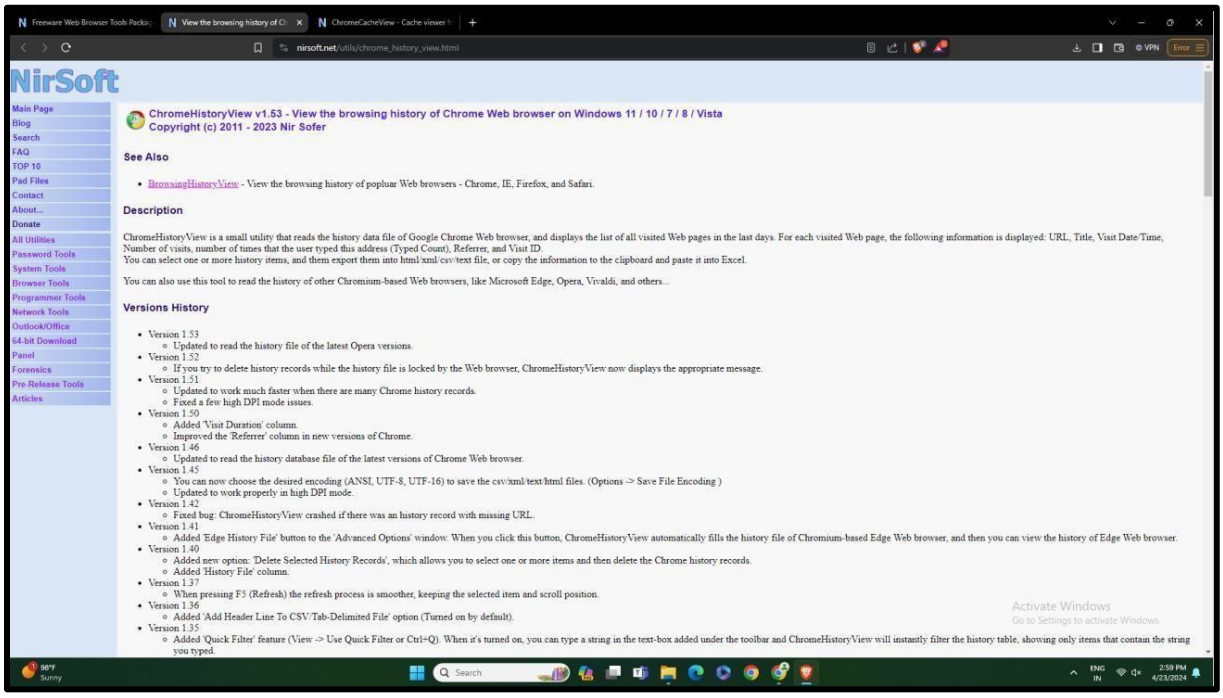
ROLL NO: D2223034

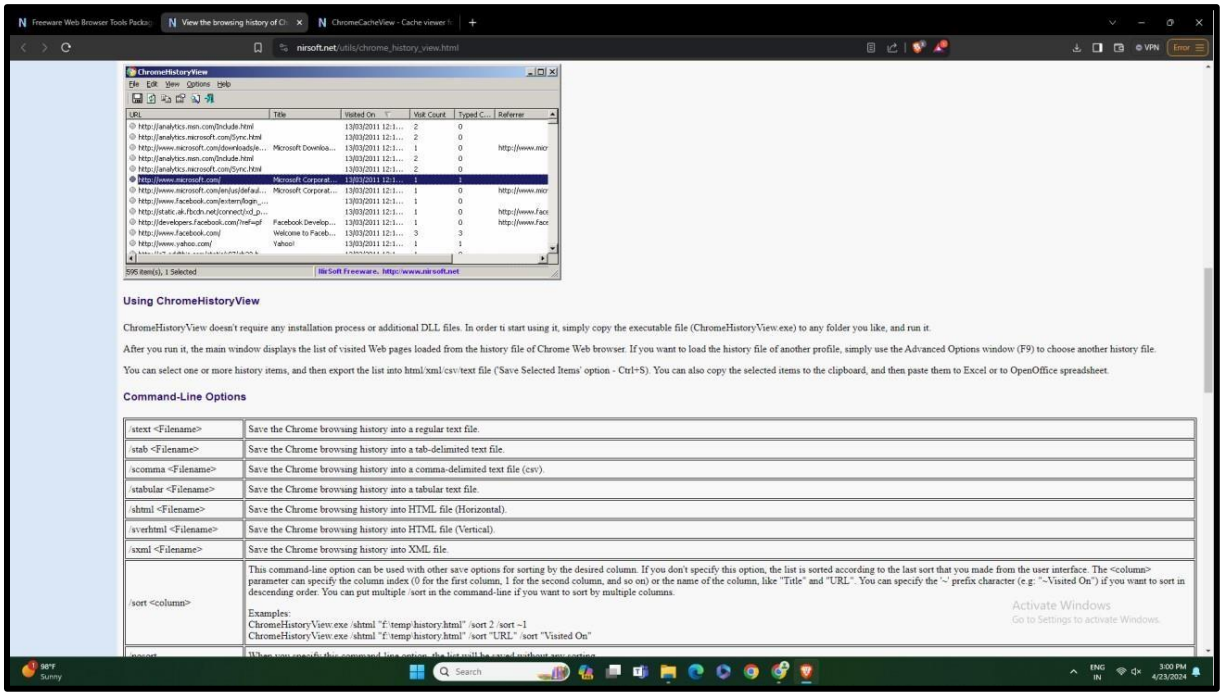
CLASS: CSF 2

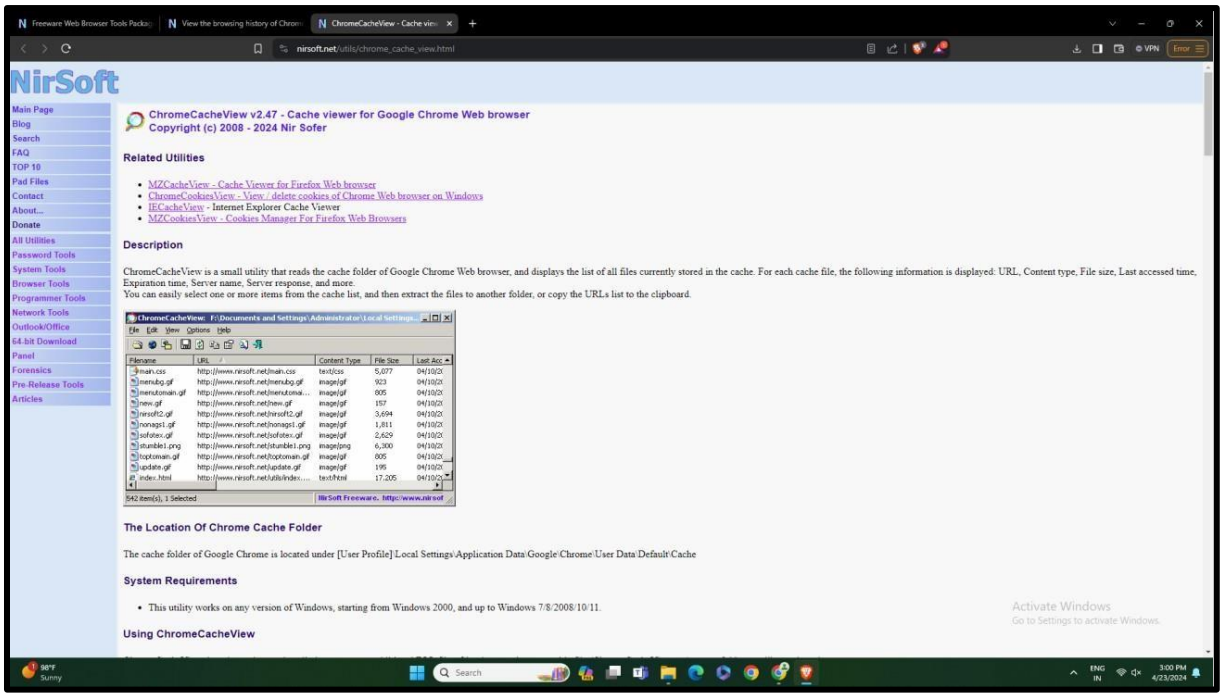
EXPERIMENT 11

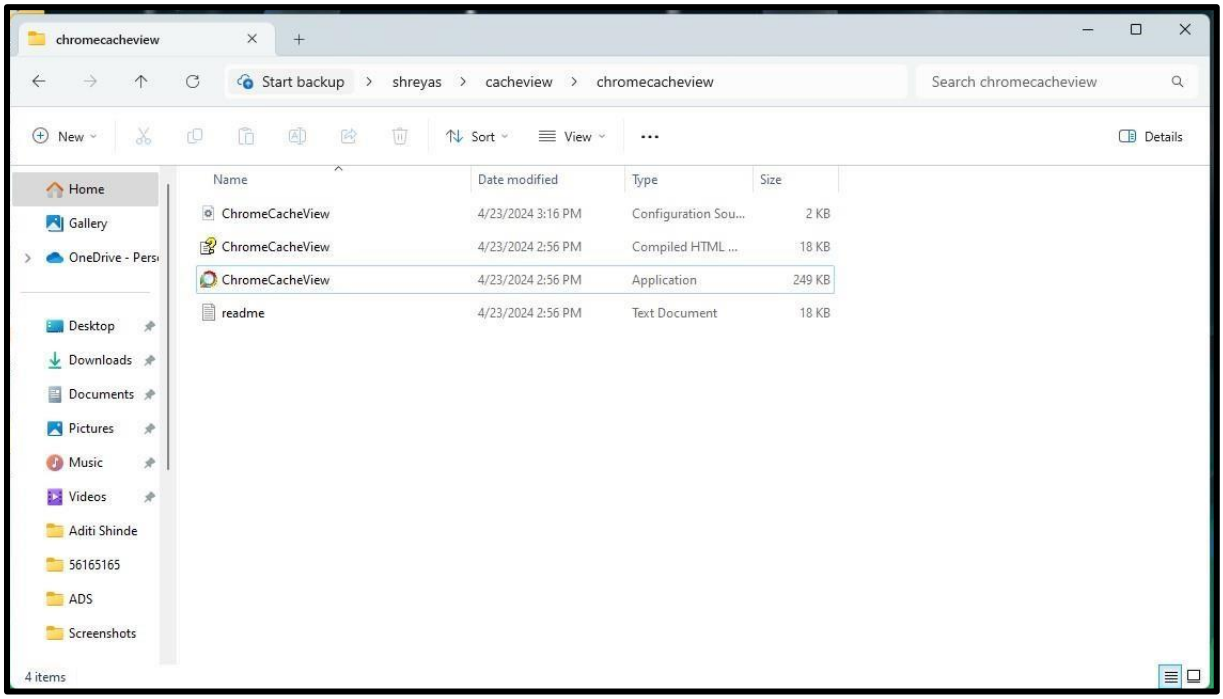
Aim: - Using Sysinternals tools for Network Tracking and Process Monitoring:

SCREENSHOTS:






NirSoft
ChromeCacheView v2.47 - Cache viewer for Google Chrome Web browser
Copyright (c) 2008 - 2024 Nir Sofer
Related Utilities
MZCacheView - Cache Viewer for Firefox Web browser
ChromeCookiesView - View / delete cookies of Chrome Web browser on Windows
IECacheView - Internet Explorer Cache Viewer
MZCookiesView - Cookies Manager For Firefox Web Browsers
Description
ChromeCacheView is a small utility that reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache. For each cache file, the following information is displayed: URL, Content type, File size, Last accessed time, Expiration time, Server name, Server response, and more.
You can easily select one or more items from the cache list, and then extract the files to another folder, or copy the URLs list to the clipboard.
The Location Of Chrome Cache Folder
The cache folder of Google Chrome is located under [User Profile]\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache
System Requirements
This utility works on any version of Windows, starting from Windows 2000, and up to Windows 7/8/2008/10/11.
Using ChromeCacheView


chromecacheview
Start backup > shreyas > cacheview > chromecacheview
Search chromecacheview
New
Sort
View
Details
Home
Gallery
OneDrive - Pers
Desktop
Downloads
Documents
Pictures
Music
Videos
Aditi Shinde
56165165
ADS
Screenshots
Name
Date modified
Type
Size
ChromeCacheView 4/23/2024 3:16 PM Configuration Sou... 2 KB
ChromeCacheView 4/23/2024 2:56 PM Compiled HTML ... 18 KB
ChromeCacheView 4/23/2024 2:56 PM Application 249 KB
readme 4/23/2024 2:56 PM Text Document 18 KB
4 items

ChromeHistoryView

File Edit View Options Help

URL	Title	Visited On	Visit Count	Typed Count	Referrer	Visit Duration	Visit ID	Profile	URL Length	Transition Type	Transition Qualifiers	History File
chrome-extension://cjpalhdlnbpafiamejdnhcphjb...	Page blocked	4/2/2024 11:14:24 ...	1	0	https://temp-mail.org/en/view/660b9b255...	00:00:09.884	48	Default	433	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
file:///C:/Users/Admin/Downloads/ADSLab%20ass...	ADSLab assignments.pdf	4/4/2024 2:12:44 PM	1	0		00:08:31.297	167	Default	57	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
http://amcatcampus.aspiringminds.com/	SHL	4/18/2024 9:40:59 ...	2	0	https://web.whatsapp.com/		218	Default	37	Link	Chain Start	C:\Users\Admin\AppDa
http://amcatcampus.aspiringminds.com/	SHL	4/18/2024 9:40:59 ...	2	0	https://amcatcampus.aspiringminds.com/		220	Default	37	Link	Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.co.in/accounts/SetSID	Redirecting	4/2/2024 1:16:03 PM	1	0	https://accounts.google.co.in/accounts/Se...	00:00:00.305	120	Default	45	Link	Chain Start	C:\Users\Admin\AppDa
https://accounts.google.co.in/accounts/SetSID?ts...	Redirecting	4/2/2024 1:16:03 PM	1	0	https://accounts.google.com/accounts/S...	00:00:00.011	119	Default	1729	Link	Chain End,Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/AddSession?hl=en&...	Gmail	4/22/2024 11:21:30...	1	0	https://mail.google.com/mail/u/0/#inbox		268	Default	117	Link	Chain Start	C:\Users\Admin\AppDa
https://accounts.google.com/CheckCookie?conti...	Security Check-Up	4/23/2024 8:46:19 ...	1	0	https://accounts.google.com/signin/v2/sp...		35	Profile 3	450	Link	Chain Start	C:\Users\Admin\AppDa
https://accounts.google.com/CheckCookie?conti...	Redirecting	4/2/2024 1:16:03 PM	1	0	https://accounts.google.com/v3/signin/ch...		117	Default	1354	Link	Chain Start	C:\Users\Admin\AppDa
https://accounts.google.com/InteractiveLogin/sig...	Sign in - Google accounts	4/23/2024 8:44:57 ...	1	0	https://accounts.google.com/InteractiveLo...	00:00:02.364	27	Profile 3	293	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/InteractiveLogin?co...	Sign in - Google accounts	4/23/2024 8:44:57 ...	1	0	https://accounts.google.com/InteractiveLo...	00:00:00.008	26	Profile 3	233	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/InteractiveLogin?co...	Sign in - Google accounts	4/23/2024 8:44:57 ...	1	0	https://accounts.google.com/ServiceLogin...	00:00:00.639	25	Profile 3	210	Link	Chain End,Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/Logout	Google Accounts	4/22/2024 11:25:57...	1	0	https://accounts.google.com/Logout?hl=e...	00:00:01.542	9	Profile 3	34	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/Logout?hl=en&con...	Google Accounts	4/22/2024 11:25:57...	1	0		00:00:00.003	8	Profile 3	165	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/Logout?hl=en&con...	Google	4/23/2024 9:20:21 ...	1	0			65	Profile 3	159	Link	Chain Start	C:\Users\Admin\AppDa
https://accounts.google.com/o/oauth2/auth?logi...	Sign in - Google Accounts	3/19/2024 12:43:13...	1	0	https://auth0.openai.com/authorize?client_...		7	Default	279	Link	Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/o/oauth2/v2/auth?g...	Sign in - Google Accounts	4/2/2024 1:15:39 PM	1	0	https://app.spline.design/signin		113	Default	347	Link	Chain Start	C:\Users\Admin\AppDa
https://accounts.google.com/ServiceLogin?tmpl...	Sign in - Google accounts	4/23/2024 8:44:57 ...	1	0	https://workspace.google.com/products/...		24	Profile 3	120	Link	Chain Start	C:\Users\Admin\AppDa
https://accounts.google.com/ServiceLogin?passiv...	Google Meet	4/23/2024 8:46:23 ...	1	0	https://meet.google.com/?hs=193&hl=en_...		44	Profile 3	195	Link	Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/ServiceLogin?passiv...	Security Checkup	4/23/2024 11:22:05...	1	0	https://myaccount.google.com/security-c...		276	Default	1505	Link	Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/ServiceLogin?passiv...	Security Check-Up	4/23/2024 8:46:19 ...	1	0	https://myaccount.google.com/security-c...		37	Profile 3	1500	Link	Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/ServiceLogin?servic...	Inbox (160) - kyamalum713@gma...	4/22/2024 11:21:19...	1	0	https://mail.google.com/mail/u/0/		263	Default	179	Link	Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/ServiceLogin?servic...	Inbox (126) - aditya18981@gmail....	4/22/2024 11:22:20...	1	0	https://mail.google.com/mail/u/0/?hl=en#...		2	Profile 3	207	Auto Bookmark	Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/signin/oauth/conse...		4/2/2024 1:16:04 PM	1	0	https://accounts.google.co.in/accounts/Se...	00:00:01.269	121	Default	825	Link	Chain End,Client Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/signin/v2/speedbu...	Gmail	4/22/2024 11:22:01...	1	0	https://accounts.google.com/signin/v2/sp...	00:00:04.172	274	Default	395	Link	Chain End,Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/signin/v2/speedbu...	Sign in - Google accounts	4/23/2024 8:46:07 ...	1	0	https://accounts.google.com/signin/v2/sp...	00:00:00.621	33	Profile 3	447	Link	Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/signin/v2/speedbu...	Sign in - Google accounts	4/23/2024 8:46:08 ...	1	0	https://accounts.google.com/signin/v2/sp...	00:00:11.233	34	Profile 3	445	Link	Chain End,Client Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/signin/v2/speedbu...	Gmail	4/22/2024 11:22:01...	1	0	https://accounts.google.com/v3/signin/ch...		273	Default	375	Link	Client Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/signin/v2/speedbu...	Sign in - Google accounts	4/23/2024 8:46:07 ...	1	0	https://accounts.google.com/v3/signin/ch...		32	Profile 3	427	Link	Client Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/challenge...	Gmail	4/22/2024 11:21:49...	1	0	https://accounts.google.com/v3/signin/ch...	00:00:11.943	272	Default	369	Link	Chain Start	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/challenge...	Sign in - Google accounts	4/23/2024 8:45:17 ...	1	0	https://accounts.google.com/v3/signin/ch...	00:00:49.953	31	Profile 3	421	Link	Chain Start	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/challenge...	Sign in - Google Accounts	4/2/2024 1:15:53 PM	1	0	https://accounts.google.com/v3/signin/id...	00:00:10.713	116	Default	1526	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/challenge...	Gmail	4/22/2024 11:21:45...	1	0	https://accounts.google.com/v3/signin/id...	00:00:04.231	271	Default	370	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/challenge...	Sign in - Google Accounts	4/23/2024 8:45:13 ...	1	0	https://accounts.google.com/v3/signin/id...	00:00:04.058	30	Profile 3	422	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/identifier?...	Gmail	4/22/2024 11:21:30...	2	0	https://accounts.google.com/v3/signin/id...	00:00:14.260	270	Default	231	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/identifier?...	Gmail	4/22/2024 11:21:30...	2	0	https://accounts.google.com/AddSession?...	00:00:00.221	269	Default	231	Link	Chain End,Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/identifier?...	Sign in - Google Accounts	4/23/2024 8:45:00 ...	2	0	https://accounts.google.com/InteractiveLo...	00:00:00.108	28	Profile 3	283	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/identifier?...	Sign in - Google Accounts	4/23/2024 8:45:00 ...	2	0	https://accounts.google.com/v3/signin/id...	00:00:13.632	29	Profile 3	283	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/identifier?...	Sign in - Google Accounts	3/19/2024 12:43:13...	2	0	https://accounts.google.com/o/oauth2/au...	00:00:00.187	8	Default	1306	Link	Chain End,Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/identifier?...	Sign in - Google Accounts	3/19/2024 12:43:13...	2	0	https://accounts.google.com/v3/signin/id...	00:00:03.024	9	Default	1306	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/identifier?...	Sign in - Google Accounts	4/2/2024 1:15:39 PM	2	0	https://accounts.google.com/o/oauth2/v2...	00:00:00.449	114	Default	1383	Link	Chain End,Server Redirect	C:\Users\Admin\AppDa
https://accounts.google.com/v3/signin/identifier?...	Sign in - Google Accounts	4/2/2024 1:15:40 PM	2	0	https://accounts.google.com/v3/signin/id...	00:00:13.162	115	Default	1383	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://accounts.youtube.com/accounts/SetSID?s...	Redirecting	4/2/2024 1:16:03 PM	1	0	https://accounts.google.com/CheckCooki...		118	Default	1762	Link	Server Redirect	C:\Users\Admin\AppDa
https://amcatcampus.aspiringminds.com/	SHL	4/18/2024 9:40:59 ...	4	1	https://amcatcampus.aspiringminds.com/	01:07:09.442	221	Default	38	Link	Chain End,Server Redirect	C:\Users\Admin\AppDa
https://amcatcampus.aspiringminds.com/	SHL	4/18/2024 9:40:59 ...	4	1	http://amcatcampus.aspiringminds.com/		219	Default	38	Link	Server Redirect	C:\Users\Admin\AppDa
https://amcatcampus.aspiringminds.com/	SHL	4/18/2024 10:49:00...	4	1		00:00:02.467	224	Default	38	Link	Chain Start,Chain End	C:\Users\Admin\AppDa
https://amcatcampus.aspiringminds.com/	SHL	4/18/2024 1:19:30 ...	4	1		02:06:17.675	249	Default	38	Reload	Chain Start,Chain End	C:\Users\Admin\AppDa

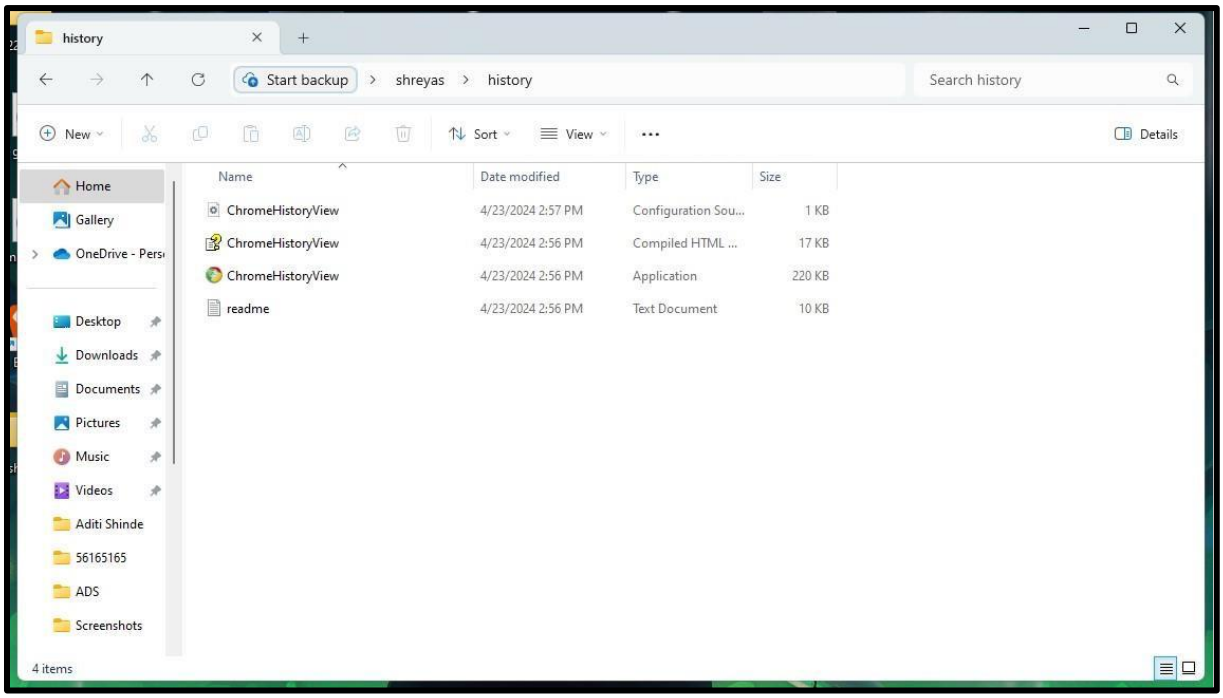
434 item(s) NirSoft Freeware. https://www.nirsoft.net

ChromeCacheView: C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Profile 3\Cache\Cache_Data

File Edit View Options Help

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server Name	Server Response	Web Site	Frame	Content En...	Cache Name
$(PUBMATIC_UI...	https://s.tribalfusion.com/z/i.match?p=b11&redirect=https%...	image/gif	43	4/23/2024 11:22:42...	4/23/2024 11:22:41...	1/1/1601 5:30:00 AM	1/1/1970 5:30:00 AM	cloudflare	HTTP/1.1 200	https://programiz.com	https://tribalfusion.com		data_1 [1456128]
$(PUBMATIC_UI...	https://a.tribalfusion.com/i.match?p=b11&redirect=https%3A...	text/html	0	4/23/2024 11:22:42...	4/23/2024 11:22:40...	1/1/1601 5:30:00 AM	1/1/1970 5:30:00 AM	cloudflare	HTTP/1.1 302	https://programiz.com	https://tribalfusion.com		
&media=adSp...	https://ecrh.quantserve.com/pixel/p-1RYxxePXT9bCS2.gif?lr=...	image/gif	35	4/23/2024 11:58:53...	4/23/2024 11:58:52...	1/1/1601 5:30:00 AM	4/30/2024 11:58:52...		HTTP/1.1 200	https://programiz.com	https://programiz.com		data_1 [1851136]
&media=adSp...	https://ecrh.quantserve.com/pixel/p-1RYxxePXT9bCS2.gif?lr=...	image/gif	35	4/23/2024 11:36:43...	4/23/2024 11:36:41...	1/1/1601 5:30:00 AM	4/30/2024 11:36:41...		HTTP/1.1 200	https://programiz.com	https://programiz.com		data_1 [1788028]
&publisher_dm...	https://ad.360yield.com/ux?&publisher_dmp_id=15&cr=https...	text/plain	0	4/23/2024 11:23:11...	4/23/2024 11:23:10...	1/1/1601 5:30:00 AM	1/1/1601 5:30:00 AM		HTTP/1.1 302	https://programiz.com	https://programiz.com		
-634301329.gif	https://accounts.youtube.com/accounts/ClearSID?tx=-634301...	image/gif	35	4/22/2024 11:25:58...	4/22/2024 11:25:58...	1/1/2007 5:30:00 AM	4/22/2024 11:25:58...	ESF	HTTP/1.1 200	https://google.com	https://google.com		data_1 [413696]
-HwBwrbpJ0ZH...	https://lh3.googleusercontent.com/-HwBwrbpJ0ZHFBlynKGbiR...	image/png	437,904	4/23/2024 8:46:20 ...	4/23/2024 8:02:18 ...	1/1/1601 5:30:00 AM	4/24/2024 8:02:18 ...	fife	HTTP/1.1 200	https://google.com	https://google.com		f_000113
0	https://mail.google.com/mail/u/0	application/binary	0	4/22/2024 11:25:59...	4/22/2024 11:25:59...	1/1/1601 5:30:00 AM	1/1/1601 5:30:00 AM	ESF	HTTP/1.1 302	https://google.com	https://google.com		
0.1	https://cdnads.geeksforgeeks.org/prebid.js?ver=0.1	application/java...	43	4/23/2024 11:59:01...	4/22/2024 4:55:30 ...	1/1/1601 5:30:00 AM	1/1/1601 5:30:00 AM	nginx	HTTP/1.1 200	https://geeksforgeeks.org	https://geeksforgeeks.org		data_1 [1086208]
0.1	https://cdnads.geeksforgeeks.org/gfg_ads.min.js?ver=0.1	application/java...	3,051	4/23/2024 11:59:01...	4/23/2024 11:38:31...	1/1/1601 5:30:00 AM	1/1/1601 5:30:00 AM	nginx	HTTP/1.1 200	https://geeksforgeeks.org	https://geeksforgeeks.org	gzip	data_2 [3309568]
0.9	https://www.geeksforgeeks.org/wp-content/themes/iconic-o...	application/java...	6,614	4/23/2024 11:59:01...	4/22/2024 9:20:50 ...	4/19/2024 12:40:48...	1/1/1601 5:30:00 AM	Apache	HTTP/1.1 200	https://geeksforgeeks.org	https://geeksforgeeks.org	gzip	data_3 [2130792]
0.gif	https://pr-bh.ybp.yahoo.com/sync/openx/2e180e17-4162-e5a...	image/gif	43	4/23/2024 11:22:37...	4/23/2024 11:22:35...	1/1/1601 5:30:00 AM	1/1/1601 5:30:00 AM	ATS	HTTP/1.1 200	https://programiz.com	https://openx.net		data_1 [1313536]
0.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/0.we...	image/webp	9,640	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [8249344]
0000	https://www.gstatic.com/chrome/autofill/password_generati...	application/octe...	3,223	4/23/2024 8:48:54 ...	4/21/2024 1:08:26 PM	1/5/2024 6:32:50 PM	4/28/2024 1:08:26 ...	sffe	HTTP/1.1 200	https://gstatic.com	https://gstatic.com	gzip	data_2 [1540096]
01_250.htm	https://s0.2mdn.net/sadbundle/9394055593971317997/728x90...	text/html	2,392	4/23/2024 11:48:43...	4/16/2024 1:16:27 ...	3/3/2023 3:38:19 AM	4/16/2025 1:16:27 ...	sffe	HTTP/1.1 200	https://programiz.com	https://2mdn.net	gzip	data_2 [3256320]
01_250.htm	https://s0.2mdn.net/sadbundle/10507897489306299413/index...	text/html	2,474	4/23/2024 11:37:14...	4/17/2024 5:26:43 ...	3/1/2024 4:26:03 AM	4/17/2025 5:26:43 ...	sffe	HTTP/1.1 200	https://programiz.com	https://2mdn.net	gzip	data_2 [3194880]
01_250.htm	https://s0.2mdn.net/sadbundle/7503683125317625890/300x25...	text/html	2,405	4/23/2024 11:18:06...	4/18/2024 9:33:05 ...	6/23/2023 11:32:38...	4/18/2025 9:33:05 ...	sffe	HTTP/1.1 200	https://geeksforgeeks.org	https://2mdn.net	gzip	data_2 [1957888]
01_250.htm	https://s0.2mdn.net/sadbundle/2566725258173329752/728x90...	text/html	2,403	4/23/2024 12:05:04...	4/17/2024 5:36:21 ...	6/26/2023 9:35:57 ...	4/17/2025 5:36:21 ...	sffe	HTTP/1.1 200	https://programiz.com	https://2mdn.net	gzip	data_2 [2772992]
08403430.min.js	https://workspace.google.com/assets/08403430.min.js	text/javascript	1,628	4/23/2024 8:44:34 ...	4/23/2024 8:44:32 ...	12/19/2023 7:18:00...	4/23/2024 8:44:32 ...	sffe	HTTP/1.1 200	https://google.com	https://google.com	br	data_2 [604160]
0a6IMYQzqqYZI...	https://pagead2.googlesyndication.com/bg/0a6IMYQzqqYZIKc...	text/javascript	20,292	4/23/2024 2:45:39 ...	4/18/2024 1:52:55 ...	4/16/2024 7:28:00 ...	4/18/2025 1:52:55 ...	sffe	HTTP/1.1 200	https://nirsoft.net	https://doubleclick.net	br	f_000296
0c99504f.min.js	https://workspace.google.com/chunks/0c99504f.min.js	text/javascript	453	4/23/2024 8:44:35 ...	4/23/2024 8:44:33 ...	8/8/2023 1:38:00 AM	4/23/2024 8:44:33 ...	sffe	HTTP/1.1 200	https://google.com	https://google.com	br	data_1 [589824]
1	https://match.prod.bidr.io/cookie-sync/ie7_bee_ppps=1		0	4/23/2024 11:22:38...	4/23/2024 11:22:36...	1/1/1601 5:30:00 AM	1/1/1601 5:30:00 AM	gunicorn	HTTP/1.1 303 See ...	https://programiz.com	https://casalemedia.com		
1----	https://pr-bh.ybp.yahoo.com/sync/improvedigital/69ec06c7-...		0	4/23/2024 11:36:16...	4/23/2024 11:36:14...	1/1/1601 5:30:00 AM	1/1/1601 5:30:00 AM	ATS	HTTP/1.1 302	https://programiz.com	https://programiz.com		
1-ie-compat.js	https://brave.com/js/1-ie-compat.js	text/javascript	1,767	4/23/2024 2:48:02 ...	4/23/2024 5:45:26 ...	4/17/2024 10:43:28...	1/1/1601 5:30:00 AM	AmazonS3	HTTP/1.1 200	https://brave.com	https://brave.com	br	data_2 [3538944]
1.3.css	https://www.geeksforgeeks.org/wp-content/themes/iconic-o...	text/css	703	4/23/2024 11:59:01...	12/30/2023 5:56:54...	11/30/2023 9:28:14...	1/1/1601 5:30:00 AM	Apache	HTTP/1.1 200	https://geeksforgeeks.org	https://geeksforgeeks.org	gzip	data_1 [1085440]
1.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/1.we...	image/webp	11,158	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [8265728]
10.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/10.w...	image/webp	10,312	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [6250496]
100.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/100...	image/webp	13,158	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [10199040]
101.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/101...	image/webp	16,092	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [10362880]
102.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/102...	image/webp	11,518	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [10100736]
103.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/103...	image/webp	20,508	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	f_0000a3
104.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/104...	image/webp	17,228	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	f_0000a4
105.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/105...	image/webp	15,660	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [10461184]
106.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/106...	image/webp	18,414	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	f_0000a6
107.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/107...	image/webp	18,328	4/23/2024 8:46:48 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	f_0000a7
108.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/108...	image/webp	17,884	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	f_0000aa
109.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/109...	image/webp	12,344	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [10641408]
11	https://ads.stickyadstv.com/user-matching?ids=11		0	4/23/2024 11:23:13...	4/23/2024 11:23:12...	1/1/1601 5:30:00 AM	1/1/1601 5:30:00 AM	nginx	HTTP/1.1 302	https://programiz.com	https://doubleclick.net		
11.21.css	https://www.geeksforgeeks.org/wp-content/themes/iconic-o...	text/css	57,503	4/23/2024 11:59:01...	4/23/2024 9:16:44 ...	4/22/2024 11:31:22...	1/1/1601 5:30:00 AM	Apache	HTTP/1.1 200	https://geeksforgeeks.org	https://geeksforgeeks.org	gzip	f_000211
11.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/11.w...	image/webp	10,488	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [6955008]
110.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/110...	image/webp	14,292	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [10657792]
111.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/111...	image/webp	14,384	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:57 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [10690560]
112.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/112...	image/webp	9,086	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:58 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [10706944]
113.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/113...	image/webp	14,790	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:58 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	data_3 [10739712]
114.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/114...	image/webp	22,716	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:58 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	f_0000ac
115.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/115...	image/webp	21,104	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:58 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	f_0000ad
116.webp	https://web.whatsapp.com/emoji/v1/15/1/2/sprite/w/40/116...	image/webp	19,546	4/23/2024 8:44:33 ...	4/23/2024 8:44:31 ...	1/1/1601 5:30:00 AM	4/22/2025 3:41:58 ...		HTTP/1.1 200	https://whatsapp.com	https://whatsapp.com	zstd	f_0000ae

3876 item(s) NirSoft Freeware. https://www.nirsoft.net


history
Start backup
shreyas
history
Search history
New
Sort
View
Details
Home
Gallery
OneDrive - Pers
Desktop
Downloads
Documents
Pictures
Music
Videos
Aditi Shinde
56165165
ADS
Screenshots
Name
Date modified
Type
Size
ChromeHistoryView 4/23/2024 2:57 PM Configuration Sou... 1 KB
ChromeHistoryView 4/23/2024 2:56 PM Compiled HTML ... 17 KB
ChromeHistoryView 4/23/2024 2:56 PM Application 220 KB
readme 4/23/2024 2:56 PM Text Document 10 KB
4 items

NAME: SUYASH SHINDE

ROLL NO: D2223034

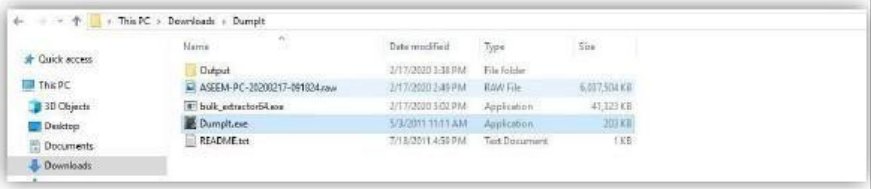
CLASS: CSF 2

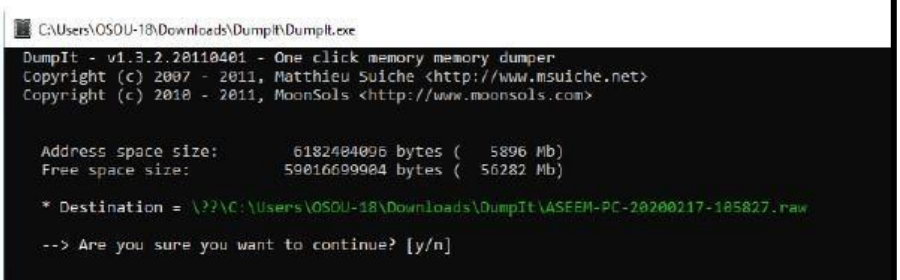
SUBJECT: CFEL

EXPERIMENT 13

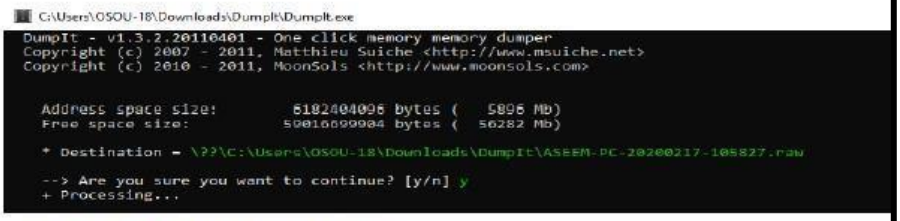
Aim of the Experiment: Email Forensics

SCREENSHOTS:

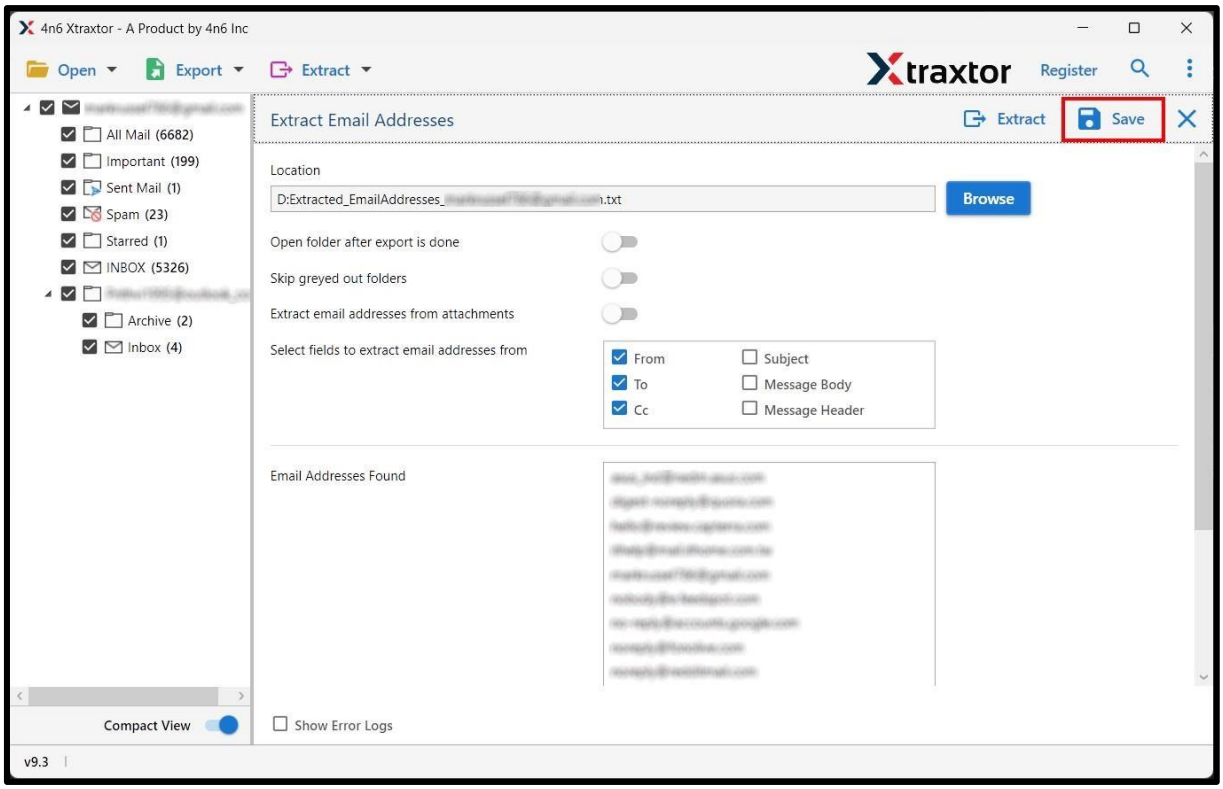


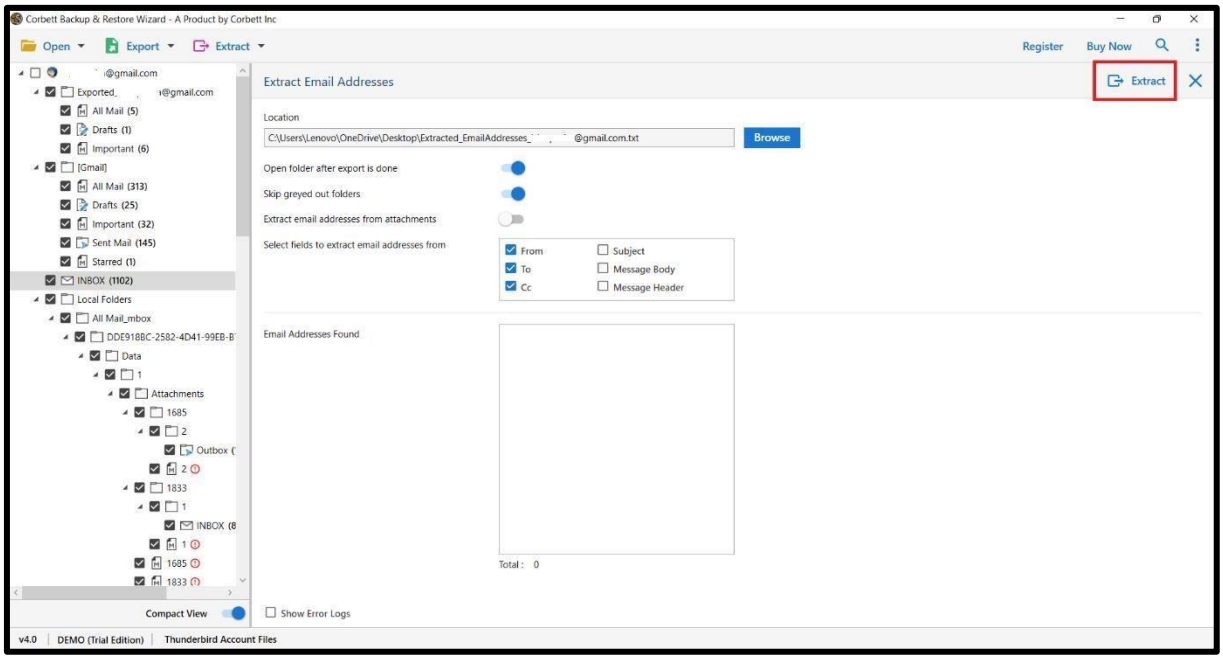


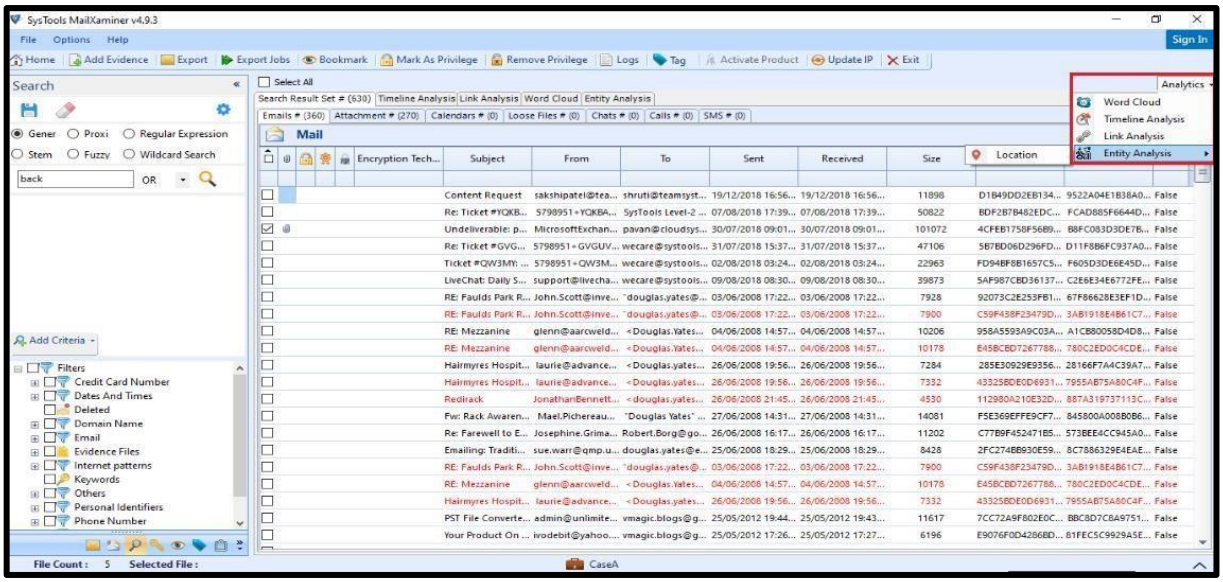
Write 'Y' for processing

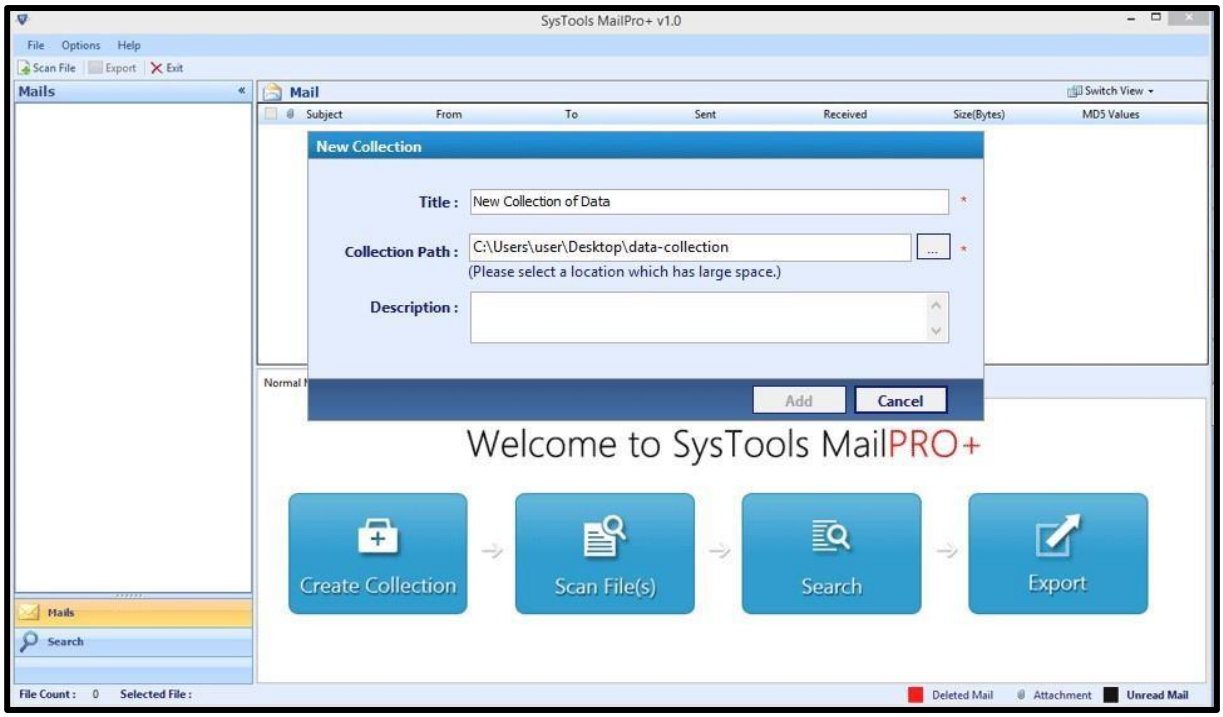


The output RAW file will be as follows


4n6 Xtraxtor - A Product by 4n6 Inc
Open
Export
Extract
Xtraxtor
Register
All Mail (6682)
Important (199)
Sent Mail (1)
Spam (23)
Starred (1)
INBOX (5326)
Archive (2)
Inbox (4)
Extract Email Addresses
Extract
Save
Location
D:Extracted_EmailAddresses_
.txt
Browse
Open folder after export is done
Skip greyed out folders
Extract email addresses from attachments
Select fields to extract email addresses from
From
To
Cc
Subject
Message Body
Message Header
Email Addresses Found
Compact View
Show Error Logs
v9.3


Corbett Backup & Restore Wizard - A Product by Corbett Inc
Open
Export
Extract
Register
Buy Now
Exported_
All Mail (5)
Drafts (1)
Important (6)
[Gmail]
All Mail (313)
Drafts (25)
Important (32)
Sent Mail (145)
Starred (1)
INBOX (1102)
Local Folders
All Mail_mbox
Data
Attachments
1685
1833
Extract Email Addresses
Extract
Location
C:\Users\Lenovo\OneDrive\Desktop\Extracted_EmailAddresses_
@gmail.com.txt
Browse
Open folder after export is done
Skip greyed out folders
Extract email addresses from attachments
Select fields to extract email addresses from
From
To
Cc
Subject
Message Body
Message Header
Email Addresses Found
Total : 0
Compact View
Show Error Logs
v4.0
DEMO (Trial Edition)
Thunderbird Account Files


SysTools MailXaminer v4.9.3
File Options Help
Sign In
Home Add Evidence Export Export Jobs Bookmark Mark As Privilege Remove Privilege Logs Tag Activate Product Update IP Exit
Search
Select All
Search Result Set # (630) Timeline Analysis Link Analysis Word Cloud Entity Analysis
Emails # (360) Attachment # (270) Calendars # (0) Loose Files # (0) Chats # (0) Calls # (0) SMS # (0)
Analytics
Word Cloud
Timeline Analysis
Link Analysis
Entity Analysis
Mail
Encryption Tech... Subject From To Sent Received Size
Location
Add Criteria
Filters
Credit Card Number
Dates And Times
Deleted
Domain Name
Email
Evidence Files
Internet patterns
Keywords
Others
Personal Identifiers
Phone Number
File Count : 5 Selected File :
CaseA


SysTools MailPro+ v1.0
File Options Help
Scan File Export Exit
Mails
Mail
Switch View
Subject From To Sent Received Size(Bytes) MD5 Values
New Collection
Title : New Collection of Data
Collection Path : C:\Users\user\Desktop\data-collection
(Please select a location which has large space.)
Description :
Add Cancel
Welcome to SysTools MailPRO+
Create Collection
Scan File(s)
Search
Export
Mails
Search
File Count : 0 Selected File :
Deleted Mail Attachment Unread Mail

NAME: SUYASH SHINDE

ROLL NO: D22230

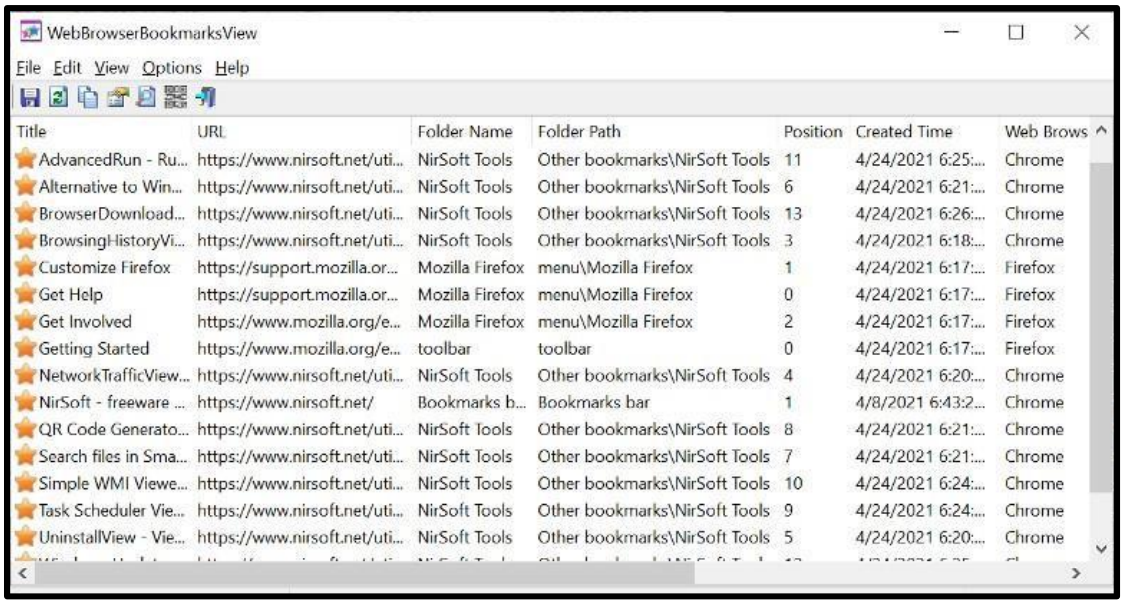
CLASS: CSF 2

SUBJECT: CFEL

EXPERIMENT 14

AIM: Web Browser Forensics

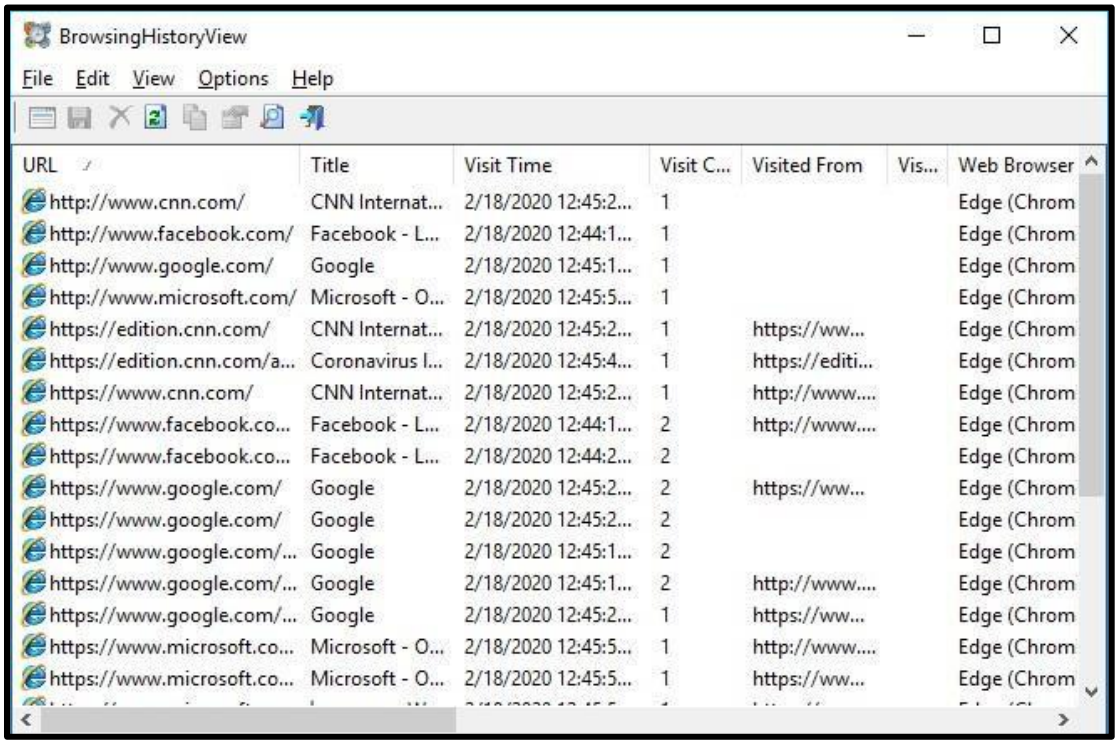
SCREENSHOTS:



WebBrowserBookmarksView

File Edit View Options Help

Title	URL	Folder Name	Folder Path	Position	Created Time	Web Brows
AdvancedRun - Ru...	https://www.nirsoft.net/uti...	NirSoft Tools	Other bookmarks\NirSoft Tools	11	4/24/2021 6:25:...	Chrome
Alternative to Win...	https://www.nirsoft.net/uti...	NirSoft Tools	Other bookmarks\NirSoft Tools	6	4/24/2021 6:21:...	Chrome
BrowserDownload...	https://www.nirsoft.net/uti...	NirSoft Tools	Other bookmarks\NirSoft Tools	13	4/24/2021 6:26:...	Chrome
BrowsingHistoryVi...	https://www.nirsoft.net/uti...	NirSoft Tools	Other bookmarks\NirSoft Tools	3	4/24/2021 6:18:...	Chrome
Customize Firefox	https://support.mozilla.or...	Mozilla Firefox	menu\Mozilla Firefox	1	4/24/2021 6:17:...	Firefox
Get Help	https://support.mozilla.or...	Mozilla Firefox	menu\Mozilla Firefox	0	4/24/2021 6:17:...	Firefox
Get Involved	https://www.mozilla.org/e...	Mozilla Firefox	menu\Mozilla Firefox	2	4/24/2021 6:17:...	Firefox
Getting Started	https://www.mozilla.org/e...	toolbar	toolbar	0	4/24/2021 6:17:...	Firefox
NetworkTrafficView...	https://www.nirsoft.net/uti...	NirSoft Tools	Other bookmarks\NirSoft Tools	4	4/24/2021 6:20:...	Chrome
NirSoft - freeware ...	https://www.nirsoft.net/	Bookmarks b...	Bookmarks bar	1	4/8/2021 6:43:2...	Chrome
QR Code Generato...	https://www.nirsoft.net/uti...	NirSoft Tools	Other bookmarks\NirSoft Tools	8	4/24/2021 6:21:...	Chrome
Search files in Sma...	https://www.nirsoft.net/uti...	NirSoft Tools	Other bookmarks\NirSoft Tools	7	4/24/2021 6:21:...	Chrome
Simple WMI Viewe...	https://www.nirsoft.net/uti...	NirSoft Tools	Other bookmarks\NirSoft Tools	10	4/24/2021 6:24:...	Chrome
Task Scheduler Vie...	https://www.nirsoft.net/uti...	NirSoft Tools	Other bookmarks\NirSoft Tools	9	4/24/2021 6:24:...	Chrome
UninstallView - Vie...	https://www.nirsoft.net/uti...	NirSoft Tools	Other bookmarks\NirSoft Tools	5	4/24/2021 6:20:...	Chrome



BrowsingHistoryView

File Edit View Options Help

URL	Title	Visit Time	Visit C...	Visited From	Vis...	Web Browser
http://www.cnn.com/	CNN Internat...	2/18/2020 12:45:2...	1			Edge (Chrom
http://www.facebook.com/	Facebook - L...	2/18/2020 12:44:1...	1			Edge (Chrom
http://www.google.com/	Google	2/18/2020 12:45:1...	1			Edge (Chrom
http://www.microsoft.com/	Microsoft - O...	2/18/2020 12:45:5...	1			Edge (Chrom
https://edition.cnn.com/	CNN Internat...	2/18/2020 12:45:2...	1	https://ww...		Edge (Chrom
https://edition.cnn.com/a...	Coronavirus I...	2/18/2020 12:45:4...	1	https://editi...		Edge (Chrom
https://www.cnn.com/	CNN Internat...	2/18/2020 12:45:2...	1	http://www....		Edge (Chrom
https://www.facebook.co...	Facebook - L...	2/18/2020 12:44:1...	2	http://www....		Edge (Chrom
https://www.facebook.co...	Facebook - L...	2/18/2020 12:44:2...	2			Edge (Chrom
https://www.google.com/	Google	2/18/2020 12:45:2...	2	https://ww...		Edge (Chrom
https://www.google.com/	Google	2/18/2020 12:45:2...	2			Edge (Chrom
https://www.google.com/...	Google	2/18/2020 12:45:1...	2			Edge (Chrom
https://www.google.com/...	Google	2/18/2020 12:45:1...	2	http://www....		Edge (Chrom
https://www.google.com/...	Google	2/18/2020 12:45:2...	1	https://ww...		Edge (Chrom
https://www.microsoft.co...	Microsoft - O...	2/18/2020 12:45:5...	1	http://www....		Edge (Chrom
https://www.microsoft.co...	Microsoft - O...	2/18/2020 12:45:5...	1	https://ww...		Edge (Chrom

ChromeCacheView: F:\Documents and Settings\Administrator\Local Settings...

File Edit View Options Help

Filename	URL	Content Type	File Size	Last Acc
main.css	http://www.nirsoft.net/main.css	text/css	5,077	04/10/2(
menubg.gif	http://www.nirsoft.net/menubg.gif	image/gif	923	04/10/2(
menutomain.gif	http://www.nirsoft.net/menutomai...	image/gif	805	04/10/2(
new.gif	http://www.nirsoft.net/new.gif	image/gif	157	04/10/2(
nirsoft2.gif	http://www.nirsoft.net/nirsoft2.gif	image/gif	3,694	04/10/2(
nonags1.gif	http://www.nirsoft.net/nonags1.gif	image/gif	1,811	04/10/2(
sofotex.gif	http://www.nirsoft.net/sofotex.gif	image/gif	2,629	04/10/2(
stumble1.png	http://www.nirsoft.net/stumble1.png	image/png	6,300	04/10/2(
toptomain.gif	http://www.nirsoft.net/toptomain.gif	image/gif	805	04/10/2(
update.gif	http://www.nirsoft.net/update.gif	image/gif	195	04/10/2(
index.html	http://www.nirsoft.net/utils/index....	text/html	17,205	04/10/2(

WebCookiesSniffer

File Edit View Options Help

Host Name	Request Path	Total Length	Cookies Co...	Cookies String
www.google.com	/	243	2	PREF=ID=b54f0
us.bc.yahoo.com	/b?P=7gK9O03uv0bA...	616	8	B=c0f448h5ju50t
www.yahoo.com	/p.gif;_ylp=A03uvzF...	1,782	14	B=c0f448h5ju50t
www.yahoo.com	/	914	11	B=c0f448h5ju50t

Name	Value	Index
B	c0f448h5ju50t&b=4&d=lFJpf8B...	0
CH	AgBOgX4QAA4kEAAxCRAADnM...	9
F	a=fzbbTNcMvTOMIPQIJ3NY0t8Y...	1
fpc	d=yRen7og7UZaPiGdUE8FQTdm...	7
FPCK2	AgBOgX4QAFp9EAALLBAAVcEQ...	10
FPCK3	AgBOgX4QAFPcEAB+yxAAb18Q...	8
FPS	dl	4
PH	fn=1lZgJiU.9eZwsRjZbVo-&l=en-...	5
T	z=197OLBJBBVLBBsyIhLfmzo/NiY...	6

NAME: SUYASH SHINDE

ROLL NO: D22230

CLASS: CSF 2

SUBJECT: CFEL

EXPERIMENT 16

AIM: Case Study: Cyber law

Forensic Analysis of Broken and Damaged Mobile Phone – A Crime Case Study

Abstract:

Forensic labs often encounter damaged mobile devices, either intentionally tampered with to destroy evidence or accidentally exposed to harm. While the chip-off technique is effective for data retrieval, modern mobiles' full disk or file-based encryption complicates this method. However, if encryption is hardware-based, restoring the device to its original state enables successful decryption, allowing access to user data for investigation. This paper presents a case study of recovering data from a severely damaged mobile phone by diagnosing and replacing its PCB, facilitating decryption and data retrieval. Keywords: Full Disk Encryption, File Based Encryption, Decryption, PCB, damaged mobile phone, UFED Touch 2, Physical Analyzer, forensic repair toolkit.

I. INTRODUCTION

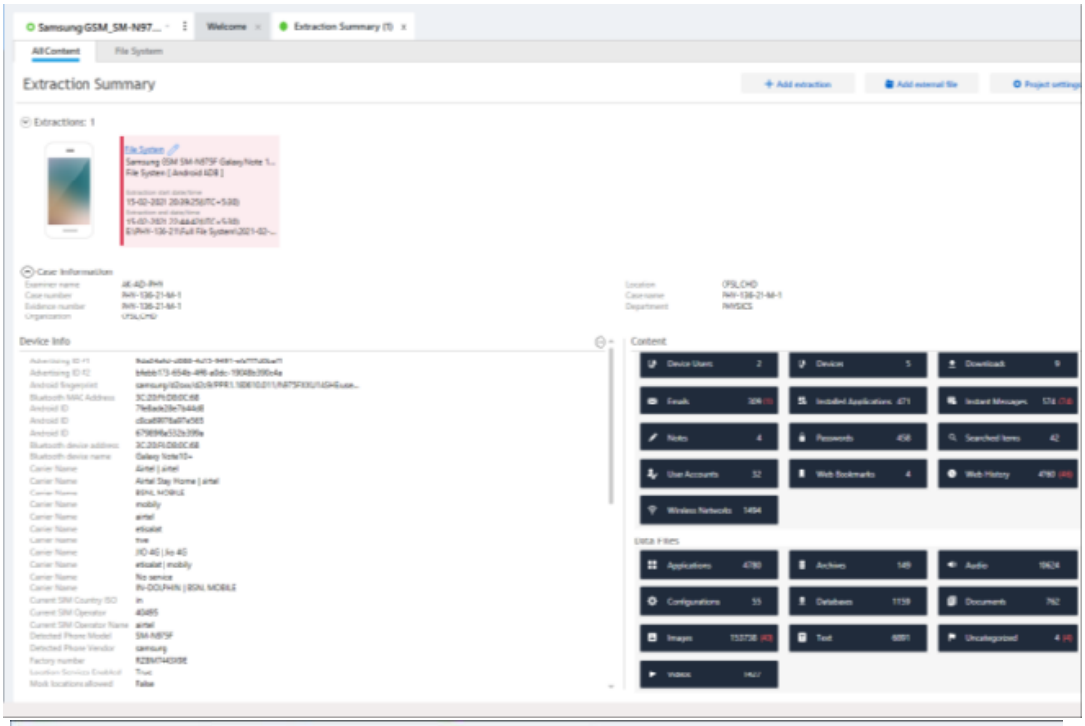
Today's world is an era of accelerated technological progress characterized by new innovations whose rapid application and diffusion typically cause an abrupt change in society. The evolution of computer, mobile, networks, the devices that run on them and their everyday services occur at an amazing rate. It is unthinkable to consider our lives without mobile phones. Mobile phones have been one of the most successful technologies ever invented and adopted in the ever-developing world. Apart from making everyday life easy, mobile phones, computers and internet are most common weapons used by criminals to commit heinous crimes (McSweeney, 2020). These weapons are commonly collected evidences in cybercrimes that are examined by investigators. Sometimes criminals intentionally damage their mobile phones and computers to destroy the evidence. Therefore, it's becoming more challenging for an investigator/ examiner to extract data from the evidences (Dongan & Akbal, 2017).

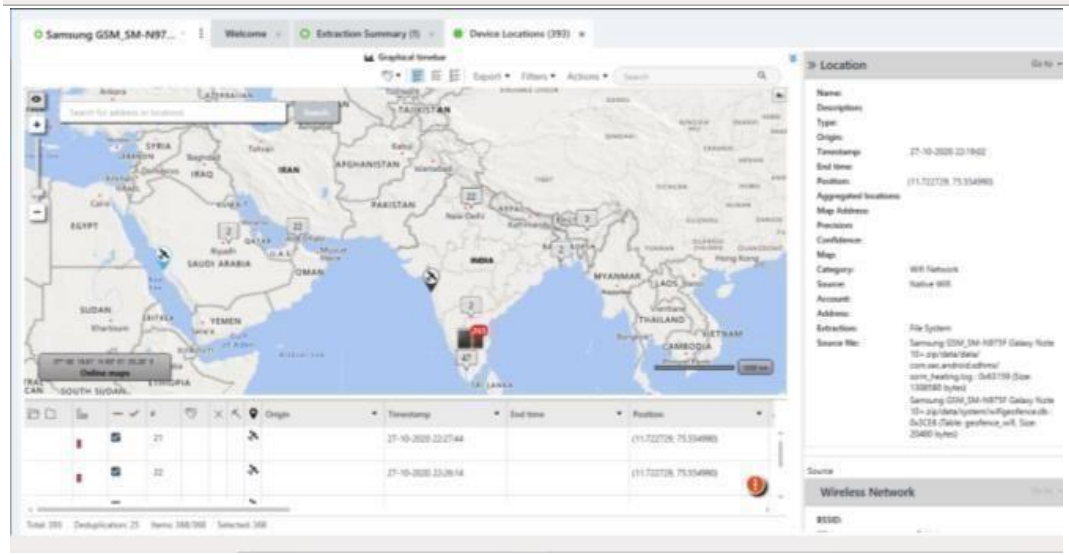
I III. RESULTS AND DISCUSSION

The extracted data comprised of contacts, call logs, messages, multimedia artifacts (images, videos, documents, etc.), internet browsing history and application data of social media accounts including WhatsApp, Facebook, Telegram, etc. (Fig. 7). This entire data was provided to the case forwarding authority along with a hard-copy report.

1.5 Extraction of data:

The device once opened with the pattern provided by the forwarding authority, it was immediately kept on airplane mode. Furthermore, USB debugging was enabled and other necessary settings to enter the extraction mode were followed.





I. CONCLUSION

In the beginning of the case, the forwarding authorities were stumped by the ingenious planning of the smugglers who had left no clues behind that could directly connect them to the crime. The suspects had already managed to destroy any implicating evidence of the crime and had even tried to destroy their mobile devices. However, the innovative and industrious efforts of the scientific officers of the case enabled a complete restoration of the mobile device. The forwarding authority's invaluable support by providing the password and an intricate work in repairing the device by the scientific officer led to the successful solution of the case. This helped the authorities to convict the suspects and provided corroborative evidence of the crime.