

---

# COMP2310

---

Assignment - 1



APRIL 19, 2021

SUJITH BELLAM

45664455

## Abstract

This report contains a forensic analysis of the DD images generated from the suspect's seized laptop. ASIO is the organisation that is responsible for the security of the country and its citizens from espionage, sabotage, terrorism, attacks on defense systems, etc. [1]. ASIO provided DD images and EnCase images, both of these images have the same MD5 hash suggesting that the images are the exact copies of the suspect's hard disk. This report only shows the usage of the DD images, but the results are as exact and accurate as of the EnCase images. This report contains the forensic analysis of the OS, registered user, installed applications, email applications, email addresses, and external drives.

## Table of Contents

Abstract.....	1
Acquisition .....	2
Q2. What operating system is installed? What is the installation date of the operating system and who is the registered owner? .....	3
Answer: .....	3
Analysis: .....	3
Evidence Analysed: .....	3
Steps Taken: .....	3
Q6. What applications were installed by the suspect after installing the operating system? .....	5
Answer: .....	5
Analysis: .....	6
Evidence Analysed: .....	6
Steps Taken: .....	6
Q10. What application was used for e-mail communication? .....	8
Answer: .....	8
Analysis: .....	8
Evidence Analysed: .....	9
Steps Taken: .....	9

Q14. What was the e-mail account used by the suspect?.....	17
Answer: .....	17
Analysis: .....	18
Evidence Analysed: .....	18
Steps Taken: .....	18
Q18. List external storage devices attached to the notebook. What files were copied from notebook to USB drive?.....	24
Answer: .....	24
Analysis: .....	24
Evidence Analysed: .....	24
Steps Taken: .....	24
Conclusion.....	25
References .....	26
Glossary.....	26
Appendixes.....	27

## Acquisition

The Australian Security Intelligence Organisation (ASIO) caught a suspect in January 2016. The suspect was tracked down by the cell phone triangulation technology, CCTV footage, and other bills that lead up to Macquarie Shopping Centre. ASIO seized the suspect's laptop and created a DD Image in eight parts, notes, and an Encase Image in 2 parts. The MD5 hash for both the DD images (suspect 1) and Encase Images (1) is aee4fcd9301c03b3b054623ca261959a tells that both the images are the same. I used Autopsy 4.18.0 to conduct the forensic analysis with Windows 10 Pro operating system. I am using lightshot software to capture snapshots and Microsoft Word to generate this report.

Q2. What operating system is installed? What is the installation date of the operating system and who is the registered owner?

Answer:

The installed OS is Microsoft Windows XP. The installation date of the OS is 19<sup>th</sup> August 2004 at 22:48:27 IST. The registered owner of the OS is Greg Schardt.

Analysis:

Checking details of Operating System Information and results of the software component contains the answers. The results tab of the software file from the Operating Information Systems contains the information on the OS.

Evidence Analysed:

The screenshot shows the Autopsy interface. At the top, a table lists results for 'Operating System Information'. The table has columns: Source File, S, C, O, Name, Domain, Version, Processor Architecture, Temporary Files Directory, Data Source, Program Name, Date/Time, Path, and Product ID. The first row shows 'system' with Name 'N-1A900W6Z0X4LQ', Version 'Windows\_NT', Processor Architecture 'x86', Temporary Files Directory '%SystemRoot%\TEMP', Data Source 'SUSPECT.001', Program Name 'Microsoft Windows XP', Date/Time '2004-08-19 22:48:27 IST', Path 'C:\WINDOWS', and Product ID '55274-640-0147306-23684'. Below the table, the 'Results' tab is selected, showing a detailed view of the first result. The 'Type' is 'Operating System Information'. The 'Value' field contains the following details: Program Name: Microsoft Windows XP, Date/Time: 2004-08-19 22:48:27, Path: C:\WINDOWS, Product ID: 55274-640-0147306-23684, Owner: Greg Schardt, Organization: N/A, Source File Path: /img\_SUSPECT.001/vol\_02/WINDOWS/system32/config/software. The 'Source(s)' column on the right lists 'Recent Activity' for each field.

Source File	S	C	O	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Date/Time	Path	Product ID
system				N-1A900W6Z0X4LQ		Windows_NT	x86	%SystemRoot%\TEMP	SUSPECT.001	Microsoft Windows XP	2004-08-19 22:48:27 IST	C:\WINDOWS	55274-640-0147306-23684

Type	Value	Source(s)
Program Name	Microsoft Windows XP	Recent Activity
Date/Time	2004-08-19 22:48:27	Recent Activity
Path	C:\WINDOWS	Recent Activity
Product ID	55274-640-0147306-23684	Recent Activity
Owner	Greg Schardt	Recent Activity
Organization	N/A	Recent Activity
Source File Path	/img_SUSPECT.001/vol_02/WINDOWS/system32/config/software	Recent Activity

Snapshot 1 - Windows Version Details

Snapshot 1 shows the information that the installed OS is Microsoft Windows XP along with some OS information, including the Date/Time of creation and the name of the owner of the system.

Steps Taken:

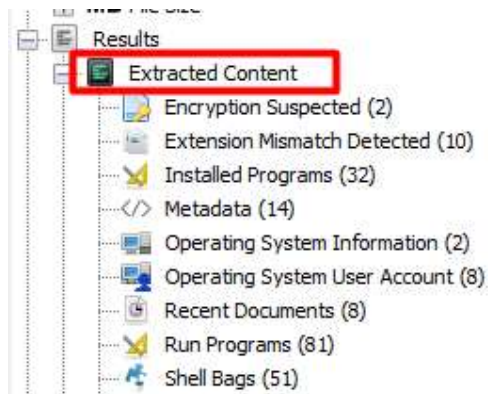
1. Open Autopsy
2. Load the Data Sources from SUSPECT.001 to SUSPECT.008, as Disk Image or VM File

3. Click on the plus button beside Results



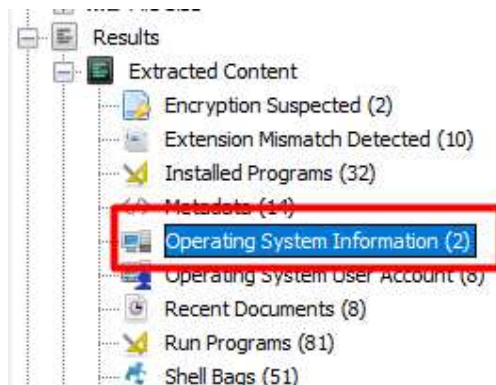
Snapshot 2- Path to OS Information - 1

4. Click on the plus button beside the Extracted Content



Snapshot 3 - Path to OS Information - 2

5. Click on the Operating System Information



Snapshot 4 - Path to OS Information - 3

## 6. Finally, Click on Software

Source File	S	C	O	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Date/Time	Path	Product ID	Owner
system				N:\A9CD66238\1\Q		Windows_NT	x86	%SystemRoot%\TEMP	SUSPECT.001					
software									SUSPECT.001	Microsoft Windows XP	2004-08-19 22:48:27 IST	C:\WINDOWS	55274-640-0147306-23684	Greg Schardt

Snapshot 5 - Path to OS Information – 4

## 7. Answers to the question can be found in the result tab of the software file.

Result: 1 of 56 Result			Operating System Information	
Type	Value	Source(s)		
Program Name	Microsoft Windows XP	Recent Activity		
Date/Time	2004-08-19 22:48:27	Recent Activity		
Path	C:\WINDOWS	Recent Activity		
Product ID	55274-640-0147306-23684	Recent Activity		
Owner	Greg Schardt	Recent Activity		
Organization	N/A	Recent Activity		
Source File Path	/img_SUSPECT.001/vol_vol2/WINDOWS/system32/config/software	Recent Activity		

Snapshot 6 - OS Information

Q6. What applications were installed by the suspect after installing the operating system?

Answer:

The suspect installed fourteen applications after installing the OS, and they are:

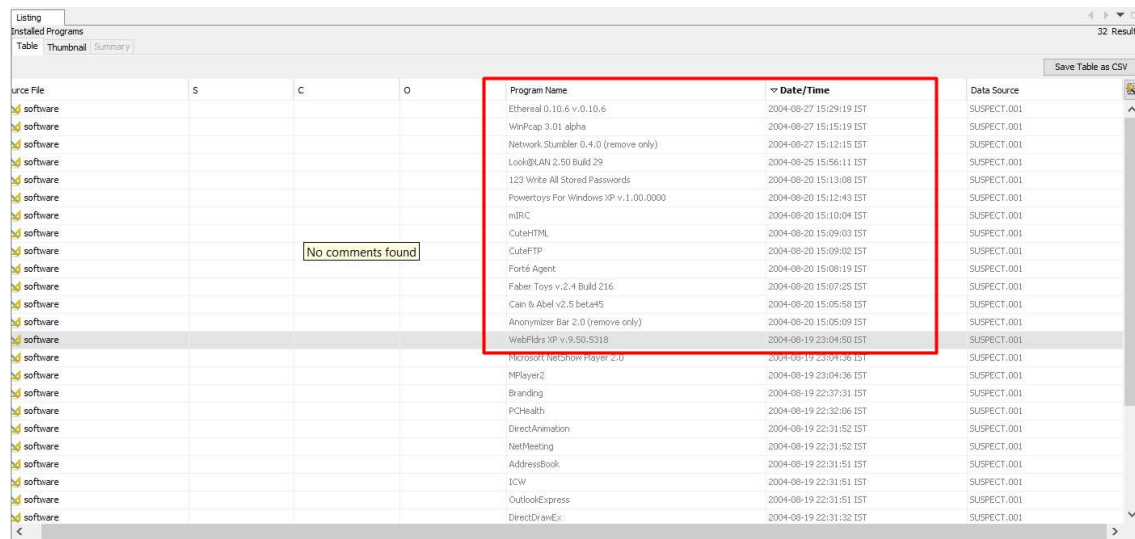
1. Ethereum 0.10.6 v.0.10.6
2. WinPcap 3.01 alpha
3. Network Stumbler 0.4.0 (remove only)
4. Look@LAN 2.50 Build 29
5. 123 Write All Stored Passwords
6. Powertoy For Windows XP v.1.00.0000
7. mIRC
8. CuteHTML
9. CuteFTP
10. Forté Agent
11. Faber Toys v.2.4 Build 216
12. Cain & Abel v2.5 beta45
13. Anonymizer Bar 2.0 (remove only)
14. WebFldrs XP v.9.50.5318

## Analysis:

Checking the Installed Programs under the Extracted Content will give the answer to this question.

Installed Programs shows that there are a total of 32 programs installed on the system. But there are only 14 programs that the suspect installed after installing the OS. The programs, Microsoft NetShow Player 2.0 and MPlayer2, were installed approximately 15 minutes after installing the OS, but both these programs were installed at the same time; this suggests that these two programs were installed by the windows OS after its installation.

## Evidence Analysed:



Source File	S	C	O	Program Name	Date/Time	Data Source
software				Ethereal 0.10.6 v.0.10.6	2004-08-27 15:29:19 IST	SUSPECT.001
software				WinPcap 3.01 alpha	2004-08-27 15:15:19 IST	SUSPECT.001
software				Network Stumbler 0.4.0 (remove only)	2004-08-27 15:12:15 IST	SUSPECT.001
software				Look@LAN 2.50 Build 29	2004-08-25 15:56:11 IST	SUSPECT.001
software				123 Write All Stored Passwords	2004-08-20 15:13:08 IST	SUSPECT.001
software				Powertoyz For Windows XP v.1.00.0000	2004-08-20 15:12:43 IST	SUSPECT.001
software				mIRC	2004-08-20 15:10:04 IST	SUSPECT.001
software				CuteHTML	2004-08-20 15:09:03 IST	SUSPECT.001
software				CuteFTP	2004-08-20 15:09:02 IST	SUSPECT.001
software				Forté Agent	2004-08-20 15:08:19 IST	SUSPECT.001
software				Faber Toys v.2.4 Build 216	2004-08-20 15:07:25 IST	SUSPECT.001
software				Cain & Abel v2.5 beta45	2004-08-20 15:05:58 IST	SUSPECT.001
software				Anonymizer Bar 2.0 (remove only)	2004-08-20 15:05:09 IST	SUSPECT.001
software				WebFlds XP v.9.50.5310	2004-08-19 23:04:50 IST	SUSPECT.001
software				Microsoft NetShow Player 2.0	2004-08-19 23:04:36 IST	SUSPECT.001
software				MPlayer2	2004-08-19 23:04:36 IST	SUSPECT.001
software				Branding	2004-08-19 22:37:31 IST	SUSPECT.001
software				PCHHealth	2004-08-19 22:32:06 IST	SUSPECT.001
software				DirectAnimation	2004-08-19 22:31:52 IST	SUSPECT.001
software				NetMeeting	2004-08-19 22:31:52 IST	SUSPECT.001
software				AddressBook	2004-08-19 22:31:51 IST	SUSPECT.001
software				ICW	2004-08-19 22:31:51 IST	SUSPECT.001
software				OutlookExpress	2004-08-19 22:31:51 IST	SUSPECT.001
software				DirectDrawEx	2004-08-19 22:31:32 IST	SUSPECT.001

Snapshot 7 - Installed Software

Snapshot 7 shows the installed applications from the notebook.

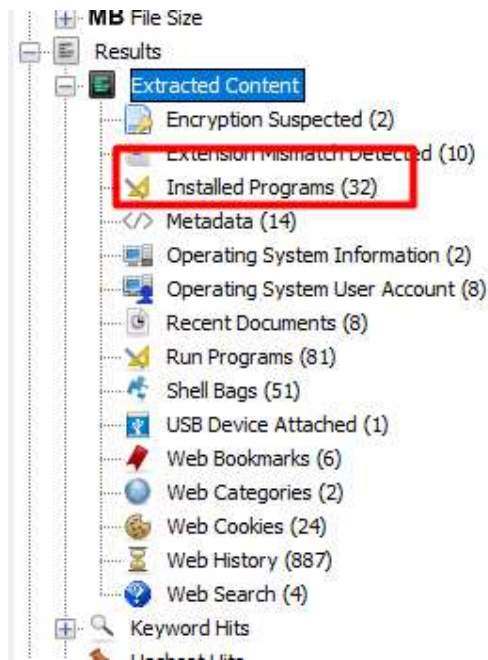
## Steps Taken:

1. Click on the plus button beside Results



Snapshot 8 - Path to Installed Programs - 1

2. Click on the plus button beside the Extracted Content



Snapshot 9 - Path to Installed Programs - 2

### 3. Click on the Installed Programs

A screenshot of a table showing installed programs. The table has columns for Source File, S, C, O, Program Name, Date/Time, and Data Source. The table is sorted by Date/Time in descending order. The first few rows are:

Source File	S	C	O	Program Name	Date/Time	Data Source
software				Ethernet 10.0.0.0 v.0.10.0	2004-08-27 15:09:19 IST	SUSPECT.001
software				WinPcap 3.0.1 alpha	2004-08-27 15:15:19 IST	SUSPECT.001
software				Network Scanner 5.4.0 (remove only)	2004-08-27 15:12:15 IST	SUSPECT.001
software				LoadLAW 1.20 Build 29	2004-08-26 15:06:11 IST	SUSPECT.001
software				123 Write All Stored Passwords	2004-08-20 15:13:00 IST	SUSPECT.001
software				PowerToys For Windows XP v.1.00.0000	2004-08-20 15:12:43 IST	SUSPECT.001
software				nBIC	2004-08-20 15:10:04 IST	SUSPECT.001
software				QuemTMS	2004-08-20 15:09:03 IST	SUSPECT.001
software				QuemTMS	2004-08-20 15:09:02 IST	SUSPECT.001
software				Port Agent	2004-08-20 15:08:19 IST	SUSPECT.001
software				Fiber Toys v.2.4 Build 216	2004-08-20 15:07:25 IST	SUSPECT.001
software				Can & Abel v.2.5 beta05	2004-08-20 15:06:50 IST	SUSPECT.001
software				Anonymous Bar 2.0 (remove only)	2004-08-20 15:06:09 IST	SUSPECT.001
software				WebPds SP v.5.50.5310	2004-08-19 23:04:30 IST	SUSPECT.001
software				Microsoft Windows Player 2.0	2004-08-19 23:04:30 IST	SUSPECT.001
software				MPower2	2004-08-19 23:04:30 IST	SUSPECT.001
software				Branding	2004-08-19 22:37:31 IST	SUSPECT.001
software				PCHHealth	2004-08-19 22:32:06 IST	SUSPECT.001
software				DirectMedia	2004-08-19 22:31:52 IST	SUSPECT.001
software				NetWorking	2004-08-19 22:31:42 IST	SUSPECT.001
software				AddressBook	2004-08-19 22:31:51 IST	SUSPECT.001
software				ICW	2004-08-19 22:31:51 IST	SUSPECT.001
software				OutlookExpress	2004-08-19 22:31:51 IST	SUSPECT.001
software				DirectMedia	2004-08-19 22:31:52 IST	SUSPECT.001
software				Frontiers	2004-08-19 22:31:52 IST	SUSPECT.001
software				ICW	2004-08-19 22:31:52 IST	SUSPECT.001
software				ICWData	2004-08-19 22:31:52 IST	SUSPECT.001
software				ICWData	2004-08-19 22:31:52 IST	SUSPECT.001
software				ICWData	2004-08-19 22:31:52 IST	SUSPECT.001
software				MobileOptionP	2004-08-19 22:31:52 IST	SUSPECT.001
software				SchedulingAgent	2004-08-19 22:31:52 IST	SUSPECT.001
software				Connection Manager	2004-08-19 22:31:41 IST	SUSPECT.001

Snapshot 10 - Installed Programs

### 4. Click on the Date/Time field to sort them in descending order



	▼ Date/Time	Data So
	2004-08-27 15:29:19 IST	SUSPEC
	2004-08-27 15:15:19 IST	SUSPEC
	2004-08-27 15:12:15 IST	SUSPEC
	2004-08-25 15:56:11 IST	SUSPEC
	2004-08-20 15:13:08 IST	SUSPEC
	2004-08-20 15:12:43 IST	SUSPEC
	2004-08-20 15:10:04 IST	SUSPEC
	2004-08-20 15:09:03 IST	SUSPEC
	2004-08-20 15:09:02 IST	SUSPEC
	2004-08-20 15:08:19 IST	SUSPEC
	2004-08-20 15:07:25 IST	SUSPEC
	2004-08-20 15:05:58 IST	SUSPEC
	2004-08-20 15:05:09 IST	SUSPEC

*Snapshot 11 - Sorting the Date for Installed Programs*

Only the installed programs with the date and time after 2004-08-19 22:48:27 IST are the programs installed by the suspect.

## Q10. What application was used for e-mail communication?

Answer:

There are five applications used for email communication by the suspect, and they are:

1. Forte Agent (Application)
2. Hotmail (Application)
3. MSN Explorer (Application)
4. Outlook Express (Application)
5. Yahoo Mail from Web Browser

However, only Forte Agent and Yahoo Mail have evidence suggesting that they were used.

Analysis:

I used Autopsy and Excel to find out all the mail applications that were installed or used by the suspect. We choose SUSPECT.001 because it is the DD image containing the OS and its files. The Mail folder under the software registry file had the data relating to the Email applications in the OS. Web History option under Results has the web history of the suspect. The web history gave information of

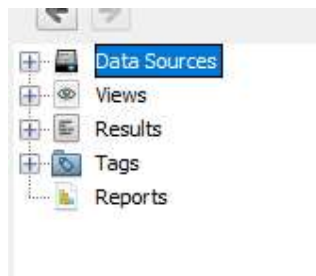
### Evidence Analysed:

[illegible]

Snapshot 13 shows that the suspect used Yahoo Mail from the web browser.

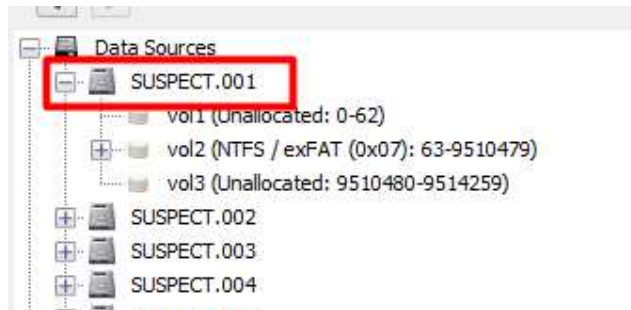
### Steps Taken:

1. Click on the plus button beside the Data Sources



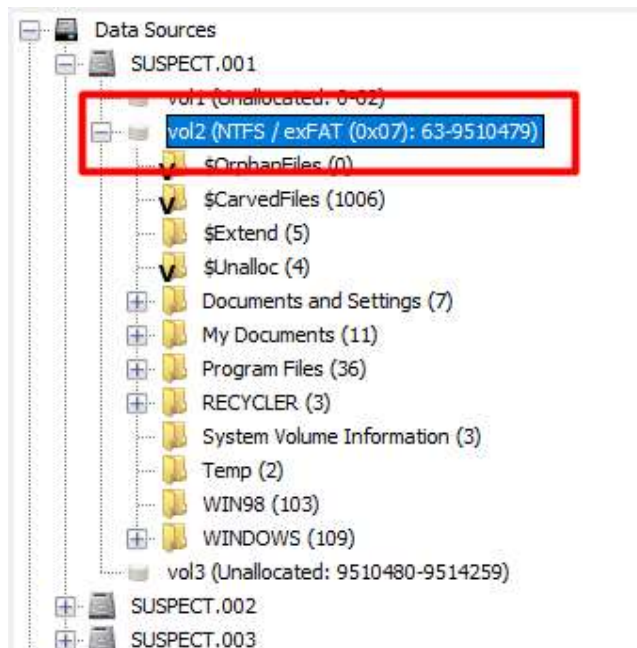
Snapshot 14 - Getting information on applications used for Email Communications – 1

2. Click on the plus button beside SUSPECT.001 data source



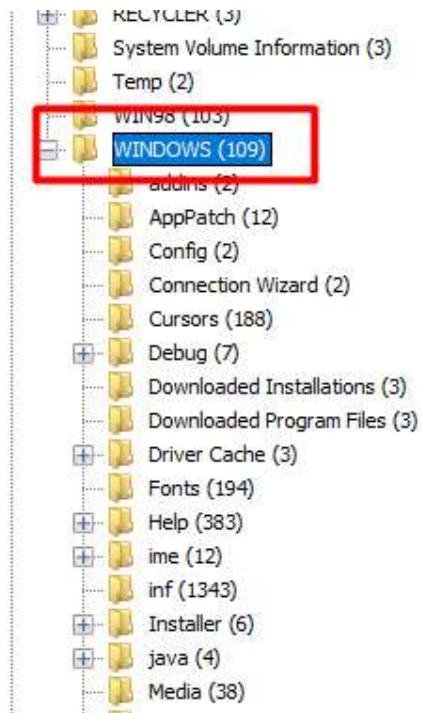
Snapshot 15 - Getting information on applications used for Email Communications – 2

3. Click on the plus button beside vol2 (NTFS / exFAT (0x07): 63-9510479) disk



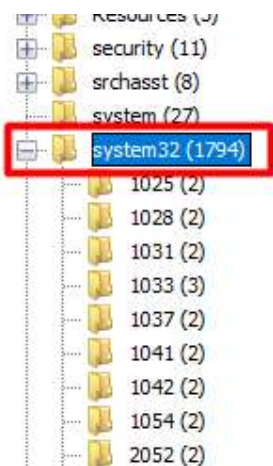
Snapshot 16 - Getting information on applications used for Email Communications – 3

4. Click on the plus button beside the WINDOWS folder



Snapshot 17- Getting information on applications used for Email Communications – 4

5. Click on the plus button beside the system32 folder



Snapshot 18- Getting information on applications used for Email Communications – 5

6. Click on the config folder



Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
systemprofile				2004-08-20 04:18:25 IST	2004-08-20 04:18:25 IST	2004-08-27 21:01:27 IST	2004-08-20 04:18:25 IST	56	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
AppEvent.Evt		1		2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-19 22:29:14 IST	65536	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
default		1		2004-08-27 21:16:33 IST	2004-08-20 04:23:22 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	262144	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
default.LOG		1		2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
default.sav		1		2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	90112	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
SAM		1		2004-08-27 21:16:33 IST	2004-08-20 04:05:21 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
SAM.LOG		1		2004-08-27 20:38:23 IST	2004-08-27 20:38:23 IST	2004-08-27 20:38:23 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
SecEvent.Evt		1		2004-08-19 22:29:15 IST	2004-08-19 22:32:15 IST	2004-08-19 22:29:15 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
SECURITY		1		2004-08-27 21:16:33 IST	2004-08-20 04:04:03 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
SECURITY.LOG		1		2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
software		1		2004-08-27 21:16:33 IST	2004-08-27 20:59:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	8650752	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
software.LOG		1		2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
software.sav		2		2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	630794	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
systemEvent.Evt		1		2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
system		1		2004-08-27 21:16:33 IST	2004-08-27 21:01:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:06 IST	2621440	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
system.LOG		1		2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
system.sav		2		2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	389120	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
TempKey.LOG		1		2004-08-19 22:26:18 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:14 IST	1024	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
userdiff		1		2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:08 IST	262144	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
userdiff.LOG		1		2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3
userdiff.LOG		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	0	Unallocated		unknown	/img_SUSPECT.001/vol_vo2/WINDOWS/system3

Hex

Text

Application

File Metadata

Context

Results

Annotations

Other Occurrences

\$\$\$PROTO.HIV

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

+

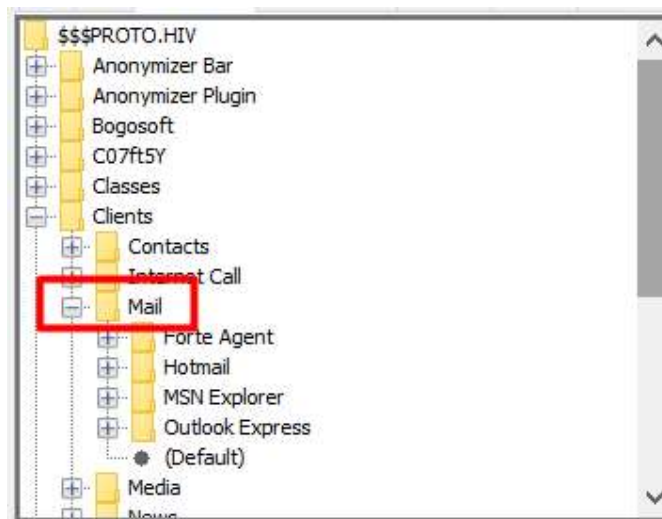
+

+

+

Snapshot 21- Getting information on applications used for Email Communications – 8

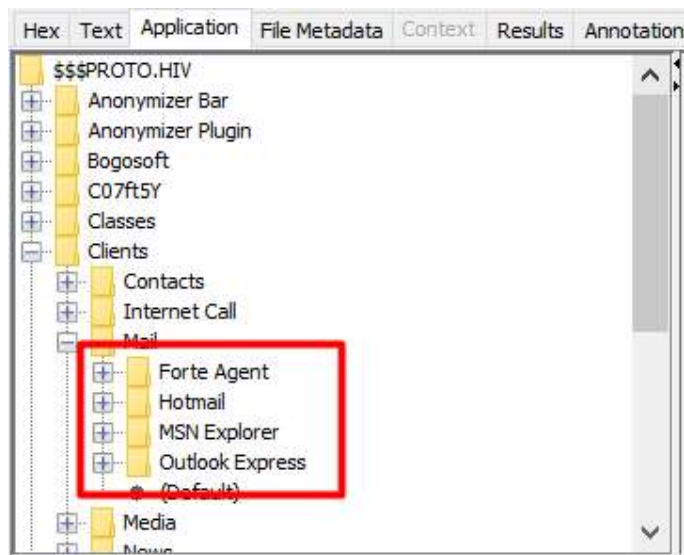
- Click in the plus button beside the Mail folder



Snapshot 22- Getting information on applications used for Email Communications – 9

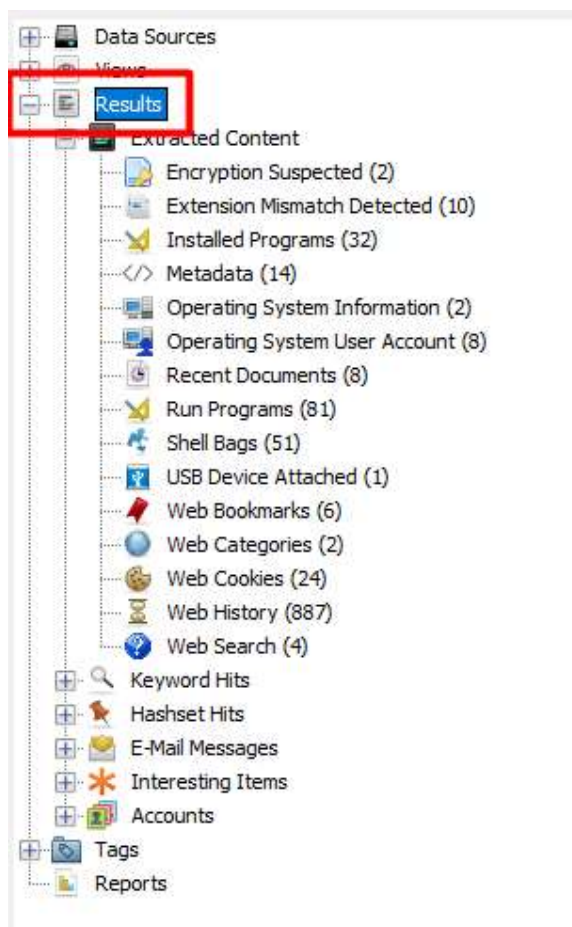
- The subfolders in the Mail folder contain the Email applications installed by the suspect





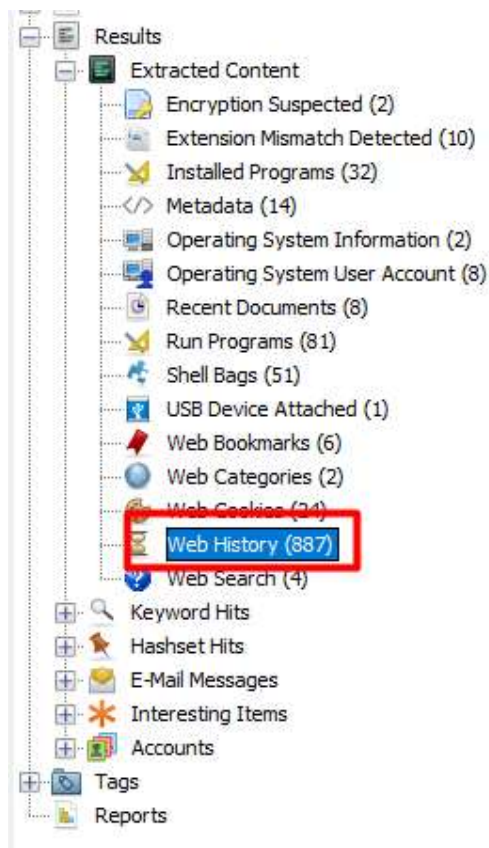
Snapshot 23- Getting information on applications used for Email Communications – 10

# 11. Click on the plus button beside Results



Snapshot 24 - Finding the email website accessed with a web browser - 1

## 12. Click on Web History



Snapshot 25 - Finding the email website accessed with a web browser - 2

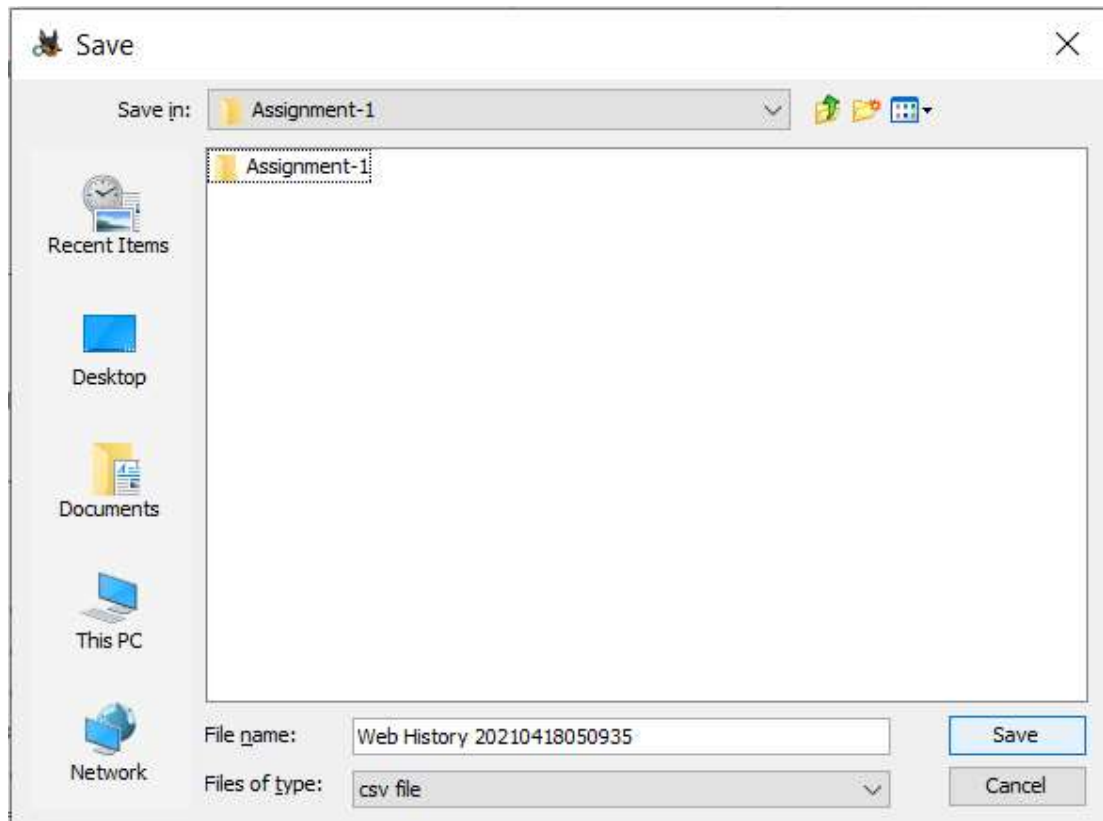
13. The tab on the right side will show all the web history for the suspect's web browser. Click on Save Table as CSV to export the web results.

[illegible]

Snapshot 26 - Finding the email website accessed with a web browser - 3

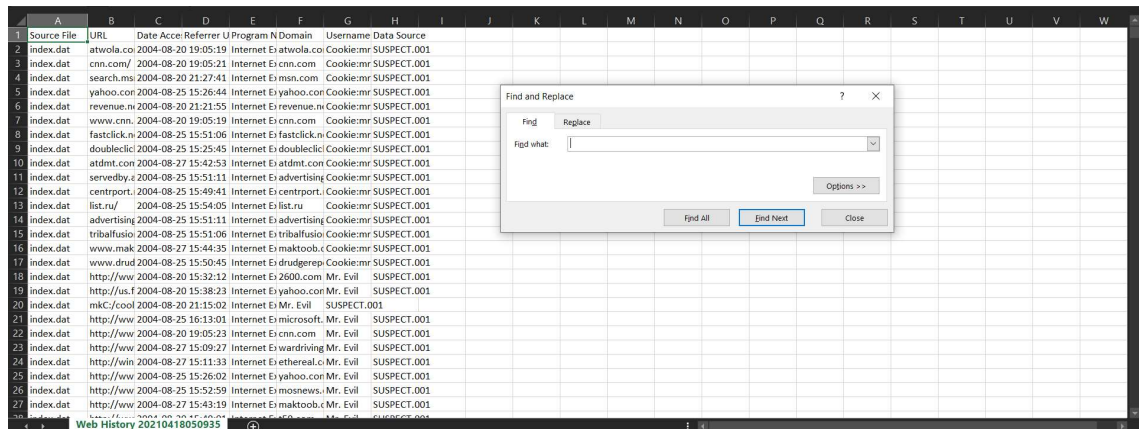
14. Save the Excel file and open it.





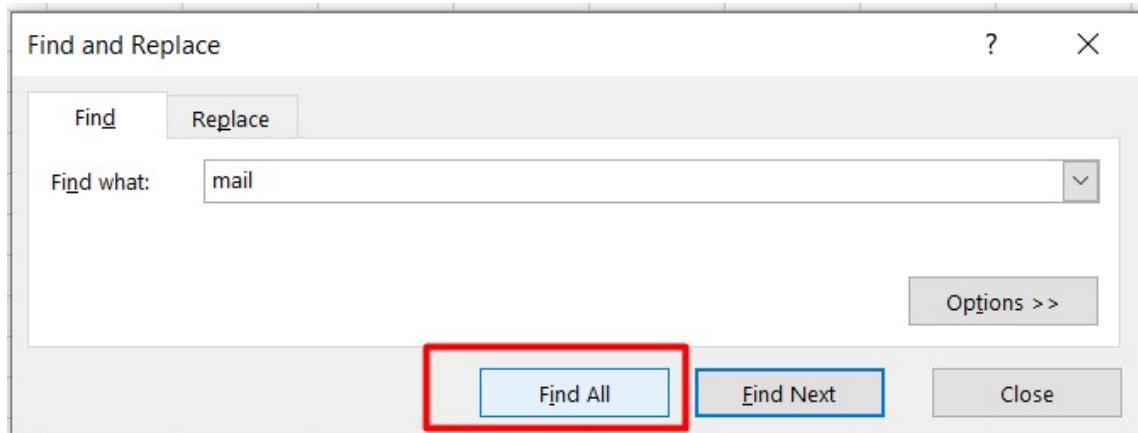
Snapshot 27 - Finding the email website accessed with a web browser - 4

15. Press ctrl+f to open find dialog box on the excel sheet



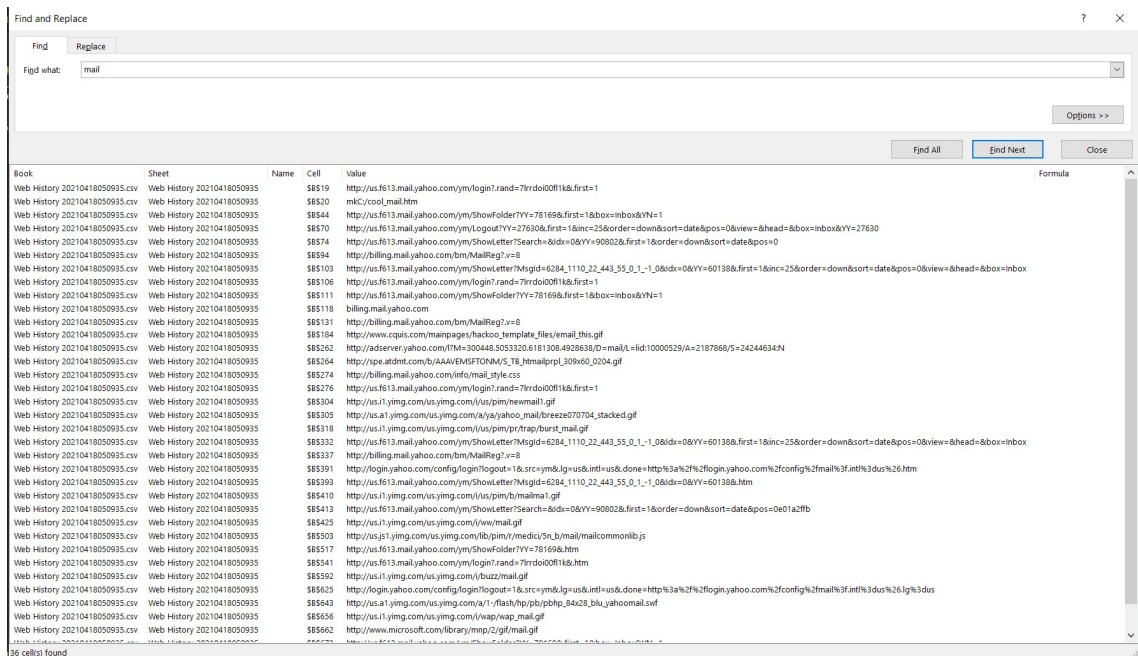
Snapshot 28 - Finding the email website accessed with a web browser - 5

16. Type mail in the box and click on Find All button



Snapshot 29 - Finding the email website accessed with a web browser - 7

17. Now we can see the history that contains the word mail



Snapshot 30 - Finding the email website accessed with a web browser - 8

The suspect accessed only Yahoo Mail.

Q14. What was the e-mail account used by the suspect?

Answer:

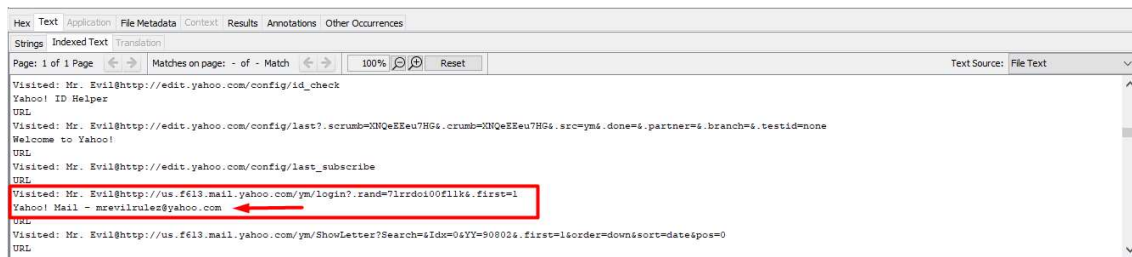
The suspect used two Email addresses, they are:

1. [whoknowsme@sbcglobal.net](mailto:whoknowsme@sbcglobal.net) (Forte Agent)
2. [mrevilrulez@yahoo.com](mailto:mrevilrulez@yahoo.com) (Yahoo Mail)

## Analysis:

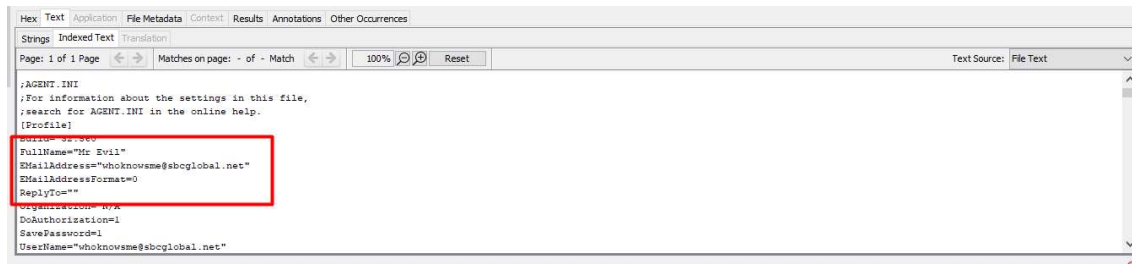
Going through the web history gave the email address used by the suspect. The web history with the domain yahoo and the URL containing the keyword login is the best place to look for the email address. As Forte Agent is an application installed on the system, going through the Program Files in SUSPECT.001 can give data and files related to Forte Agent. Agent folder from Program Files contains the data of the Forte Agent application. The Data folder from the Agent folder has the file AEGNT.ini which has the email address used by the suspect in the Forte Agent application.

## Evidence Analysed:



### Snapshot 31- Yahoo Mail Email Address

From snapshot 31, we can find the email address used by the suspect to log in to the yahoo mail.



### Snapshot 32 - Forte Agent Email Address

From snapshot 32, we can find the email address used by the suspect to log in and use Forte Agent.

## Steps Taken:

1. Do steps 11 and 12 from Q6.
2. Click on Domain to view the URL in Descending order (easier to find yahoo domain)

Save Table as CSV										
Source File	S	C	O	URL	Date Accessed	Referrer URL	Program Name	Domain	Username	Data Source
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/ldr/eh/uh_bk.gif	2004-08-25 15:26:05 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/medic/all/sort_dh_1.gif	2004-08-20 15:38:26 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.a1.yimg.com/us.yimg.com/s/ya/yahoo_domain/umbrella_super_v3_081604.jpg	2004-08-20 15:38:31 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/medic/blue/shd_j_1.gif	2004-08-20 15:38:40 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/medic/blue/rc_vwc35_sw_1.gif	2004-08-20 15:38:42 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			https://sec.yimg.com/us.yimg.com/lt/reg/yh.css	2004-08-20 15:38:47 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/et/bub1.gif	2004-08-20 15:38:21 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/dtct1.gif	2004-08-20 15:38:40 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/medic/all/qd_b_1.gif	2004-08-20 15:38:26 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.a1.yimg.com/us.yimg.com/s/lf/freeze/f6104_728_jsp_backugames.gif	2004-08-20 15:38:27 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/medic/blue/rc_vwc35_ne_1.gif	2004-08-20 15:38:42 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/et/echw465_50.jpg	2004-08-25 15:26:08 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/trap/em2_cr7.gif	2004-08-20 15:38:31 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/et/spacer.gif	2004-08-20 15:38:55 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.a1.yimg.com/us.yimg.com/s/vo/vonage/logo_25x25.gif	2004-08-20 15:38:41 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/et/spacer.gif	2004-08-25 15:25:43 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/trap/3box_2.jpg	2004-08-20 15:34:19 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/et/shft1.gif	2004-08-20 15:38:41 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.a1.yimg.com/us.yimg.com/s/aco/compaq/powdayhp_blu_84x28_yahoo.gif	2004-08-25 15:25:43 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.i1.yimg.com/us.yimg.com/us/pin/r/medic/blue/shd_m_1.gif	2004-08-20 15:38:40 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat	1			http://us.a1.yimg.com/us.yimg.com/s/aco/consumer_info/cc_b_25x25_0803_3.gif	2004-08-20 15:38:40 IST		Internet Explorer	yimg.com		SUSPECT.00

Snapshot 33 - Finding suspects Yahoo Mail email address - 1

### 3. Scroll down to the yahoo domain

Listing										887 Results	
Web History											
Thumbnail Summary											
Save Table as CSV											
Source File	S	C	O	URL	Date Accessed	Referrer URL	Program Name	Domain	Username	Data Source	
index.dat			1	http://us.i1.yimg.com/us.yimg.com/us/pin/r/medic/all/bt_b_dh_2.gif	2004-08-20 15:38:30 IST		Internet Explorer	yimg.com		SUSPECT.00	
index.dat			1	http://us.i1.yimg.com/us.yimg.com/us/pin/r/trap/em2_cr3.gif	2004-08-20 15:38:31 IST		Internet Explorer	yimg.com		SUSPECT.00	
index.dat			1	http://us.a1.yimg.com/us.yimg.com/s/flash/chrysler/JH0824_300x100.swf?clickTAG=...	2004-08-25 15:25:45 IST		Internet Explorer	yimg.com		SUSPECT.00	
index.dat			1	http://us.i1.yimg.com/us.yimg.com/lib/pin/r/medic/5n_b/mail/us/mail_blue_all.css	2004-08-20 15:38:38 IST		Internet Explorer	yimg.com		SUSPECT.00	
index.dat			1	http://us.i1.yimg.com/us.yimg.com/us/pin/r/trap/em2_cr1.gif	2004-08-20 15:38:30 IST		Internet Explorer	yimg.com		SUSPECT.00	
index.dat			1	http://us.i1.yimg.com/us.yimg.com/lib/common/yv_css_cstate.js	2004-08-25 15:26:05 IST		Internet Explorer	yimg.com		SUSPECT.00	
index.dat			1	http://us.i1.yimg.com/us.yimg.com/lib/w/dh_2.gif	2004-08-25 15:25:44 IST		Internet Explorer	yimg.com		SUSPECT.00	
index.dat			1	yahoo.com	2004-08-25 15:26:44 IST		Internet Explorer	yahoo.com	Cookie:mr_evil	SUSPECT.00	
index.dat			1	http://us.f613.mail.yahoo.com/m/login?rand=7mdo00f11&first=1	2004-08-20 15:38:23 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://www.yahoo.com/_ylt=X3c0MTB1M2EzYWF0eF9Ta2t3MTYxNDkEdGZzZDAMwBHRt...	2004-08-25 15:26:02 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://edtf.yahoo.com/config/eval_register?v=0&id=0&new=1&done=0&src=yml&part...	2004-08-20 15:34:27 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://us.f613.mail.yahoo.com/m/ShowFolder?Y=78169&first=1&box=1&box3Y=1	2004-08-20 15:38:27 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://edtf.yahoo.com/config/id_check	2004-08-20 15:35:47 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://edtf.yahoo.com/config/register?	2004-08-20 15:38:01 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://us.f613.mail.yahoo.com/m/logout?Y=27630&first=1&inc=25&border=down&so...	2004-08-20 15:38:45 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://story.news.yahoo.com/news?tmpl=story&cid=5648&ncid=5648&e=1&u=/nn/2004...	2004-08-25 15:26:09 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://us.f613.mail.yahoo.com/m/ShowLetter?Search=0&id=0&Y=90802&first=1&cor...	2004-08-20 15:38:34 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://www.yahoo.com/_ylt=X3c0MTB1M2EzYWF0eF9Ta2t3MTYxNDkEdGZzZDAMwBHRt...	2004-08-20 15:34:16 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://www.yahoo.com	2004-08-25 15:25:45 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://edtf.yahoo.com/config/last_subscribe	2004-08-20 15:38:11 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	
index.dat			1	http://edtf.yahoo.com/config/last?scrumb=1NqeEEu7HG8&crumb=1NqeEEu7HG8&src...	2004-08-20 15:38:07 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00	

Snapshot 34 - Finding suspects Yahoo Mail email address - 2

### 4. Select the web history that contains login as the keyword

Listing										
Web History										
Table Thumbnail Summary										
Save Table as CSV										
Source File	S	C	O	URL	Date Accessed	Referrer URL	Program Name	Domain	Username	Data Source
index.dat			1	http://us.i1.yimg.com/us.yimg.com/l/us/pim/r/medic/all/bt_b_dd_2.gif	2004-08-20 15:38:30 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.i1.yimg.com/us.yimg.com/l/us/pim/r/rap/en2_cr3.gif	2004-08-20 15:38:31 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.a1.yimg.com/us.yimg.com/a1/-flash/chrysler/040824_300x100.swf?clickTAG=...	2004-08-20 15:25:45 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.i1.yimg.com/us.yimg.com/l/us/pim/r/medic/5n_b/mail/us/mail_blue_all.css	2004-08-20 15:38:38 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.i1.yimg.com/us.yimg.com/l/us/pim/r/rap/en2_cr1.gif	2004-08-20 15:38:30 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.i1.yimg.com/us.yimg.com/lb/common/yq_cstare.js	2004-08-20 15:26:05 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.i1.yimg.com/us.yimg.com/l/wv/dn.gif	2004-08-20 15:25:44 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	yahoo.com/	2004-08-20 15:26:44 IST		Internet Explorer	yahoo.com		SUSPECT.00
index.dat			1	http://us.f613.mail.yahoo.com/m/login?rand=7m9d00f1k6&first=1	2004-08-20 15:38:23 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://www.yahoo.com/_yfh=X3dMTB1M2EzYWw0bF91A2l3MTYyNDIEZGVzZDAwMwBHRt...	2004-08-20 15:26:02 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://edit.yahoo.com/config/eval_register?v=8&int=8&new=1&done=8&src=ymlb.part...	2004-08-20 15:34:27 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://us.f613.mail.yahoo.com/yml/ShowFolder?Y=78169&first=1&box=Inbox&Y=1	2004-08-20 15:38:27 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://edit.yahoo.com/config/id_check	2004-08-20 15:35:47 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://edit.yahoo.com/config/register?	2004-08-20 15:38:01 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://us.f613.mail.yahoo.com/yml/Logout?Y=27630&first=1&inc=25&order=down&so...	2004-08-20 15:38:45 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://story.news.yahoo.com/news?tmpl=story&cid=564&ncid=564&e=1&u=/nn/2004...	2004-08-20 15:26:09 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://us.f613.mail.yahoo.com/yml/ShowLetter?Search=83d=&0/Y=90802&first=1&or...	2004-08-20 15:38:34 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://www.yahoo.com/_yfh=X3dMTB1M2EzYWw0bF91A2l3MTYyNDIEZGVzZDAwMwBHRt...	2004-08-20 15:34:16 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://www.yahoo.com	2004-08-20 15:25:45 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://edit.yahoo.com/config/last_subscribe	2004-08-20 15:38:11 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://edit.yahoo.com/config/last?scrumb=0NqEEeu7HG&crumb=0NqEEeu7HG&src=...	2004-08-20 15:38:07 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00

Snapshot 35 - Finding suspects Yahoo Mail email address - 3

## 5. On the bottom panel, click on the text tab

Source File	S	C	O	URL	Date Accessed	Referrer URL	Program Name	Domain	Username	Data Source
index.dat			1	http://us.i1.yimg.com/us.yimg.com/l/us/pim/r/medic/all/bt_b_dd_2.gif	2004-08-20 15:38:30 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.i1.yimg.com/us.yimg.com/l/us/pim/r/rap/en2_cr3.gif	2004-08-20 15:38:31 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.a1.yimg.com/us.yimg.com/a1/-flash/chrysler/040824_300x100.swf?clickTAG=...	2004-08-20 15:25:45 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.i1.yimg.com/us.yimg.com/lb/pim/r/medic/5n_b/mail/us/mail_blue_all.css	2004-08-20 15:38:38 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.i1.yimg.com/us.yimg.com/l/us/pim/r/rap/en2_cr1.gif	2004-08-20 15:38:30 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.i1.yimg.com/us.yimg.com/lb/common/yq_cstare.js	2004-08-20 15:26:05 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	http://us.i1.yimg.com/us.yimg.com/l/wv/dn.gif	2004-08-20 15:25:44 IST		Internet Explorer	yimg.com		SUSPECT.00
index.dat			1	yahoo.com/	2004-08-20 15:26:44 IST		Internet Explorer	yahoo.com		SUSPECT.00
index.dat			1	http://us.f613.mail.yahoo.com/m/login?rand=7m9d00f1k6&first=1	2004-08-20 15:38:23 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://www.yahoo.com/_yfh=X3dMTB1M2EzYWw0bF91A2l3MTYyNDIEZGVzZDAwMwBHRt...	2004-08-20 15:26:02 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://edit.yahoo.com/config/eval_register?v=8&int=8&new=1&done=8&src=ymlb.part...	2004-08-20 15:34:27 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://us.f613.mail.yahoo.com/yml/ShowFolder?Y=78169&first=1&box=Inbox&Y=1	2004-08-20 15:38:27 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://edit.yahoo.com/config/id_check	2004-08-20 15:35:47 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://edit.yahoo.com/config/register?	2004-08-20 15:38:01 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://us.f613.mail.yahoo.com/yml/Logout?Y=27630&first=1&inc=25&order=down&so...	2004-08-20 15:38:45 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://story.news.yahoo.com/news?tmpl=story&cid=564&ncid=564&e=1&u=/nn/2004...	2004-08-20 15:26:09 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://us.f613.mail.yahoo.com/yml/ShowLetter?Search=83d=&0/Y=90802&first=1&or...	2004-08-20 15:38:34 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://www.yahoo.com/_yfh=X3dMTB1M2EzYWw0bF91A2l3MTYyNDIEZGVzZDAwMwBHRt...	2004-08-20 15:34:16 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://www.yahoo.com	2004-08-20 15:25:45 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://edit.yahoo.com/config/last_subscribe	2004-08-20 15:38:11 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00
index.dat			1	http://edit.yahoo.com/config/last?scrumb=0NqEEeu7HG&crumb=0NqEEeu7HG&src=...	2004-08-20 15:38:07 IST		Internet Explorer	yahoo.com	Mr. Evil	SUSPECT.00

Text

Strings Indexed Text

Page: 1 of 1 Page

Matches on page: - of - Match

100%

Reset

Client UrlCache MIF Ver 5.2

HASH

4a41

#72;

URL

Visited: Mr. Evil@file:///D:/Drivers/Anonymizer/keys.txt

URL

Visited: Mr. Evil@about:Home

(DEEFA160-8640-01C4-0000-0000B3868648)

URL

Visited: Mr. Evil@file:///C:/Program%20Files/Anonymizer/thanks/index.html

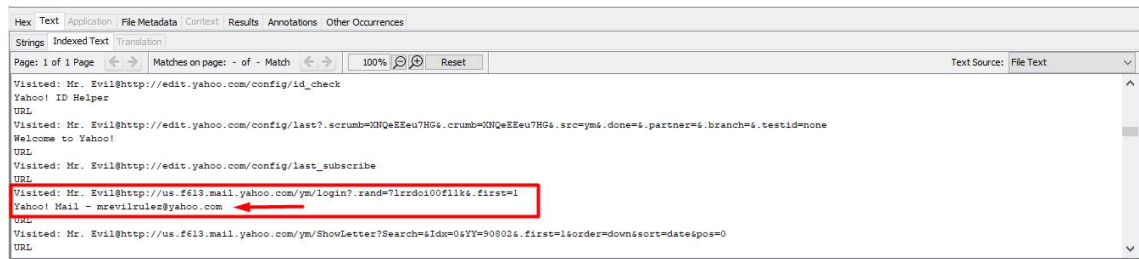
Anonymizer.com - About the Standard Privacy Toolbars Settings and Features

URL

Snapshot 36 - Finding suspects Yahoo Mail email address - 4

## 6. Scroll down a bit in the text tab

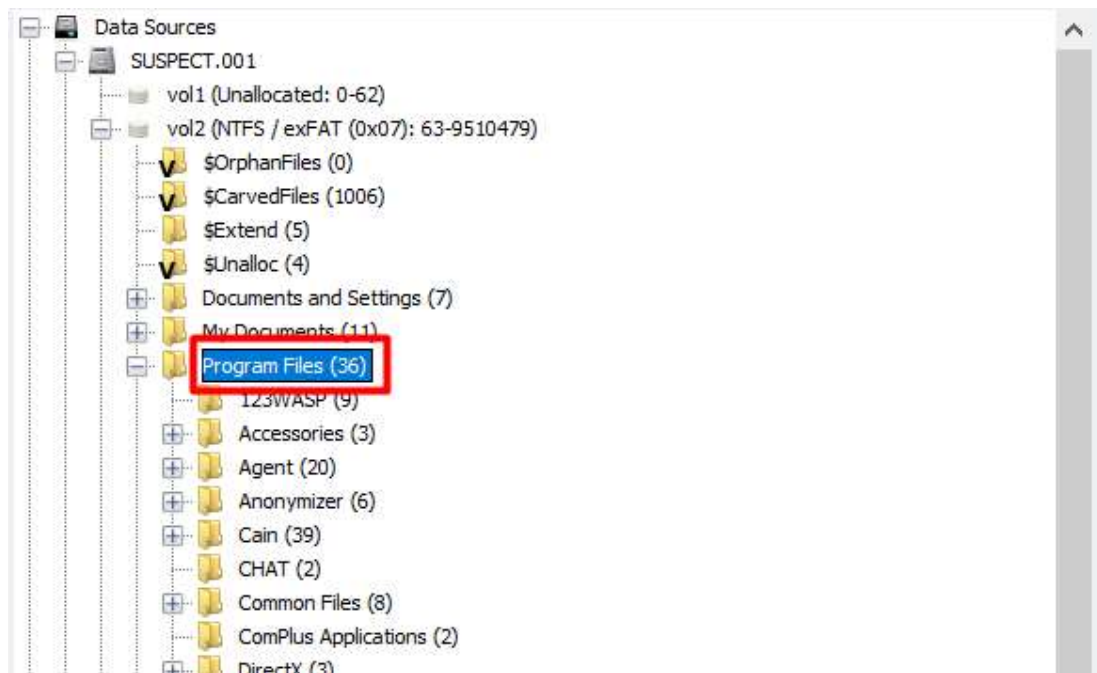




Snapshot 37 - Finding suspects Yahoo Mail email address - 5

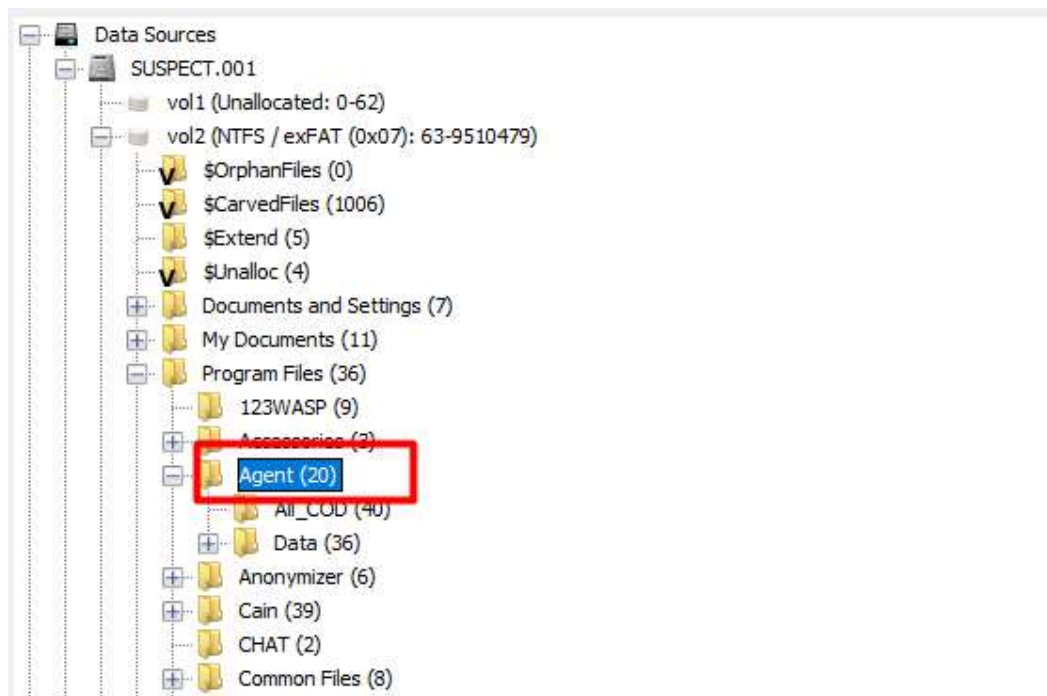
We can find the eMail Id that is used for logging in.

7. Follow steps 1 to 3 from Q10
8. Click on the plus button beside the Program Files folder



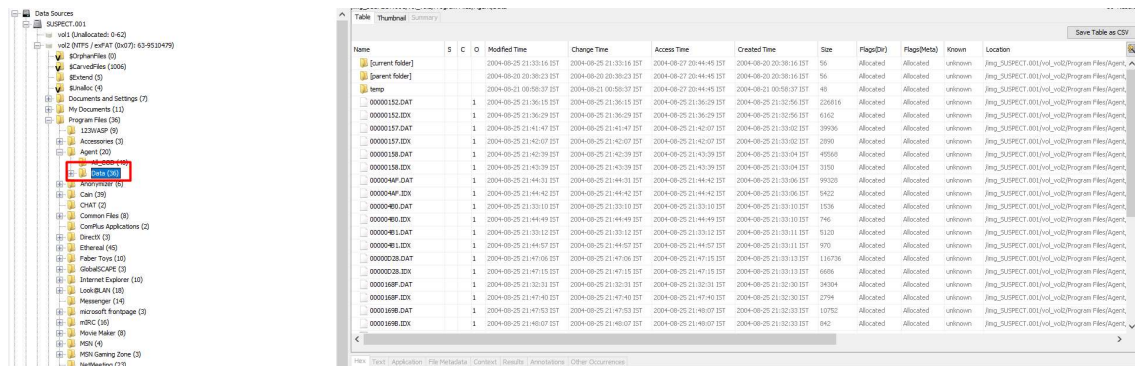
Snapshot 38 - Finding suspects Forte Agent email address - 1

9. Click on the plus button beside Agent Folder



Snapshot 39 - Finding suspects Forte Agent email address - 2

10. Click on the Data folder



Snapshot 40 - Finding suspects Forte Agent email address - 3

11. In the right tab, locate the file AGENT.ini and click on the AGENT.ini file

Listing											
/img_SUSPECT.001/vol_v02/Program Files/Agent/Data											
Table Thumbnail Summary											
Save Table as CSV											
Name	S	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
0000028.DAT		1	2004-08-25 21:47:06 IST	2004-08-25 21:47:06 IST	2004-08-25 21:47:15 IST	2004-08-25 21:33:13 IST	116736	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
0000028.IDX		1	2004-08-25 21:47:15 IST	2004-08-25 21:47:15 IST	2004-08-25 21:47:15 IST	2004-08-25 21:33:13 IST	6686	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
0000168F.DAT		1	2004-08-25 21:32:31 IST	2004-08-25 21:32:31 IST	2004-08-25 21:32:31 IST	2004-08-25 21:32:30 IST	34304	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
0000168F.IDX		1	2004-08-25 21:47:40 IST	2004-08-25 21:47:40 IST	2004-08-25 21:47:40 IST	2004-08-25 21:32:30 IST	2794	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
0000169B.DAT		1	2004-08-25 21:47:53 IST	2004-08-25 21:47:53 IST	2004-08-25 21:48:07 IST	2004-08-25 21:32:33 IST	10752	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
0000169B.IDX		1	2004-08-25 21:48:07 IST	2004-08-25 21:48:07 IST	2004-08-25 21:48:07 IST	2004-08-25 21:32:33 IST	842	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
AGENT.INI		2	2004-08-25 21:48:07 IST	2004-08-25 21:48:07 IST	2004-08-25 21:48:07 IST	2004-08-21 00:58:37 IST	11309	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
errorlog.txt		1	2004-08-21 01:17:30 IST	2004-08-21 01:17:30 IST	2004-08-21 01:17:30 IST	2004-08-21 01:15:44 IST	605	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
FILTERS.DAT		0	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	0	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
FILTERS.IDX		0	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	0	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
GROUPS.DAT		1	2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-21 00:58:37 IST	835657	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
GROUPS.IDX		1	2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-21 00:58:37 IST	568944	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
GRPID.BAK		1	2004-08-21 02:43:07 IST	2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-21 00:58:37 IST	835578	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
GRPID.IDX		1	2004-08-21 02:43:07 IST	2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-21 00:58:37 IST	568880	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
RANGES.BAK		1	2004-08-21 02:43:07 IST	2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-21 00:58:37 IST	64	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
RANGES.IDX		1	2004-08-25 21:33:16 IST	2004-08-25 21:33:16 IST	2004-08-25 21:33:16 IST	2004-08-21 00:58:37 IST	704	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
urthpe.dat		2	2004-08-21 00:58:38 IST	2004-08-21 00:58:38 IST	2004-08-25 21:25:36 IST	2004-08-21 00:58:38 IST	5430	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
WORDS.DAT		0	2004-08-25 21:32:56 IST	2004-08-25 21:32:56 IST	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	0	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
WORDS.IDX		0	2004-08-25 21:32:56 IST	2004-08-25 21:32:56 IST	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	0	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
XPOST.DAT		1	2004-08-25 21:33:16 IST	2004-08-25 21:33:16 IST	2004-08-25 21:33:16 IST	2004-08-25 21:32:08 IST	294912	Allocated	Allocated	unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/
XPOST.IDX		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	0	Unallocated		unknown	/img_SUSPECT.001/vol_v02/Program Files/Agent/

Snapshot 41 - Finding suspects Forte Agent email address - 4

## 12. On the bottom panel, click on the text tab

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

```

;AGENT.INI
;For information about the settings in this file,
;search for AGENT.INI in the online help.
[Profile]
Build="32.560"
FullName="Mr Evil"
EmailAddresses="whoknowsme@sboglobal.net"
EmailAddressesFormat=0
ReplyTo=""
Organization="N/A"
DoAuthorization=1
SavePassword=1
UserName="whoknowsme@sboglobal.net"

```

Snapshot 42 - Finding suspects Forte Agent email address - 5

## 13. In the text tab, we can find the email address used for the Forte Agent Email application

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

```

;AGENT.INI
;For information about the settings in this file,
;search for AGENT.INI in the online help.
[Profile]
Build="32.560"
FullName="Mr Evil"
EmailAddresses="whoknowsme@sboglobal.net"
EmailAddressesFormat=0
ReplyTo=""
Organization="N/A"
DoAuthorization=1
SavePassword=1
UserName="whoknowsme@sboglobal.net"

```

Snapshot 43 - Finding suspects Forte Agent email address - 6



Q18. List external storage devices attached to the notebook. What files were copied from notebook to USB drive?

Answer:

There is one external storage device attached to the notebook, and it is:

- TOSHIBA CD-ROM XM-1902B

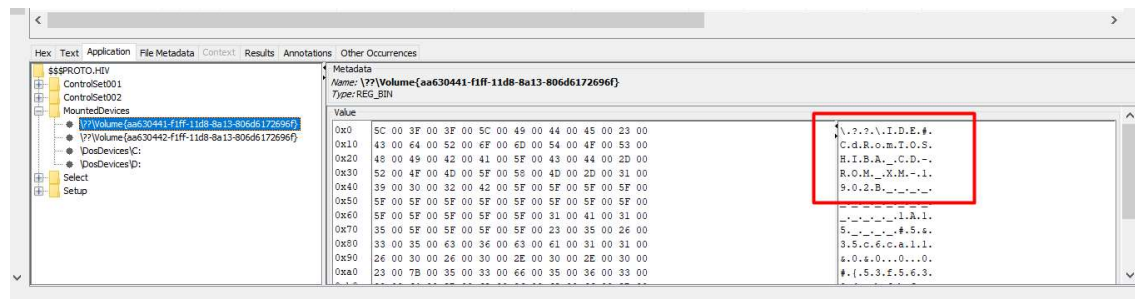
The files that were copied from notebook to USB drive are:

\*NOT FOUND\*

Analysis:

From the system registry file, we can find the mounted device folder that contains the details about the external devices attached. By inspecting the HEX value, I found out the name of the external storage. However, I could not find the files that were copied onto the external storage.

Evidence Analysed:



Snapshot 44 - External Storage

Snapshot 44 contains the name of the external storage device that was connected to the suspect's notebook.

Steps Taken:

1. Follow steps 1 to 6 from Q10.
2. Click in the system file on the right tab and click on the Application tab on the bottom panel



3. Network Stumbler 0.4.0 (remove only)
4. Look@LAN 2.50 Build 29
5. 123 Write All Stored Passwords
6. Powertoy For Windows XP v.1.00.0000
7. mIRC
8. CuteHTML
9. CuteFTP
10. Forté Agent
11. Faber Toys v.2.4 Build 216
12. Cain & Abel v2.5 beta45
13. Anonymizer Bar 2.0 (remove only)
14. WebFldrs XP v.9.50.5318

There are also 18 other programs installed on the system by the OS during its installation. The programs the suspect installed can be used for hacking. For example, Ethereal 0.10.6 v.0.10.6 is used for sniffing packets on the network, and Anonymizer is used to hide internet activity, etc. The suspect created a user Mr.Evil after the installation of the OS. Four applications were present on the system that is used for Email communication. There is evidence that the suspect also used a web browser to access Yahoo Mail. The suspect used two emails, and they are:

1. [whoknowsme@sbcglobal.net](mailto:whoknowsme@sbcglobal.net) (Forte Agent)
2. [mrevilrulez@yahoo.com](mailto:mrevilrulez@yahoo.com) (Yahoo Mail)

Evidence suggests that an external device TOSHIBA CD-ROM XM-1902B was connected to the suspect notebook. The data of the external storage devices are generally stored under /\$\$\$PROTO.HIV/ControlSet00x/Enum/USBSTOR, but there is no USBSTOR folder in the registry. The suspect might have deleted the registry file. I could not find any files that were copied from the suspect's notebook to the external storage.

## References

[1]"Australian Security Intelligence Organisation |", Asio.gov.au, 2021. [Online]. Available: <http://www.asio.gov.au/>. [Accessed: 14- Apr- 2021].

## Glossary

- Autopsy Version 4.18.0 - Autopsy

## Appendixes

- OS – Operating System
- ASIO – Australian Security Intelligence Organisation