



Solving Computer Forensic Case Using Autopsy

Computer Forensics is the well-planned series of procedures and techniques used for obtaining evidence from computer systems and storage media. This evidence can then be analyzed for relevant information that is to be presented in a court of law.

This article focused on a particular case and a forensic tool to give you a 'feel' of what computer forensics investigations are like. However, it is in no way comprehensive enough to cover the variety of problems and complications faced by the investigator.

Scenario

A complaint was made to the authorities describing alleged Wi-Fi hacking activity. When the authorities reached the spot, they found an abandoned Dell computer which is suspected that this computer was used for hacking purposes. Schardt uses "Mr.Evil" nickname when he goes online.

He is also accused of parking his car in wireless range (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords. We're going to solve 20 important questions that will be related to this case by examining the images of his computer.

Tasks performed:

During the course of investigation, analysis of the evidence would require performing the 12 basic tasks of computer forensics:

- 1. Generating an image hash and confirming the integrity of the image
- 2. Determining the Operating System used on the disk
- 3. Determining the date of OS installation
- 4. Determining the registered owner, account name in use and the last recorded shut down date and time
- 5. Determining the account name of the user who mostly used the computer and the user who last logged into it
- 6. Determining the hacker handle of the user and tying the actual name of the user to his hacker handle
- 7. Determining the MAC and last allocated IP address of this computer
- 8. Locating the programs installed in this computer that could have been used for hacking purposes
- 9. Collecting information regarding the IRC service that was used by the owner
- 10. Searching the Recycle Bin for relevant information
- 11. Listing the Newsgroups that the owner of the computer has registered to
- 12. Determining the SMTP email address in use

My Blog:

https://qaishussainy.blogspot.com/

Video tutorial for this investigation

https://youtu.be/0TUHpYIscBA

Seized Laptop's Disk Image:

Part 1: http://www.cfreds.nist.gov/images/4Dell%20Latitude%20CPi.E01

Part 2: http://www.cfreds.nist.gov/images/4Dell%20Latitude%20CPi.E02

Autopsy download link:

https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.14.0/autopsy-4.14.0-64bit.msi

After downloading the evidence disk and installing Autopsy, run Autopsy it and select New Case



Step 2:

Set a name for this case as i have set Mr.Evil and also set the location where you want to save your forensic investigation data. click next and provide information but it's optional. click finish.

😹 New Case Information			×
Steps	Case Informatio	n	
Case Information Optional Information	Case Name: Base Directory:	Mr.Evil C:\Users\USER\Desktoo\Forensic Case\ Brow	vse
	Case Type: Case data will be	Single-user Multi-user stored in the following directory:	
	C:\Users\USER\	Desktop\Forensic Case\Mr.Evi	
		< Back Next > Finish Cancel +	felp

eps	Optional Info	rmation
Case Information Optional Information	Case Number:	FRC-1177
	Examiner Name:	Qais
	Phone:	1234567890
	Notes:	Karipya kar ke Hard Disk ko haat mat lagaye warna haat kaat kar pehr mai dedenge.
	Organization	
	Organizatio	n analysis is being done for:

Step 3:

Select the first options Disk Image

Add Data Source	
Steps	Select Type of Data Source To Add
Select Type of Da Source To Add Select Data Source Configure Ingest Mo Add Data Source	ta dules Disk Image or VM File
	Local Disk
	Logical Files
	Unallocated Space Image File
	Autopsy Logical Imager Results
	XRY Text Export
	<8ack Next > Finish Cancel Help

Select the evidence disk image which you have downloaded before. i have created a separate folder by the name of Forensic Case and pasted the disk images into it.

Note: Although both parts of the downloaded image are there in this folder, you will only see the first part to select. Autopsy will automatically take the second part of the downloaded image.

Steps	Select Data So	urce				
1. Select Type of Data Source To	Path:					
Add 2. Select Data Source	C:\Users\USER\	Desktop\Forensic Ca	ise\			Browse
 Configure Ingest Modules Add Data Source 	📉 Ignore orpha	n files in FAT file sy	stens			
	Time zone: (G	MT+5:30) Asia/Calo	utta		•]	
	Sector size: Au	to Detect			-1	
	-	😸 Open				
	Hash Values (or	Look in:	- Forensic C	Case	• 🖻 👉 🔲 •	
	MDS:	æ	Mr.Evil			
	SHA-1:	Recent Items	4Del Lao	tude CPI.EUI		
	5HA-255:	NECCITY NUMB				
	NOTE: These v	Desktop				
		P				
		My Documents				
1711						
		Computer				
			File name:	4Dell Latitude CPI.E01		Open
		Network	1.1			

Click next and let all options as default.

eps	Configure Ingest Modules								
Select Type of Data Source To Add	Run ingest modules on:		The selected models has no new sup settings						
Select Data Source Configure Ingest Modules	All Files, Directories, and Unallocated Space		The abected module has to perform acturgs.						
Add Data Source	Recent Activity								
	 Hash Lookup File Type Identification Extension Mismatch Detector Embedded File Extractor Exif Parser Keyword Search Email Parser Encryption Detection Interesting Files Identifier Correlation Engine BhoteDate Convert 	10							
	Virtual Machine Extractor Image: Data Source Integrity		Extracts recent user activity, such as Web browsing, recently us						
	Select Al Deselect Al History		< Back Next > Finish Concel Hel						

Wait until all steps of analysis and integrity check loads completely.

make sure you have sufficient storage minimum 1GB otherwise the modules will not completely load and the investigation will be incomplete.



So now let's start our investigation

We will find the solution for these given tasks from the disk image of the suspect.

- Q1. What is the image hash?
- Q2: What operating system was used on the computer?
- Q3: When was the install date?
- Q4. Who is the registered owner?
- Q5. What is the computer account name?
- Q6. When was the last recorded computer shutdown date/time?
- Q7. How many accounts are recorded (total number)?
- Q8.Who was the last user to logon to the computer?
- Q9. List the network cards used by this computer?
- Q10. What is the IP address and MAC address of the computer?
- Q11. Search for programs/tools that aided in the crime (Wireless Hacking)
- Q12. Which Email client is used by Mr. Evil?
- Q13. What is the SMTP email address for Mr. Evil?
- Q14. How many executable files are in the recycle bin?

Q15. Are there any malware on the computer?

Q16. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the userid,

Q17. Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?

Q18. Which internet browser was used?

- Q19. What websites victim was accessing?
- Q20. What is the web-based email address for the main user?

Q1. What is the image hash?

Ans1: The HASH of image is AEE4FCD9301C03B3B054623CA261959A.

How?

Click on Data source --> Select the image Dell Latitude CPi, E01 --> Click on Metadata

MD5: AEE4FCD9301C03B3B054623CA261959A



We check hash to see if the image is not altered or something is not added or not deleted from the activities. It's very important because a single tamper to data would make an accused, guilty or innocent.

Q2: What operating system was used on the computer?

Ans2: Microsoft Windows XP was used.

How?

Click on results --> Extracted Content --> Operating System Information

then on the right side click on software you can see the under Program Information tab which is written Microsoft Windows XP.



Q3: When was the install date?

Ans3: 2004-08-19 22:48:27

How?

Click on results --> Extracted Content --> Operating System Information

then on the right side click on software you can see under the Date Time tab which is written Microsoft Windows XP.



Q4. Who is the registered owner?

Ans4: The owner is Greg Schardt

How?

Click on results --> Extracted Content --> Operating System Information

then on the right side click on software you can see the under Owner tab which shows Greg Schardt.



Q5. What is the computer account name?

Ans5: The account name is N-1A90DN6ZXK4LQ

How?

Click on results --> Extracted Content --> Operating System Information

then on the right side click on System you can see the under Name which it shows N-1A90DN6ZXK4LQ

🔶 Add Data Source 🌆 Images/Videos 🞇 Communications 🗮 Timeline 🚚 File Discover	V 🙀 Close Case	Genera	ate Report				• Keyword Lists	Keyword Search
€ ⇒ Q	Listing	oor Annour	at					
Data Sources	Table Thumhnail	asi ruccou						o read
4Dell Latitude CPI.E01	Thumphun						Ċ	den and a date
vol2 (NTFS / exFAT (0x07): 63-9510479)								Save Lable as CSV
uli vol3 (Unallocated: 9510480-9514259)	Source File	S C	Username	User ID	Path	Data Source	Date Created	Date Accessed
Views	🌴 software		systemprofile	S-1-5-18	%systemroot%\system32\config\systemprofile	4Dell Latitude CPI.EI	01	
E S File Types	4 software		LocalService	S-1-5-19	%SystemDrive%\Documents and Settings\LocalS	. 4Dell Latitude CPI.El	01	
B & MIME Type	🌴 software		NetworkService	S-1-5-20	%SystemDrive%\Documents and Settings\Networ.	4Dell Latitude CPi.El)1	
🖃 👷 Deleted Files	🌴 software		Mr	S-1-5-21-2000478354-688789844-1708537768-1.	. %SystemDrive%\Documents and Settings\Mr. Evil	4Dell Latitude CPi.El	01 2004-08-20 04:33:54 IS	T 2004-08-27 20:3
X File System (365)	4 SAM		Administrator	S-1-5-21-2000478354-688789844-1708537768-50	3	4Dell Latitude CPi.El	01 2004-08-19 22:29:24 IS	T
All (365)	SAM SAM		SUPPORT_388945a0	S-1-5-21-2000478354-688789844-1708537768-1		4Dell Latitude CPI.El)1 2004-08-20 04:05:19 IS	Т
MB 50 - 200MR (4)	SAM SAM		Guest	S-1-5-21-2000478354-688789844-1708537768-50	1	4Dell Latitude CPi.El	01 2004-08-19 22:29:24 IS	Т
MB 200MB - 1GB (2)	SAM SAM		HelpAssistant	S-1-5-21-2000478354-688789844-1708537768-1		4Dell Latitude CPI.El	01 2004-08-20 03:58:24 15	т
Web Bookmarks (a) Web Sections (3) Web Sections (3) Web Sections (3) Web Section (3) Scher (4) Web Section (4) Scher (4)				m 	_			
E Rail	Hex Lext Applica	tion Mess	sage File Metadata Co	ontext Results Annotations Other Occurrences				
μ togi lags _ <u>k</u> Reports								
								Show deskto

Q6. When was the last recorded computer shutdown date/time?

Ans6: The last recorded shutdown time of the computer is 2004/08/27-10:46:27

How?

Click on Data Sources select 4Dell Latitude --> vol2 -->

 $WINDOWS \system 32 \config\software \Microsoft \Window NT \Current \Version \Prefetcher \Exit Time e$

i Data Sauran 📠 Bragozi/Videas 🌇 Communications 🗮 Timeline 🚚 File Decover	Gloss Case & Genera	ti Rep	ort						• - toyou	duine	Q: Report Search	
0	Loging	AND AND A REAL PROPERTY AND										
a m (num)	(mg_40ell Latriala CPU231/m	Cell	nincon2/news/seeds								33 Face	
(m. pr. Declator (n)	Table [Benfine]											
Moda (18)											- Sant Toble as CSI	
E a magest (11)	kate	sic	Picitive Tinia	Change Time	Access Time	Constant Types	520	Fig005	RepOND	Showing -	LOCHEM.	
III a mappe(2)	Comment Publics]		2004-08-20 R4120-28 RF	1804-05-20 0+:00 18 197	2004-08-01 20.2008-051	1804-08-19-11-00-17-857	35	Alladenid	algested.	Unthiowh	And Call Linksle 18	
Differe Web Faces (7)	(2 (periet folder)		2019-c9-c7 21:00:01:07	1009-00-01 (1 00.01 001	NOP-OR 27 21 10101 (RT	1004-00-18 22 20 17 011	-	district	abcater	usinom	(vigtoil Lattale to	
(e) 🕹 PORIALINE(H)	3. systempreille		1004 OF 20 H (19 25 157	380400-0004430-08.87	2010/08/07 21:00:07:07	2004/00/00 01/10/05 07		Alected	Alterated	winen	(mg) Oct Lattate (
- 🔐 Profitib (H)	Applivent lint		1004-06-27 21:32:30 mT	3804-08-27.21:12:28.29.527	2004-08-27 31 15:25 55	2804-08-(8-22:29-14-57	68704	Allapoord	Alcosted.	uniques	(mg. Kell Linksle 1	
🖶 📮 Pagittisten (II)	default		1004-09-21 21-15-11 37	1004-00-00-04-00.07.07	THE R. I. I. T 60-101	2004-09-29 22:20:08 107	307244	chicaged	abusted	uncon	(ingtoid twittable to	
in team (14)	E defeale.LOC		200400 2121/02/56 207	2004/00/27 21:02:09 217	2004-00-27-21-02:38-357	2004/08/20 20:00:001	Aller	Alterated	Altopted	winters	Ave. On Labors O	
a security (1.1)	diffection		2004-08-19 22:29:20 167	2004-08-29 22:12 15 157	2004-08-19 85-20:00 167	2004-06-09 22-26-19 57	10112	Alecased	Alocated	utinovin	/mc.404LMMIN 0	
a orboat (k)	LAM.		3004-08-27 21.16 mi mt	1004-00-02-04-05121 87	2004-08-27 21 10:33 07	2004-00-29 22 20 28 201	302044	discosed.	advated	ustraism	AND ROOT LOLLING OF	
a sphiss (17)	SAM LOC		2014/08/27 20:09:20 201	2004/08/07 20:06:03 10*	2004-08-27 20:08:23 257	2304-08-09-22-08-68-857	1524	Allocided	Allocated	University	/ins_/Oel Latkate (7	
a odosta (17M)	Section Live		2004-08-09 22:29:15 107	1004-04-09 32120 19 847	1004-08-09-22:20:10 (07	2004-08-09 0102015 07	80518	Alsoned	Advented	uttracen	(the 40xh Lankate Of	
1535 (2)	WEISTY		TER-OR-27 21-10-11 TT	1004-00-00 04,94,03 007	THE R. O. C. W. S. W. S. W.	2004-00-14-20-2010 BT	312244	discond	Abaahoi	utinim	/mg-forf1.attute-07	
- 2 1811 (2)	Statienvuoc		2004 CP-27 Z1-02-10 201	2004-00-07-21-02/29-027	2004/08/27 21:02:58:222	2004/09/09 22:02:03 22	1000	Alterated	allocated .	Laboration .	/inc. Coll. alkald (7)	
- 2. 1233 (2)	afway.		100+04-37 21 30: 11 IL	1004-06-21 10:201-44 107	100+04-27 11 18:31 104	Distances in his locked and	1650/52	Antend	alizated 1	Uttion	Ang Collaboration	
2 1817(2)	Distant state		2204-c8-27 21:10 20 27	1004-00-0121-02-017	INDE-CH (21 (1) 10 10 TT	100400-04222008-011	1224	diffusion d	administeria	Lebrain	Anici - exist Cathole (21)	
4 1041 (2) R 1041 (2)	advice as		ID0+08-20-22-20-ID-ID7	30100-2022-0218	2010/08/20 05:00 00:001	2004/00/20 22:00:01 107	0.00784	Alected	abusted	ceirem.	(mu) Del Laterie (T)	
1004(2)	Svillvert Svt		1004-06-37 21:35:10 mT	1004-00-27 Jan 15-24 St7	200408-0711115/25-54	2004-05-09 22:00 15 G7	48504	Alacoad	adjointed.	uninees	Anna Wall Linkste (P)	
1 1002 (2)	autors.		1004-09-27 21-15-11-17	1004-00-07 21 25 44 227	mps-co.ev p1.10.01.07	1004-00-0112-06-08 FIT	3031443	character?	advanted .	Laborator	And she wanted	
A 30/16 (2)	Diseases 100		200409-2121-04-01-027	2004/00/21 21:30:30 527	200408-20121-04-00-022	2009-08-20 20-20-08	1004	Alleraded	Altracted	antranier.	Jaco (California) (Cal	
trans, Are (1)	00000.004		2014-08-09 X2-04-20167	200 au 200 au 201 201 au 2017	30A/8-10 PC 2010-57	2010a.00.00 10-06-18 KP		Alected			Any and unsultate	
Carthold (4)	Templey 100		100+00-00 27 00 Lt 07	(100+00-19-22) to 15 pt	Direction in the state of	INTERNATION DE LOS DE LA TELT	1.024	Ancional	abusted	Latinian.	AND REAL MADE OF	
Cables (1)	Controll		TTACK TO 27-06 15 197	THE R. LEWIS CO., NO. 14, NO.	TRACK IN IN WALKS	THE R. P. LEWIS CO., NO. 101	and at	distant	Alterated	i minerare	Ann all of a state of the	
a costo (21)	and the second second		1004/0.0012/30 m m7	100 March 10, 27-10, 48, 817	Instances of a Western State	Intraction in the second second	4100	Alternation	adventeri	1.0000000	June allock Lank Mr. (11)	
E 🔒 Rectampristia (24)	the second second		services and services and	COMPANY OF THE OWNER.	and the set of the set of	Values, de un décembre		1 marked and		1.41/10/00	Annu Annu Landon Charles	
2 chop [1]	T bearing		and the post states.	dependence includente	10000 (01 10 10 10 10 10 10	(400-00-00-00-00-00-00-					Table of the Contrast of the	
Oracle (1)												
Coversition												
- (1 aspet (2)	4 <u>U.</u>			10410								
- 🗸 as (9)												
 Isoland (7) 	lack Test Appharant March	2018	de Metadoba Facto	Ro Annotation I Wei Dere								
# 240 (b)	 Opericitatives 	4	M	Cardielle .								
A Pacored (II	E Partio			CV. EXPERIM								
Pasionett (2)	H & Parts											
Aller (4)	E & Prafatcher		20	NAT								
4 ma (4)	 Versen Versen 											
- P opp (N)	· TrocasPro	inset	N2									
	- · Tholastica	const a										
- 2 Metterii (k)	Ladirison	120.00										
- 🦊 metap (18)	- 83673											
2 should [2]	 Icol7 (Inc) 	ACRO D	4 11									
to the opposition of the second secon	 Lactivica 	VOLTO:	neitine .									
(ii) (ii) solare (24)	e la roat											
- 4 whi(d) *	ID & Frafficial		-									

Q7. How many accounts are recorded (total number)?

Ans7: There are 5 accounts

Mr, Administrator, Guest, Support388945a0, HelpAssistant

How?

Click on Results --> Operating System User Accounts



Q8. Who was the last user to logon to the computer?

Ans8: Mr. Evil

The system will obtain the last user who logged on from the key 'DefaultUserName'. This information can be uncovered from the following path

How?

Click on Data Sources select 4Dell Latitude --> vol2 -->

WINDOWS/SYSTEM32/CONFIG/SOFTWARE/MICROSOFT/WINDOWS NT/CURRENT VERSION/WINLOGON/DEFAULT USER NAME

M Miler Autops 4143											u @ 3
🔶 Add Data Source 👪 Bragos/Yolean 🔛 Communications 🗮 Timeline 🚚 File Decomm	Cher Care b	Generate Rep	ve.						• · uyu	dute	Qr keyward Search
(¢.)) = ((ma) + (ma)(ma) + (ma)(ma)(ma) + (ma)(ma)(ma) + (ma)(ma)(ma)(ma) + (ma)(ma)(ma)(ma)(ma)(ma)(ma)(ma)(ma)(ma)	Loting (mg_40el (attude (P Table Thursboal	(81/ml, vel)	withEOWS/splant2/certig								(ain)(a) 3) head
ter 🚚 para (4)											- Save Toble as COV
E interpret (13)	August .	100.00	matched time	(Dance Time	Access Tatle	Output Trave	100	Painteri -	(HearWest)	- anima	License
10 mappe (2)	Convertibiliter 1		Disco Name of Street,	1004-05-20 04:00 18 167	1004-08-31 20 20 Jan ST	INCHARGE-OR DE UNIT OF BUT	-	Alacend	algested	Lationeo	And the latter the
Plan (2) Officer Web Ficker (2)	(Line and Solder)		2004-08-07 21 00:10 BT	100+00-01 (1 (0.1) 10 FT	000-00-01-01-00-00	100 w 00 10 22 20 17 101		discond.	adocatery	Labracore	Ave Coll Laboration of the
+ A POHMADR(4)	antonprolite		104 OF 2014 10 25 37	304-00-00 04-30-05-827	2004-08-27 21-01-27 02	2010/02/02 04:00:05 07		Alecated	Altorated	orinered	(No. Of Little (1)
- A Prinkin (H)	Applivent Set		1004-08-07 21:00-08 BI	1004-01-01 01:00:01 107	100-08-27 21:10:29:59	2004/08/07 02:09:04 07	69104	Almonto	viccout.	uninpen	And Kiel Lanual 21
🖶 📮 Registration (8)	delad		2004-09-27 (1.16-21.27	2014/02/02 04:21:22 07	.000+08-21 21-16 01 017	2004-08-09 22-20-08 817	2023 H	discast	Advanted	140000	/settheir adults (7)
Figure (12)	S defeatutor		200+04-27 21 42:55 27	2004/09/27 21:02:09 107	2010/08/27 21:02:39:07	2040032228.00.07	1014	Alasated	4 located	urinten	/we_downakde (Pi
18 2 security [11]	distan		2014/08/27 22:20:20:20	100+00-09 20:02 15 67	2014-08-09 (5-200) (61	2004-08-09 12:38:18 57	90112	Alucated	alicand	utinnin	/mg_4NELMLIN (PL
(i) 🚚 without (ii)	LAM		2004-08-27 21-14:31 287	2004/09/02 04:05 21 87	2004-08-21/21 21:20:31 02	2010/08/2012/2013/07	HOUSE	Abs also	adocated.	(altraser)	AND RECORDER OF
	SAM LOG		300-08 27 20:00 23 257	100408-012000-03-001	2014-08-27 20:30:21 157	2804-08-29 (2105-19.87	1524	Altrophyl	Alacabst	University.	/hg. Oil Litteb (%
[2] 4 Append 2 (1794)	Sectored.int		2004-08-09-22-29-15-227	1004-01-010110-1510	2004-08-0922-2912.07	100408-0102215-018	1001.08	Abstand	Advanted	saturen	AND REPORT OF
U 1838 (2)	S RECURITY		2014/09/27 21:34:31:31	(ID+0100.000) = 01107	300408-07 (11)0-31 (12	2010/02/02 20:00:00 207	HIDH.	-104(100a)	abcohu	salarapin	/seg_dist1.slitute (2)
4 1001 (2)	SUCHEFTY.LOG		2014/08/27 71:00:98:257	2004-00-07-01-02-09-057	2004-08-07 21:02:58:22	2804-09-19-22-25-58-58 207	1210	Allected	Alterated	utinon	Ang, Kell Liekals (h)
- 2. 1231 (Y)	afware:		100-CP-17-11-11-11-11	1004-00-27 (0:20-24 b)7	INDECK 27 21:10:01 INF	10408-012008-07	3630,752	discosid	182.001	Gitten	/reg_domination into
1917(2)	201.treeba 🔅		220-082721-0922	100408-010131-00-02-021	300-08-27-21-36-30 HT	2004/02/11 22:00:08 07	12/10	1.04(4)	400000	1.001(100000)	/wij_40#144446 (7)
2 1042 (Z)	ofware.see		3004-08-19-32-28-28-287	30401352:00.07	2014/08/19 (5:30.00.00)	2804-08-012028-18-007	000784	Alexand	Algorid	uniners	(http://www.ukubi.ch
2 1894 (2) III	System.int		2014/06/27 21:00:00:01	1004-08-07-11-10-28-167	300408-27.01.1028-39	2804 (8-19.20.29.15.57	10724	Alacend	Alexand.	salaren	/mg_404E1.08U29-121
- J 2012 (2)	spiles		2004-04-01 11-19-20 301	780408-1721-02-04927	1004-08-21 21 3A 31 33	1014-09-00 22:00:08 202	2612-003	Alsonid	Advided	uningin	Available to the second
2 (100 (2)	geten.005		2004-08-27 21-35:30.057	2804/09/27/21:55:59 E7	2004/08/27 21:35:31:07	2024/02/02 22:05:08 107	1004	Alterated	who extend	uninging	Avg.404Lab.de.01
12 Collina (10)	_ systematy		2004-08-29 22:06:01:01	3809-09-09 22:32:15 157	2004-08-09 85 20:02 51	309-08-09 22-39 28 81	39123	Alucated	wildcamed	utentiin	Verif April Charles Ch
(i) 2 Calibrat2 (3)	TempRey IDG		2010/01/22 22:05 01:021	2004/01-30 22:52:53 87	2014/08/2018/2018/201	2804-08-29 22/28/14 812	1529	Micule)	1400abi0	(altern	Ave_doin calls also the
Cen (S)	Porem -		10.4 OF 19 22:30 20 207	30408-3922-5218-87	20408-0919-0000-07	2804-08-39 22-35-08-357	202144	Altypologi	Alizatet	UNITED	(ing, Kell Lines (in
is a contraction (14)	OCUPERING [1004-08-09-22108-00107	1004-05-09 22102 15 817	2004-06-09 \$1,00.00.007	104-08-09 (2126-08-01)	titter.	Abcased	alocated.	satinten	(H)_0H_20H_20H_1H
2. chep (2) () 2. Greats (2)	¥ sensitiog		0000-08-80 80/08/18:	1000-02-02 01.00 01	3000-00-00-00-00-00	0800-08-05-00-08		Unitability		Outracin	AND DRIVEN TO
diffusible (2012) deves (174) deves (174)	íu			11							
4 485 (10)	Construction and the	10. 11		-							
(i) 0 MC(1)	Day	and the second s	For Michaeles	sita (Annataliana) Misicita	1010411						
 Berneret (1) Berneret (1) 	D & Type D & Liver	i installor ustallable draw	1	anv. DefaultitionName per 186_57							
III **errors(1,0) III **errors(1,0) III *errors(1,0) III *errors(1,0) IIII *errors(1,0) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		sen gat tickensoni Hy ecoleccentra attendentia fillene at patholocitor patholocitor patholocitor patholocitor patholocitor el el	Susteen	Mar - Tud							
											Show desktor
🚯 📋 🖪 🔞 👩 🦉 O 🖉 .	1 2	4	R R C	*							1200 AM

Q9. List the network cards used by this computer?

Ans9: Compaq WL110 Wireless LAN PC Card, Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface).

How?

Click on Data Sources select 4Dell Latitude --> vol2 -->

WINDOWS\system32\config\software\Microsoft\Windows NT\CurrentVersion\NetworkCards\

click on descriptions





Q10. What is the IP address and MAC address of the computer?

Ans10: IP=192.168.1.111, MAC=00:10:a4:93:3e:09

How?

Click on Data Sources select 4Dell Latitude --> vol2 --> Program Files/Look@LAN/irunin.ini

	Toble Thumbhail				
— III vol1 (Unallocated: 0-62)					
vol2 (NTF5 / exFAT (0x07): 63-9510479) \$0mbarElles (0)	Name	s	c	Modified Time	Change Time
SExtend (5)	Courrent folder)			2004-08-25 21:26 51 251	2004-08-25 21:26 51 15
SUnalloc (4)	(narent folder)			2004-08-27 20:58:40 151	2004-08-27 20:58:40 15
Documents and Settings (7)	Report			2004-08-25 21-26-04 IST	2004-08-25 21-26-04 19
My Documents (11)	a countr			2004-06-25-21-26-07 IST	2004-09-25 21-26 07 15
E J Program Files (36)	C Manual data			2004/00/23 21:20:0/151	2004-00-23 21.26.07 15
Accessories (3)	Coviandation.			2004-06-17 10:31:40:31	2004-08-23 21:26:11 15
E Agent (20)	nostist.dat			2004-08-25 21:25:51 251	2004408-25 21:26:51 15
H Anonymizer (6)	S irunin.bmp			2004-08-25 21:25:27 IST	2004-08-25 21:25:27 15
🗄 📜 Cain (39)	irunin.dat			2004-08-25 21:25:27 IST	2004-08-25 21:25:27 15
- 📜 CHAT (2)	(invinini) (invinini)			2004-08-25 21:26:10 IST	2004-08-25 21:26:10 15
E Common Files (8)	🗌 irusin.lng			2004-08-25 21:25:27 IST	2004-08-25 21:25:27 15
ComPlus Applications (2)	≣ lalassoc.dat			2003-04-27 19:01-26 IST	2004-00-25 21:26:05 15
El process (3)	lalservices.dat			2004-02-10 14:54:32 IST	2004-00-25 21:26:05 15
E-Faber Toys (10)	License.txt			2004-02-17 16:19:00 IST	2004-00-25 21:26:11 19
GlobalSCAPE (3)	Look@LAN on the WEB.url			2084-02-17 16:01-21 IST	2004-00-25 21:26:11 15
Internet Explorer (10)	LookAtHost ENG			2003-05-18 12:30-18 IST	2004-09-25 21-26 07 15
🗆 🜙 Look@LAN (18)	in Contraction			2003-06-10 17-30-17 ICT	2004-00-22 20-40-04 10
E Report (4)	Lock Man Ster			2003-00-13 17-30-17-131	2004-00-27 20.46-04-15
sounds (7)	COOKHILEN, ENG			2004-02-18 15:21:40 191	2004-06-23 21-20-07 15
microsoft (14)	By LookAttantexe			2004-02-10 10:21:09:001	2004-06-27-20-46-04-15
mill(16)					
Movie Maker (8)					
Mavie Maker (8)					
Movie Maker (8) Movie Maker (8) Movie (4) Movie (4) Movie (3)					
Movie Maker (8) Movie					
Michael (14) Michael (14) Michael (15) Michael (14) Michael (15) Michael (14) Michael (14) Mi					
Music (16) MSN (4) MSN (5) NetWeeting (23) NetWeeting (23) Online Services (5) Outlook Express (14) Dutlook Express (14) Dutlook Express (14)					
Index (19) MSN (4) MSN (4) MSN (6aring Zone (3) NetWeek Stambler (15) Outlock Express (14) Outlock Express (14) PLUS (4)					-01
House (14) MSN (4) MSN (4) MSN (4) MSN (5) MSN (4) MSN (4) MSN (4) State (15) Online Services (5) Outlook Express (24) Dubok Express (24) Uninstal Information (20) Whois (8)					40). -
Index (14) Index (15)	+ Litex Text Application Mossage	File Me	tada	ta Contest Results Anno	tations Other Occurrences
Marve Maker (8) Marve Maker (8) MSN (4) MSN Germing Zone (3) NetWork Stumbler (15) Dutlook Express (14) Dutlook Express (14) Uninstal Information (20) Whole (8) Windows Mada Player (15) 	Hier Text Application Monorary Stange Indexed Text Translet	• File Me	tada	ta Context Results Anna	tations Other Occurrences
Index (46) Move Meker (8) Move Meker (8) Move Meker (8) Move Meker (8) NetWeeting (23) Network Stumbler (15) Outlook Express (14) Uninstall Information (20) Whois (8) Whois (8) Windows Media Player (15) Windows VDpdate (3)	Hex Text Application Mossage Strings Indexed Text Translat Matches on page: - of	File Me	tada	ta Context Results Anno	tations Other Occurrences
Muchael (a) Mission (a) Mission (b) Mission (c) Mission (c) Missi	Hex Text Application Message Strings Indexed Text Translat Matches on page: - of	File Me	tada ¢	ta Contest Results Anno Page: 1 of 1	tations Other Occurrences
House (16) MSN (4) MSN (4) MSN Gaming Zone (3) NetWork Stumbler (15) Online Services (5) Outlook Express (14) Usis (4) Usis (4) Windows Media Player (15) Windows Media Player (15) Windows Moda Player (15) Windows Moda Player (15) Windows Update (3) Windows D (2)	Hex Text Application Moreover Stings Indexed Text Transler Matches on page: - of (Conf.ig)	File Me on Match	tada e	ta Context Results Anno Page: 1 of 1	tations Other Occurrences
Hulse (16) MSN (4) MSN (4) MSN Gamma Zone (3) MSN Gamma Zone (3) Network Stumbler (15) Outlook Express (14) Uninstal Information (20) Whole (4) Windows Media Player (15) Windows NT (7) Windows NT (7) Windows NT (7) Windows NT (3) Windows (3) RECYCLER (3) Sector Molece Information (2)	+ Hex Text Application Movies Strings Indexed Text Transfer Matches on page: - of [Config] Config11=C:\Tragram Files\Les	File Me on Match	tada e	ta Context Reserve Anno → Pege: 1 of 1	tations Other Occurrences
Marke (14) Marke Maker (8) MSN (4) MSN (4) MSN (5) MSN (4) MSN (5) Network Stumbler (15) Outlook Express (14) Uninstall Information (20) Whois (8) Whois (8) Windows Ndola Player (15) Windows Ndows Ndola Player (15) Windows Ndola Player (15) Windows Ndola Player (15) Windows Ndola Player (15) Windows Ndows Ndows Ndows Ndola Player (15) Windows Ndows Ndola Player (15) Windows Ndows Ndow	Hex Text Application Message Stangs Indexed Text Translat Matches on page: - of (Config) Config1Config1Config1Config1LetCi/Program FilePlice IncompfilePliceCi/Program FilePlice	File Me on - Match ABLAN, London CRAN, London	tada e	ta Contract Results Anno Page: 1 of 1	III tations Other Occurrences Page 🗲 🗲
Index (48) Mone Maker (8) Mone Maker (8) Mone Maker (8) Mone Garring Zone (3) NetWeeting (23) NetWeeting (23) NetWeet Stumbler (15) Outlook Express (14) Pluss (4) Uninstal Information (20) Whois (8) Windows Media Player (15) Windows Update (3) Winfcap (7) RECYCLER (3) RECYCLER (3) System Volume Information (3) Temp (2) WUNPCap (15)	Hex Text Application Mossage Strings Indexed Text Translat Matches on page: - of (Config) Config:Index.Throughan Files/Low Lasgesfile=C.\Program Files/Low Lasgesfile=C.\Program Files/Low LasgetFile=C.\Program file	File Me m - Match satativ, trus satativ, trus	tada (e	ta Context Result- Anno Page: 1 of 1 ten Ling P	tations Other Occurrences
Marke (Ney Marke (Ney MSN (4) NetWeet Sumbler (15) Unitstall Information (20) Whole (8) Windows Media Player (15) Windows NT (7) System Volume Information (3) Temp (2) WiNDOWS (109)	Image Text Application Intersects Stangs Indexed Text Intersect Matches on page: - of (Config) Config1le=C:\Frequent Files\Look LangerLis=C:\Frequent Files\Look LangerLis=C:\Frequent Files\Look LangerFile=C:\Frequent Files\Look LangeFile=C:\Frequent File=C:\Frequent Files\Look LangeFile=C:\Frequent Files\Look LangeFile=C:\Freq	File Me Motch setUN, inter setUN, inter setUN, inter	tada e	ta Context Forsette Anno Page: 1 of 1	rill tations Other Occurrences Page 🗧 🔶
Image: (av) Image:	Image Text Application Program Strings Indexed Text Translat Matches on page: - of - (Config) Config11e=C:\Program File=\Loo LooperFile=C:\Program File=\Loo LoopErfile=C:\Program File=\Loo LoopErfile=C:\Program File=\Loo Textberling=0 (Percenter1 LoosExter1 LoosExter1 Textberling=0 (Percenter1 LoosExter1 LoosExter1 LoosExter1 LoosExter1 Textberling=0 (Percenter1 LoosExter1 LooxExter1 LooxEx	File Me Match A 81.00% street A 81.00% street	tada e	ta Contest Results Anno Page: 1 of 1 tes Ling P	tations Other Occurrences
Move Maker (8) Move Maker (8) Move Maker (8) Move Maker (3) Move Maker (3) Move Maker (3) NetWeeting (23) NetWeeting (23) Online Services (5) Online Services (5) Online Services (14) Uutlook Express (14) Windows Media Player (15) Windows Media Player (15) Windows NT (7) Windows Vedia Player (15) Windows Vedia Player (15) Windows Vedia Player (15) Windows Vedia Player (15) Windows Vedia Player (3) Windows NT (7) Windows Vedia Player (15) Windows Vedia (3) Windows Vedia Player (15) Windows Vedia (3) Windows Vedi	<pre></pre>	File Me on - Match set (1347) is not set (1347) is not (1347) is not	tada ein d	ta Contract Resorts Anno Page: 1 of 1 ten tan p	III tations Other Occurrences
Index (14) Index (14) Index (14) Index (14) Index (15) Index (15) Index (15) Index (15) Index (14) Index (15) Index (16) Index (16) I	<pre>4 Hex Text Application Monorpy Strings Indexed Text Transfer Matches on page: - of (Config) Config) Config(Ilent:\Tregram File=\Loo LasgregFile=C:\Program File=</pre>	File Me Motch Motch Motch Motch Motch Motch Motch	tada e	ta Contract Results Anno Page: 1 of 1 Int P	III tations Other Occurrences
Marce Maker (8) MSN Gamming Zone (3) MSN Gamming Zone (3) MSN Gamming Zone (3) Network Stumbler (15) Online Services (5) Outlook Express (14) Outlook Express (14) Outlook Express (14) Windows Media Player (15) Windows Media Player	Hex Text Application Message Strings Indexed Text Textmass Matches on page: - of Configi Configi Configite-C:\Frogram Files\Los LangeTile-C:\Frogram Files\Los Lan	Elle Me mi Match statan i con	tada	ta Context Results Anno Page: 1 of 1 tes 	tations Other Occurrences
Index (aby Move Maker (8) Move Maker (8) Move Maker (3) Network Stumbler (15) Network Stumbler (15) Outlook Express (14) Uninistall Information (20) What (4) Uninistall Information (20) Windows Media Player (15) Windows Update (3) WindowsUpdate (3) WindowsUpdate (3) System Volume Information (3) Temp (2) WiNdows (109) Widdows (109) WindowsUpdate: SS10480-9514259) Aews File Types System Super Expression Super Expression System Super Expression Supe	Example of the second sec	File Me Motch Motch ABLAN, Lowel GLAN, Lowel	tada	ta Context Results Anno Page: 1 of 1 tex lag p	tations Other Occurrences

Q11. Search for programs/tools that aided in the crime (Wireless Hacking)

Ans11: The programs which will be used for hacking purpose

1. Look@LAN

Look@Lan is an advanced network monitor that allows you to monitor your net in few clicks.

2. Cain

Cain and Abel is a password recovery tool for Microsoft Windows. It can recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks.

3. Network Stumbler

NetStumbler is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP.

4. mIRC

mIRC is an Internet Relay Chat client for Windows, created in 1995.

5. Ethereal/Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

6. 123WASP

WASP will display all passwords of the currently logged in user that are stored in the Microsoft PWL file.

How?

Click on Results --> Extracted Content --> Installed Programs

3 Milleri - Autopsy 4 14.0								21218
Case tries. Tools Weekna Help								
🔶 Add Data Seurce 🛍 Brages/Yideot 🎇 Cananuscotions 🗮 Tanetee 🚑 He Decov	ery Chie Case & Geler	ite Report				🖾 🐼 - 60p	and Lists	Qr Anyword Search
A	Links							(m.k.).*
	Installed Programs							32 Aug
G III Andres Clean	Telle Ittention							
- in with (mailwated: 0-62)	A CONTRACTOR OF							Save Table on ESV
(i) = volz (inter) / exect (tot2) (i) -troot/ii)								
	Southe File	1 0	Program Barre	2.8	9/1369	Toda Accerce	. 8	. C.
Li di Min Tanan	1d autoralia		8 Exessi 0.90.4 + 0.10.4		0-0-27 10.00 (0.01	-READ LANAUAS CPUBICS		
is g. Debeted Files.	M software		international and a second		4 00-07 (5:15:16151	4Ced Late are 0°1800		
in WD min taxe	M software		Tyrt-on: Sturker E-4.0	(teatore ces); 20		-Eleft LAMILIN (PERC)		
G W Results	N software		1.000(\$1.0% 2.50 Public 28	- 20	1-m-20 211 m-11 217	spearcounter (heral)		
E Extracted Curterit	M software.		123 Wints All Stoned Par	eniteda 200	44-00-20 15:13:00 IDT	-Cell Lattruby (MUD) -		
Enterprise Subjective (1)	waveflos br		For-artists Far Introduce	1P 01.00.0000 208	H-00-30 25.12 (0.151	-ENGLANAUM OF LEGT		
W Installeri Precesses (12)	N software		years.	-200	44-10-20 15 13 04 197	-iDel Laborator (PLEC)		
Copyrating System Information (2)	scare/more bo		Cristina	-20	# 00-20 25:09 II) IST	40x8 LMINUM 075800		
Coperating System User Arcount (8)	to an a second a se		028811	208	111 121 10101 1011	-stipit LAMA de OFISIO		
If Recent Decements (II)	M software		Forte agent		101-021-021-021-021-021-021-021-021-021-	4Dell Lottude (PUBD)		
Statistical Control (Statistical Control (Statisticae Control (Statis	variation br		Fabor Soys 4.2.4 Suml 2	13	4-00-00 10:07 20 107	-Delhustrute ONEDS		
# Web Backmarks (SI	M selfarers		Can & Abri (2.1 brief)	- 218	0-m-p) 2005-00 PT	Hall LMILLE ON TO		
Web Cookies (34)	M software		Anonymeter Bar 2.0 Oct	nora otto) 200	H 00-20 15X8 09 107	«Dell'Lannude (P1800)		
- E Web Websty (967)	to anti-take		Insident of a constant	6	H-ID-21 (23.04 76) 191	-Riel LMADE-DHECK		
With Search (4)	M software		Herosoft NetStein Pher	+ 210	100-2122-04 (0 T0T	40x11.x89.x8x 071800		
TO 15 Earth (Josef County County ())	terretice by		PPIant2	-20	H-00-30 22:04:26 807	4Dell LAMAste OF LEDI		
31 1 Single Come Report Depression Search (8)	N sufference		insideg.	10	PHILE R. 10, 10, 10, 10, 10, 10, 10, 10, 10, 10,	-cost concels more		
(a) 15 Email Addresses (a)(527)	Nanofice br		PC eadle	200	101 00 20 20 00 00 40	4Dell Lothude (PVIDO)		
Hudpet Hts	wantics br		Orwith/orward/	20	H-99-19 22:22 52 191	-Only Latitude (PLEC)		
G St C-Mail Messager	N solution		torPhysics)	200	04-020-19 20:00 02 001	-Rowit LAURAGE CPN 800		
a) go subar (journe)	to software		AddressBook	20	0-00-10122-01-01707	«Dall Lottude (PLDO)		
E Residie Zo Iorté (1)	te software		EDW:	10	P-01-19-22:31-51 Dr1	-Evel LMILde OF1805		
Accounts	tel software		Outstationesi	29	101-101-102 CT ICL RT	-theil Lobitate (PUBS)		
- Stat	to another		Overfit and a		4-00-09-22:20:07:07	«Dell'Lottuite CPUEDO		
e 🔐 tage	to automatic		PORTARIA		100.00.00.00.00.001	-Earl LANSING CHURCH		
-h Reports	34 internet							
	Inter Total Assistant Livin	I sta Metadata [(Ben fri Assessed					
	Paradit 5 of 37 1	4.4 fax		31	stated Programe			
	T.m.	1945 at					Re-shafed	
	104	Vese	144.54				new of it	
	Program Name	LOOKIDLAW 2.50 S	urio 28				Record Activity	
	Estivities	2004-08-25 13-3		Allow Mala Marine			Record Active)	
	hourse ree rubs	yeng 4ben Latta	a chilithia wanwadowa iyawa	11 contractors				
	1							1.0
								Show deals
	0 0 4	10.00					and the second second	Contraction of the local division of the loc

Q12. Which Email client is used by Mr. Evil?

Ans12: Outlook Express, Forte Agent, MSN Explorer, MSN (Hotmail) Email

How?

Click on Data Sources select 4Dell Latitude --> vol2 -->

WINDOWS\system32\config\software\clients\Mail

€ ⇒	0	Listing				
ur 🥦 neib (1921)		/img_4Dell Latitude CPi.E0	1/vol_v	012/	WINDOWS/system32/config	1
🕀 🔛 ime (12)		Table Thumbnail				
inf (1343)						
installer (6)						
Java (4)		Name	S	C	Modified Time	C
(15)		Current folder]			2004-08-20 04:20:28 IST	20
msapps (3)		(parent folder)			2004-08-27 21:02:31 IST	20
🔒 mui (2)		2 systemprofile			2004-08-20 04:18:25 15T	20
- Offline Web Pages (3)		AnnEvent Evt			2004-08-27 21:16:29 157	2
DE PCHEALTH (4)		default			2004-09-27 21-16-22 167	2
Prefetch (84)		default LOC			2004-00-27-21-10-35-151	
E Registration (8)		derault.cog			2004-08-27 21:02:50 151	2
repair (12)		derault.sav			2004-08-19 22:26:20 351	20
Resources (3)		SAM			2004-08-27 21:16:33 15T	50
erchaset (8)		SAM.LOG			2004-08-27 20:38:23 157	50
system (27)		SecEvent.Evt			2004-08-19 22:29:15 IST	20
system32 (1794)		SECURITY			2004-08-27 21:16:33 1ST	20
- 1025 (2)		SECURITY.LOG			2004-08-27 21:02:56 15T	20
- 📜 1028 (2)		software			2004-08-27.21:16:33.151	- 21
- 1031 (2)		software LOC			2004-08-27 21:16:32 15T	21
1033 (3)		and and a set of the s			2004 00 10 20/06/00 107	13
- 1037 (2)		Software.sav			2004-08-19 22:20:20 151	21
- 1041 (2)	Ξ.	SysEvent.Evt			2004-08-27 21:16:29 197	-21
1042 (2)		system			2004-08-27 21:16:33 157	20
2052 (2)		system.LOG			2004-08-27 21:16:33 15T	51
3076 (2)		system.sav			2004-08-19 22:26:20 IST	20
- 3 com dmi (2)		TempKey.LOG			2004-08-19 22:26:18 IST	20
E CatRoot (4)		userdiff			2004-08-19 22:26:20 IST	20
E CatRoot2 (9)		userdiff LOG			2004-08-19 22:26:20 15T	21
— 📜 Com (9)		acordiff LOC			0000-00-00 00:00:00	
🖂 🏓 config (23)		T aserdanceos			0000-00-00 00/00/00	
🕀 🛃 systemprofile (14)						
dhcp (2)						
Unerty (3)		1				
Glicache (2352)			_	-		_
export (2)		Haw Taut Application	Macina		The Metadata Content Dee	aulter
ias (4)		Text rext approximit	The paper light		tid metadata	Juits
- Licsami (7)		🕀 🍶 Anonymizer Bar			· · ·	lama
⊞ 📜 IME (5)		Anonymizer Plugin			A N	lumb.
inetsry (2)		E cozesy			N	lumbe
🕀 📜 Macromed (3)		E Classes			V	alue
🕀 📜 Microsoft (3)		Clients			Ξ.	
🕀 🔔 MsDtc (4)		🗊 🔔 Contacts			4	Vame
🖽 🔑 mui (4)		Internet Call			2	Defa
		Eorte Agent				
Let (a)		Hotmail				
Pastera (6)		MSN Explore	er			
Satur (18)		🕀 🗼 Outlook Exp	ress			
ShellExt (2)		(Default)				
(F) 3 spool (5)		A News				

Q13. What is the SMTP email address for Mr. Evil?

Ans13: The SMTP email address iswhoknowsme@sbcglobal.net

How?

F

Click on Data Sources select 4Dell Latitude --> vol2 -->

Program Files\Agent\Data\Agent.ini

🗠 Add Data Source 🚛 Brages/Videos 🌇 Communications 🇮 Timeline 🚚 File Descrier	e Close Case L. G	nerati Ra	port						O · toyou	dute:	Qu keyward Search
e e O	Loting (mg.shift Latitude CPU)	(mi_vel)	Program Files/Apert/Bale								(auto) (a) 35 Face/fr
G III 40el Lattade CKUD1 w volt (Unallocated: # 425	Lines (Targetone										Come Table as COL
D = vs2.0(75.) mFAT (bit7): 63.9(10470)	hatte	14.1	and the time	There are	Annual Term	Constant Trans	inter 1	(sheet)	- montherit	Proved.	Location III
 Solution (2) 	R Internet Balant		There is a real of the set	Include State	Drada in maker of	Tarray and the last set and		arrow sheet	alcored.		Jerry alterit actives (104
Unaloc (4)	C (periet Sales)		2014-08-00 (0.10.10.10.17	100408-0120-0121-027	BID-08-01 20-44-0 RT	1004-00-00 20 30 10 507	-	arra ated	abouted -		ing statistics of
B documents and Settings (7)	a terms		1000 OF 21 80 YO 27 27	1004-00-01-00160-07-007	2010/08/27 20:44-0.02	2004/09/21 00:50/22 022		Mitcahori	distant		Into strell attach C
III III My Documents (11)	0000152.047		1004-08-25 21 20 15 ST	1004-08-25 11:06:19:57	200-08-25-21:20:05-51	2004-08-25 ht 12-58 \$27	200005	to be a local and	Alcored	winely:	And whether the O
120MASP (9)	amodur 1 %2. 8000		mb4-cm-21 21, m 24 mz	2004-02-05 21-00-28 527	mp+ce-pt 21 (m.24 m7	2004-00-05.21 30:58 FtT	1.000	billocated	showed	atoms	And stretters of
iii 🔐 Azzezeo/een (2)	IDODE157.DAT		200409-25-21-41-47-87	2004/00-29 21-41-47 817	200408-25-23 45:07 [37	2009-02-25 21-12-02-827	20228	Miscoled.	clourer	ricer	Irra, Kellantek O
III Apent (20)	00000157.804		2004-08-25 21:42:07 (67	2004/08-25 21:42:07 57	2094-08-25 21:42:07 (57	2004-08-25 21 22:02 157	2090	40 oc shed	victored	winner.	/mg_40eliantede Cl
- ALCOV(4)	0000011M.DAT		3004-08-25 21 45 39 32	100101-05-21-42-39 817	2004-08-25 21 30 29 007	1004-00-05 21 10:09 817	-1111.0	line and	shored	or benefit.	Jug Relieven
a mmu-(2)	00000136.20x		2014/08/25 21:40:20 251	100408-25 21-40-08 22*	2004-08-25-21-43-09-157	2004-00-05-01-00104-027	3190	Allocated	ARCHER	veletion	Are deliated o
🚎 🚨 Anonymister (6)	00000449-204T		2004-08-25-21:94:20.007	100406-2521-99-25.007	2009-08-25 21:44 47:07	2004-00-25 11:100 08 67	99.228	stocated	Alcored	utitizen.	/mg_abetLateda 0
🗃 🥥 Cair (29)	000014/0.203		2010/08/25 21:44-41 227	100+00-01/1.4+-0 brt	3004-00-0521244-40107	2004-02-05-21-21/08 [07	240	plusted.	Inhomed -		/wg_meltamation
OWT(2)	ID000406.0A7		2004 CP 25 21-50 13-23	2004/01/25 23:50 13:57	2004/06/25 (1:00/14/05	2004/02/25 21:20:18 187	1550	Dested	Abored	rinne	Ing. Collatere C
ComPut registration (2)	model+id. IDX		300+04-2520-40-00 007	1004-05-25 12:449-46 127	101-08-25 21:49-64 51	104-06-25 11:52-01 402	745	triccated	Hoorist	intervit.	/rig 40s1(attate 0
III 🔔 DesctX (0)	10000401.5A7		2019-03-03-21-01-12-227	100408-0121-0112-02	INDP-CR-25 21-00-12 RT	10H0-01131UR1	1241	siturated.	shooted -		/wqmettamak-cr
🗟 🚨 Othereal (%)	00080483.EX		ID04 OF 25 21 (14/37/37	3004-00-25 21-44-67 827	201002521445725	2004/09/25 23 23 23 21	070	Historied	Alcosted	original	Ing. Kellande D
 Fober Teyr (10) Constraint Fit 	10000033.547		1014-06-25 21:47:00 017	3804-09-25 33 412-06 67	1004063521421535	3894-08-25.31 57 13 107	12036	dilocated.	Alcored	prineiro.	/eng_+Ourliartes/b (0
Solemet Copierar (s)	00000008.000		000449-2521-41.03.02	2004-02-21-21-47-28.827	2004-08-05-21-47-12-87	2004/09/05 21:00:10 07	A105	proceed.	integrat.	orknee	And the lattice of
E LookBurn (10)	TAG WACKING		200409-25-21-22-33-897	2009/00/25 21:12:01 817	2004-08-25-23 (25:33 (27)	2004/02/20 21:12:00 87	51304	Miscoled.	Aborted	riter	/ing.40e11amele C
Mansanger (14)	00003565-820		2004/08-25 21:47:48:167	2014/06-25 21 97:08 167	20449-25219796-61	2004-06-25 21:02:08 67	256	(ilocated	victored	stringen	/mg_40eliantede C
 a recrossft frontpage (0) 	TAL INCOME		300408-25.21.41/10.02	2004/01/25 23:47:53 8:7	2014/08/20 21:46:02 021	2014/01/25 22 32 32 31 107	Licrut	lincanel	stored	or lateral sectors.	(init) 400 Listen C
Dia Masia Malar (II)	000003688.20x		20140325214007.07	2304-08-25 21-40-07 87*	201408-0521-40-01-221	2804-00-25-21.52-33 32*	042	4000493	ARONE	printen	(ing., itel (article 0)
III A MSH(4)	ELAGONTUNE		2004-06-25-21:48:02-337	2014/06/25 21:00:02 31	1009-08-25-21-98-07-017	200408-210000-0267	LOOK	Hiscored	Accent	attravel.	(mg_4/millantesk-0)
iii 🔒 MSH Caming Zone (1)	ecolog.td		INF-0-2111-11-IL-IT	1009-00-01.01.07-00.027	3004-08-01 81/17/30 817	1004-00-0121-01-04 207	- 10	miniated	alcored.		/mg_40+14/646-0
- a settemoting (22)	TETERS DAT		2004 OP 21 82-41-00 227	2014/01/01 12:40:04 57	2004/01/01 02:40:00:22	2004/08/21 10:40 Ob 87*	3.	ADoc shot	Alteret	orining	long. Collattate C
Pethylox Sources (15)	FILTERS. DOC		30(+44-2112)42(10)107	1004-09-21 12:+0-08.827	2014/08/01 10:48:05:357	1004/06-01 02:40 02:167	10.	trice and	+looret	unicasió.	/rig_40s1(attack 0)
Outbolk Express [14]	*			and the second s							and the second s
III I NUSC(4) III Visional Information (36) Information (36)	lass field in more	Lesson I	File Metadota	its Annotations Uther Uco	eneration in the second se						
III unindows Modia Player (25)	Surge Indexed Ford										
tilindevet WT (7) tilindevettigdate (2)	Matcheo or page:	at	Ratch II - Pager I	1 of 1 Page + +					10	d Seurce:	milec *
	ANDEL DE For Information dans Formation de Marco Marco Perfola Formation de Marco Perfola Companya de Perfo Performante de Performante Performante de Perf	4 4411144 4 4 441144 4 4 4414	p ta maa fala, a Mija arma								â
E PART IN THE PART INTERPART IN THE PART INTERPART INT	*200000#0000000000000000000000000000000										

; 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"
EMailAddress="whoknowsme@sbcglobal.net"
EMailAddressFormat=0
ReplyTo=""
Organization="N/A"
DoAuthorization=1
SavePassword=1
UserName="whoknowsme@sbcglobal.net"
Password="84106D94696F"
SMTPLoginProtocol=2

Q14. How many executable files are in the recycle bin?

Ans14: There are 4 files in recycle bin

How?

Click on Data Sources select 4Dell Latitude --> vol2 -->

Recycler

M. McEan - Autophy 4 (MD)											hand the state
Case View Tools Window Help											
🔶 Add Data Seurce 👰 thispec Videos 🎇 Camerum catlens 🗮 Titheline 🚚 F	ie passwy 👩 Close Car	🗼 Generata Res	ert						O - tape	000 Lilles	Q: keyword likesd)
6 A	O Lotting										10100-0010
日 豊 Dels Sources 日 間 Abel Leftude (PLIN)	Talle Ithania	Teley, Links Lethnik (PLD1/WC)/RC/RC/RL0/5-1-5-21 2000/10/24 480/2644 (2002)/248 (2002)									
											Sale Table as CS#
	home	5.5	Modified Time	therge time	Access Tatw	Created Time	524	(100000)	Hap(Het)	toorei	Location
	(2. journent fail	(sec)	2004-0-21 2018 19151	2004-00-27 20:255 for the	2004-09-27 20 Skits BI	1004-09-25 21 10 22 247	10	incost-	stond-	antonists.	. Ang_east Lations of an
	W. Spin and Spin	ler]	1001-0-0115-0-05107	100+00(212)-01-02107	2014/01/22 42:01/21	100108-0520-0107	101	Alcolet.	410,000	about	/imp_stice[1406ade/07/08
 B Social and Social (1) B My Recurrents (11) 	F Bct.est		1004-06-05-01-01-02-07	10H (0 223 H) 251T	204-01252138-00387	1004-00-2521101-34107	1100000	Aborts!	200200	street.	ing statuted on it
Triggtan (file) (20) Altrians (2) Altrians (2) Altrians (2) Altrians (2) Altrians (2) Altrians (2) Altrians (2)	8 82.00		100H-00-07,80.40.011611	2004-00-2110-40101111	208-0-2730-0710.01	1004-de er picke af tel	LIDYDE:	which the	short-	arkitelery.	/wgmail.intole-cPut
	(States)		3009-00-07 30-44 00 507	3004-09-27-20-45-00-057	2004/01/27 22:49:14:27	2004-00-07-20-44-20-207	4124[7	Allocated	Alterial	articularly	/ing_dGell Littlede CP\ 53
	E lot.mo		2004-01-27 20:54 34 517	2004-00.27 20:59:50 GT	2010/08/27 20:59-47 187	2804-09-27 20:04-24 557	046850	+located	Alecater	arkenet.	/ing_40ed Latitude CP-20
	(5) destroy in		2004-08-05 (1.46 (2. 101	2014/09/25 21 46:25 217	2004-06-27 20-42 81 81	(004-00-05-01-08-05-Diff	45	interated	smooth.	40000	/ing_40x11415.dk cPuit
- wrone (1x)	, p.P03		2004-08-07-02-08-07-PUT	3034-09-27-23-08-17-197	309-01-2721-0-12-02	2014/08/25 21:48 25 257	100	Are stat	10x,4yl	20110	integration (athone circum

Q15. Are there any malware on the computer?

Ans15: Yes there is a zip bomb malware by the name of unix_hack.giz in this system. **How**?

Click on Results --> Extracted Content --> Interesting Items --> Possible Zip Bomb -->Interesting Files



Q16. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the userid,

Ans16: user=Mini Me, email=none@of.ya, nick=Mr, anick=mrevilrulez **How**?

Click on Data Sources select 4Dell Latitude --> vol2 -->

Program Files\mIRC\mirc.ini





Q17. Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?

Ans17: File name is Interception

How?

Click on Data Sources select 4Dell Latitude --> vol2 --> Document and Settings\Mr.Evil\intercerption

Mittel - Autopsy 4.140											
Case Yiew Tools Window Help											
🕂 Add Sele Searce 🛺 Janges Walves 📓 Communications 🗮 Trimologi 🚑 Tile Discovery 🍙 Elser Ease 🗽 Generative Report											
6.5.	Liston 1										
T B. Data Garage	/mg_40ell Lutitude CPLEEL	(vol_soD/Documents and Settings/Wr.	Evil								
	Table Thursbried										
(ii) ···································											
Gi SCrphanFilex (0)	Norse my Locusioners	S C Medited Time	Change Time	Access Time	Credice Time:	5454	Pilogs(Dy				
standar (5)	Authood	2004-08-26 20:30:15 157	2004-08-36 20:36:13 151	2004-08-26 20 38:15 151	2004-08-20.04 (94) 05 EST	35	Allocated				
E Doouments and Settings (7)	Printbood	2004-08-19 22190-09157	2004-08-20 04 94 08 fST	2004-08-26 20 37 44 151	2004-08-20 04 94 09 157	-8	Allocated				
iiir 💄 All Users (9)	Recent	2004-08-25 20:38:14 157	100+-09-26 20138: 14 157	2004-08-27 20 H4 40 IST	2004-08-20 04:34:05 197	36	Allocated				
🖶 🛃 Default User (98)	SendTo	2004-09-20 04:34 15 157	2004-09-20 04:34:15 167	2004-09-20.20 x7:59 IST	2004-09-20-04:24:05 IST	- 55	Necated				
E Locifience (ii)	Start Menu	2004-09-19-22 20:09 157	2004-09-20 04:34:05 157	3004-09-27 20:30:08 IST	2004-08-20.04-24-05 157	255	Alticated				
B Application Data (6)	Templetes	2004-00-20 03:54-35 157	2004-00-20-04-34-00 157	1004-08-20 20:47:59 (51	2004-02-00-04-34-05 157	-90	Alterated				
Contien (27)	gtt-bestments	2004-08-27 21 10 45 157	2004-08-27 21 10-43 157	2004-08-27 21 10 43 157	2004-08-27 21 00 49 157	- d	Allocated				
(i) Denklop (2)	aderception	3004-08-27 21:11:00 157	1004-09-17 21 11:00 IST	2004-08-07 21:11:00:157	2004-09-27 21:11:00-157		Alecated				
B Fevorities (6) Figure 1 Settings (7)	ATUSER.DAT	2004-08-37 21:16 23 197	3004-09-27 21:16:15 157	2004-06-37 21:16:23 197	2004-08-20 04:34:05 IST	796432	discaled				
E Ma Documents (8)	muner, dat.105	2004-08-27 21:16:22 157	1004-08-17 11:16:27 07	3004-00-27 21:16:23 121	2004-09-20 04:24:06 15T	1024	Allocated				
(ii) (ii) Netritood (9)	ilij atuser.ini	2004-08-27 21-16-22 157	2004/08/27 21:16:23 157	2004-08-27 21:18:23 151	2004-00-20-04-34;00.157	100	Allocated				
Print-Isod (2) Recent (11)	•		14		1						
- Sendfa (7)	Ince Test Internet Internets Internets Internets Annalis Annalis Annalis Other Occurrences										
🔒 Templates (14)	Strings, Indexed Test discrimina										
WetworkSeries(0) We Decaments (11)	Matches on page:	al - Math 4.4 Page: 1	ul S Page 🗄 🚸								
	Re-Manage PROM Reference integrational and a Normal program in the Source of the Sou	n markat kalen argabar 1800 (1944) Gan magaziden, 2012 A.G., Badere D., DR Market-da-Ottore Posterie Sciences (1990) (1990) (1990) (1990) (1990)	+ 1988-1986 (alars - ACTORA C. 1998-1981) Setu: PCTICIM PRIMAR (parts of Setu: PCTICIM PRIMAR (parts of Setu: PCTICIM PRIMAR (parts of parts of par	ergeli TTTRactority, LTMA TTTTLA LTRACANONIQ(1	11244. Karacarapati datu		u. 197 (d. 19				

Q18. Which internet browser was used?

Ans18: Internet explorer **How?**

Click on Data Sources select 4Dell Latitude --> vol2 --> Document and Settings\Mr.Evil\intercerption

scroll down and see User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)

Miller Autops 4142											- CI 62	38
Case Vive Tooli Window Herp												
Add Data Source 🛄 Brages Weese 🔛 Communications 🗮 Timeline 🚚 File Despe	wry 👩 Close Cause 🔈 Gener	ato Popo	w.					-	• • • • • •	verd Later	Q: toyward Sear	¢.
(t) (t) (D)	USA									(A) A		
🖓 🖬 Beta Sources	Trade Table Strategies (Constraints of the Strategies of the Strategies of the Strategies of the Strategies (Strategies of the Strategies											
S III 450 Little OVB1	and the second second										Contract Watter and	
D w vs2 0075 / auFAT (buf 2: 63-95(0420)											- 5400 (Orac 44)	100
🖌 SOrphonFiles (II)	Note	5.5	Modified Time	Charge Titlet	Accost Tatto	Created Time	501	Flags(3v)	Flags(Meta)	Ancest	Location	. 8
2 204mrd (5)	Darrenk Kokler)		2004/09/02 04:04 65:07	2004-00120.0+14-01 257	2004-09-02 00 06 95 827	2004-00-10-225-03-01.157	-85	Alterial	Alterial	19171-01	/wg.idel/Lithier	10
2. Stratec (4)	🙀 Apployser beta		1004-06-07 31:05 52:57	3004-69-22 24:38:55 557	1004-06-/715-12-40-57	2004-89-20.04.04 85 597	55	Abouted	Abrahd	URDED.	Ving_40481.000008	
ID Althers(9)	🙀 tostaes		309-09-27 20-48 2010	3204-0317721.12.81737	2004-00-07-21-12-40-071	304 01:00 04 29 00 151	210	alasied.	alaxied.	(b)b(b)(c)	/re_statute	2
🚃 🥥 Dufbult Boor (54)	Restau		2004-00-07-21-08-05-027	300+02-07-21-05-07-197	2004/02/27 21:48:45:121	2004 80:00 04:04 05:57	- 55	48,000	Abortot	IFRIDAY.	/ing_10eX (actual)	
E Lossferice (I)	🗸 Fayodias		2004-35-30 04 34 57 117	3004-69-22-04 31 57 67	2004-09-22.00.08.23.057	2004-89-29 04:34 05 ST	35	K8catel	KRcated	animent of	Jung Alab Laboration	(m.
 MCBH (29) Application (and (2)) 	Lick Settings		3004-08-29 22 28 89 517	2004-09-27 20 88-24 207	2004-020/27 20:38-20.227	2004-00:00 04:34 05:511	-50	sticted	sticited	10000000	/mg_distantion	2
Cooker (27)	Ma Gecumento		3004-09-20 04-04-81 57	2004-80-20 20:58 (07 157	2004 00:27 20 38 40 357	2004 40:00 04:04 00 107	-86	Alcolari	Alcolari	and the second	/wg.itetistee	25
(2) 2. Ondersp (2)	Activity Sections		2004-08-05 20138 15 67	3004-09-25 20 10:25 157	2004-08-38 20:38 55 157	2004-89-22 04:24 (25 557	35	Abouted	Abouted	aritra international	Ang_4041 Latters	10
(ii) iz Failerthia (k)	🐺 Ty attead		2004-02-19 22:28 39 197	2004-05-20 04:34 20 151	2004-03-20.20.27-44 211	2004-01-20 04 04 20 201	10	1000 April 10	1000485	arkininen	And the production of	
 a cost settings (7) b motorement (8) 	Contract of Contra		2004-06-36-20.08 (9-15*)	2004 89/25 20 38 34 201	2004 (0) 17 20 44 40 157	2004 00:20 04:34:05 157	.50	ARCENT	ARCHIT	and a second	Veg, KDel Libbary	
Mo Music (4)	Seedia Seedia		2009-09-00 04:09:05 5/1	2004-09-22-04 241-05-047	2004-08-00 30 =7 59 57	2004-09-22 04:39 151 151	55	wpeaked.	Abutal	210 Dept	Judi April and and	
A My Petrova (4)	A That Plans		2004-02-14-22-28 (0.127	2004-01/201104-04-02-217	2004-08-277 (0.188-86) 227	1004-00-00-04-04 (00-027	20	Audel	(dashe)	4000000	/mg_4541.48.0.00	m
(ii) iii Hechood (iii)	Completion 2		2004-09-20 02-04-35 127	2004 00/20.0+/34/00 107	2004-06-00 20-41-59 201	2004-00120-04-24-055-557	- 86	Aborted	Alterial	1911	Avg. Rehlattice (25
Prind Rood (2)	gik-baskmadat		100+060731111 x0.527	3004-68-22 24:12:40-657	2004-06-/715-18-47-57	2004-09-07-01:12:50:101	1	Alternation (Alternite)	intro-h	/ing_40481.utitude (01
 Pochiti (11) Sandia (11) 	ateceptor		2014/08/27 21:12 09:07	1084-00-07 St. 11 St. FT.	THE R. P. LEWIS CO., NAMES AND ADDRESS OF ADDRESS OF ADDRESS A	100+2007211130.0T	112111	o'Tauled	standed .		And support of the second	15
(i) Z Start Mena (4)	TAR, REBUTA		300+00-07-22-38 02-507	300+49-07-25 (5-0) 197	2004-00-27-21-1A-25-ET	2004 82:20 04 24 05 57	700412	10,000	480.001	TRIDE	/reg_40e3 (althout	2
Z. Tempintur (14)	There del LOS		2004-06-07-21:18 (2) 87	3004-69-32 28:10:32157	2004-02-27 21-18:27 157	2004-89-22.04.34.05.197	5004	K Example	x-bcated	animore	Jung Alebiantics	(n)
III III Mahvarkšenica (II)	S-share as		2004-08-277 21, 18, 23, 517	1004-0107721-11221107	2004-08-07-21-18-21-021	2024-00-20.04.34 20.017	245	Alighted	Alizabet.	10.000	/wq_4041484001	(P)
Me Decuments (11)	1	_		10								*
III I RECYCLER (D)	Concernance of the second second											
 System Volume Information (3) 	Inter Test Internet Internet Fac Metadate Free Annuals Acceletations (the Generation										_	
Temp (2)	-strengs, Indexed 7-od 1020	coding.										-
2 WHOR (103)	Matchae of page: - If		Mdh # Paper 6	11'5 Page #						feet Searce:	Sill Loc.	
at which makes that a Solate a Solate	The second											
E E Neve	Filt											1
Lik vill. File Types	Arrent +(*											18
G + Deleted Files	Th-10: Women CE (Traded F)	5 - PH	1118 4.12									
Li Bander	Repionia: Dibilit											
G 🗃 Genetid Caman	Th-OT, Invelide Points											
Staryptice Suspected (1)	lines in maile and	and by D	dan any he think that	-Litter in Log-Million	49-1							
8 Edension Momatch Extended (II)	The Languages, Developing and a serie											
M butsled Programs (12)	Decimer, Southers, Line	mate	Mill Avia Tamer, Rollin	a privite								
 See Operating System Enter Revolution (2) Characterize Sectors Enter Revolution (3) 	Tissaition Bassing											
 Recent documents (9) 	haar benefit, ara, and	Las-line	aspertation water products	Mail III I Containing Propagation	The second second second second	Gall, withor-tystyledalab	(elisatoria	a Wisefiling	ngalitation	Collocation (Collocation)	inghter mitteer Right	65
 Shell logs (St) 	Print Provide State		and a second second second	are in a new manifestion	and the second							
 El infili bevos Attached (3.) 	HTELL HAR Prove											
Web Societaria (K)	falls, byle, if any sitts of all	10.00										
 Web sintex (307) 	to Transmitty, Mit. Mit.	- 181	The last last, read									
web Search (10)	incoment total controls and	I (m) Text	NAME AQUITATION CONTACT	an investment of a second second	*****							
18 3 Reymond Reto	Dente The method, the	interior.	54									
G 🐂 Haufued Hitz	· Tronast-Sample 110											1
	And the second se										Statio de	aktro
	0.00	-		34						20	And in case of the local division of the loc	100
											23014	

Q19. What websites victim was accessing?

Ans19: login.passport.com, mobile.msn.com, <u>www.passportimages.com</u> How?

you can also copy all texts from **intercept** file and search for the .com it will show you the websites which were visited.



Q20. What is the web-based email address for the main user?

Ans20: mrevilrulez@yahoo.com was found in web history.

How?

Click on Results --> Extracted Content --> Web History

I have used Windows 7 Magnifier to zoom in

		Matches on page: - of - Match - Page: 1 of 1 Page -				
	= 	RL isited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/JhowFolder?YY=701696.first=14box=I ahoo! Mnil - mrevilcules@yahoo.com RL /isited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/Logout3YY=276306.first=16ine=256or RL /11-	nbostW=1	=dateSpor=0/		
10 10 10 10 10 10 10 10 10 10 10 10 10 1	1000.1	Similar Me. PoilShann://www.s50.com/artes.html		10-100 h		
tiew Togs Bindow HeD				1 Standard		
tal bata les.es 💼 (menes/Valeon 🛐 Campus cations 🗮 Timele	ine a File Descrive	ry 📸 Close Eau 🗽 Sciences Report	49 - Report Lata	Qr Reported Seenth		
*	0	Linny Vice Linner		ida e iz aŭ 2. de		
III A TANKANS (1) III and repair(1) (ad-(1)	6	Tolde Thurderso		Save Table an CS		
(a) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c		And a second	Maniforme	Owto Source		
- · · · · · · · · · · · · · · · · · · ·		There are a construction and a c	H. Dil	mont Larbards (11) ED		
ie (j 44(1)(1) ie 🖓 deveload, il ato (1)		Z rdeuter http://www.f0.com 2004-00.00 ET InvenierEuptore www.f0.com	597. Eccl	Cod Lanuale CPSIII		
iiiiiioaaa/Wiv(i)(i) iiiiiioaaa/Wiv(i)(i)		Enderstall By prevery sy-depail adopted units for 2019 27 2017 2017 2017 2019 2019 2019 2019 2019 2019 2019 2019	NY LVV	-Last Larcholy CPL PE		
III- 🖉 PTVHINIQ (IIN)		E wins data Trips (swith an convention approximation of the convention of the second s				
$ 0 = w _{2}(1)(1)$ $ 0 = w _{2}(2)(1)$						
arCADDOBLORMATE(1); arCADDOBLORMATE(1);		Team Tead /				
12(1).ev(1)		Story Ment Tel Contant	Teel Names Pale Test			
Manager (4)		Refer to both a series of the				
By Facharon (*)		na Razeri Ia, Parinapi lan dil and presente la fasteri della di antica da antica da antica da antica da antica da a				
Providenced (2)		New York The Control of the Control of the Control of C				
haryElo (/)		ma. I la				
and a Mark More (4) Transplated (14)		Restance Bar Excellence (New All conclusion from		1		
E 2 Autoconcervers (1)		Proceeding Annual Annual Construction of the Annual A				
E E Program Films (15)		No. 200 Transfer and antiparticipation of a financial statements and a financial statements and a financial statement a	47338am			
Splan Value Murstalia (3)		No. 1 Control of the second statement of the second st				
A Terrar (2)		Alarah Terret Tea.				
Canal American And Ann American		Ale Provide Bit Antighting (1999 All 199				
T Year		ten del ville lectri e hecitte ficiel. Mil				
in a Desited Field		10 Transf. W. Antilling C. S. Comparent and Michael Sciences in the				
a Million Sets		The set is the set of		(e)		
det 2000				0		

Conclusion

Computers Forensics is a vast field of study and includes topics like Processing Crime Scenes, Operating Systems and File Structures, Recovering Graphic Files and Defeating Steganography, Email Investigations, Mobile Device Investigations, Report Writing.