Investigation Methodology

This methodology outlines the high-level process for conducting a digital forensics investigation using Autopsy 4.20 on a seized hard drive from a washer. Autopsy 4.20 is a powerful open-source digital forensics tool that allows investigators to analyze, search, and recover potential evidence from the storage media. The investigation follows a systematic approach, including preparation, acquisition, examination, analysis, and reporting stages, to ensure the integrity and admissibility of the digital evidence collected. This methodology aims to assist digital forensics professionals in effectively utilizing Autopsy 4.20 for the examination of the washer's hard drive while adhering to best practices and maintaining the chain of custody.

Autopsy assists forensic investigators and law enforcement agencies by recovering deleted files, conducting keyword searches, creating timelines of user activities, analyzing metadata, comparing hash values, examining the Windows Registry, analyzing artifacts, establishing link analysis, generating comprehensive reports, and integrating with other digital forensics tools and databases. Its capabilities aid in efficiently and effectively examining and analyzing digital evidence, providing valuable insights and evidence for legal proceedings. However, it is essential to emphasize that the successful outcome of any investigation relies on the expertise and adherence to proper procedures by the forensic investigators handling the case.

To ensure a seamless and efficient investigation, we diligently adhere to the standard operating procedures (SOPs) outlined in the provided documentation. These SOPs encompass every aspect of our investigation, from incident reporting and response protocols to meticulous documentation and reporting procedures. We handle evidence with the utmost care, preserving its integrity and admissibility to bolster the credibility of our findings. With these protocols as our guide, we set out on a journey of examination and analysis, utilizing the full potential of Autopsy and FTK to extract relevant data and unearth hidden information that may hold the key to the case.

Evidence

1. Time Zone analysis

Drag a column header here to group by that column

Value Name	Value Data	Value Data Raw
Bias	300	300
StandardName	Eastern Standard Time	Eastern Standard Time
StandardBias	0	0
StandardStart	Month 10, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-0A-00-05-00-02-00-00-00-00-00-00-00-00-00
DaylightName	Eastern Daylight Time	Eastern Daylight Time
DaylightBias	-60	429496723 6
DaylightStart	Month 4, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-04-00-01-00-02-00-00-00-00-00-00-00-00-00
ActiveTimeBias	300	300

2. Operating System information

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID	Owner	Data Source
Washer (5).E01				WASHER1	Microsoft Windows XP	x86	%SystemRoot%\TEMP	C:\WINDOWS	55274-338-5471047-22865	John Washer	Washer (5).E01

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
BuildLab	RegSz	2600.xpclient.010817-11...			
CurrentBuild	RegSz	1.511.1 () (Obsolete dat...	69-00-6E-00		
CurrentBuildNumber	RegSz	2600	01-00		
CurrentType	RegSz	Multiprocessor Free	40-9F-01-00		
CurrentVersion	RegSz	5.1	40-9F-01-00		
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-0...			
InstallDate	RegDword	1185326166			
LicenseInfo	RegBinary	34-96-57-38-58-42-42-8...	10-6B-7D-00		
PathName	RegSz	C:\WINDOWS	00-00-00-00-00-00		
ProductId	RegSz	55274-338-5471047-228...	00-00-00-00		
ProductName	RegSz	Microsoft Windows XP	44-00		
RegDone	RegSz				
RegisteredOrganization	RegSz				
RegisteredOwner	RegSz	John Washer	24-8A-72-88		
SoftwareType	RegSz	SYSTEM	01-00-A8-3A-01-00		
SourcePath	RegSz	D:\I386	00-00-00-00		
SystemRoot	RegSz	C:\WINDOWS	01-00-70-A4-01-00		

Computer Name:

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Valu
ComputerName	RegSz	WASHER1	41-0

3. Installed programs

Installed Programs 23 Results

Table Thumbnail Summary

This is a DataResult window

Save Table as CSV

Source Name	S	C	O	Program Name	Date/Time	Data Source
software			0	WinZip 11.1 v.11.1.7466	2008-02-13 01:17:01 EET	Washer (5).E01
software			1	WebFldrs XP v.9.50.5318	2007-08-04 01:19:51 EEST	Washer (5).E01
software			1	Microsoft NetShow Player 2.0	2007-08-04 01:19:49 EEST	Washer (5).E01
software			1	MPlayer2	2007-08-04 01:19:49 EEST	Washer (5).E01
software			0	Viewpoint Media Player	2007-07-25 17:52:43 EEST	Washer (5).E01
software			0	Adobe Flash Player 9 ActiveX v.9	2007-07-25 01:38:30 EEST	Washer (5).E01
software			0	AOL Instant Messenger	2007-07-25 01:27:20 EEST	Washer (5).E01
software			1	Branding	2007-07-25 01:14:06 EEST	Washer (5).E01
software			1	PCHealth	2007-07-25 01:13:05 EEST	Washer (5).E01
software			1	AddressBook	2007-07-25 01:13:01 EEST	Washer (5).E01
software			1	DirectAnimation	2007-07-25 01:13:01 EEST	Washer (5).E01
software			1	ICW	2007-07-25 01:13:01 EEST	Washer (5).E01
software			1	NetMeeting	2007-07-25 01:13:01 EEST	Washer (5).E01
software			1	OutlookExpress	2007-07-25 01:13:01 EEST	Washer (5).E01
software			1	DirectDrawEx	2007-07-25 01:12:58 EEST	Washer (5).E01
software			1	Fontcore	2007-07-25 01:12:58 EEST	Washer (5).E01
software			1	IE40	2007-07-25 01:12:58 EEST	Washer (5).E01
software			1	IE4Data	2007-07-25 01:12:58 EEST	Washer (5).E01
software			1	IESBAKEX	2007-07-25 01:12:58 EEST	Washer (5).E01
software			1	IEData	2007-07-25 01:12:58 EEST	Washer (5).E01
software			1	MobileOptionPack	2007-07-25 01:12:58 EEST	Washer (5).E01
software			1	SchedulingAgent	2007-07-25 01:12:58 EEST	Washer (5).E01
software			1	Connection Manager	2007-07-25 01:07:57 EEST	Washer (5).E01

4. Documents, media, pictures, etc.

Listing

Images 1058 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(D...	Flags(Meta)	Known	Location
frmp-bg-savedclose[1].png			0	2007-07-25 22:05:56 EEST	2008-02-13 21:37:39 EET	2008-02-13 21:37:39 EET	2007-07-25 22:05:56 EEST	567	Allocated	Allocated	unknown	/img_Washer (5).E0
frmp-bg-smallboxbtm[1].png			0	2007-07-25 22:06:19 EEST	2008-02-13 21:37:44 EET	2008-02-13 21:37:44 EET	2007-07-25 22:06:19 EEST	1049	Allocated	Allocated	unknown	/img_Washer (5).E0
icon-btn-aerial-view-v2[1].png			0	2007-07-25 22:06:22 EEST	2008-02-11 21:29:13 EET	2008-02-13 21:37:49 EET	2007-07-25 22:06:22 EEST	2702	Allocated	Allocated	unknown	/img_Washer (5).E0
icon-start1[1].png			0	2007-07-25 22:09:30 EEST	2008-02-13 21:37:46 EET	2008-02-13 21:37:46 EET	2007-07-25 22:09:30 EEST	1942	Allocated	Allocated	unknown	/img_Washer (5).E0
logo_su_36x36[1].png			1	2007-07-25 23:21:39 EEST	2008-02-13 21:37:47 EET	2008-02-13 21:37:47 EET	2007-07-25 23:21:39 EEST	2207	Allocated	Allocated	unknown	/img_Washer (5).E0
map-controls-top-bg[1].png			0	2007-07-25 22:06:22 EEST	2008-02-13 21:37:47 EET	2008-02-13 21:37:47 EET	2007-07-25 22:06:22 EEST	216	Allocated	Allocated	unknown	/img_Washer (5).E0
revert[1].png			0	2007-07-25 22:06:22 EEST	2008-02-13 21:37:49 EET	2008-02-13 21:37:49 EET	2007-07-25 22:06:22 EEST	2909	Allocated	Allocated	unknown	/img_Washer (5).E0
z-7[1].png			1	2007-07-25 22:06:21 EEST	2008-02-13 21:37:39 EET	2008-02-13 21:37:39 EET	2007-07-25 22:06:21 EEST	571	Allocated	Allocated	unknown	/img_Washer (5).E0
z-on[1].png			0	2007-07-25 22:06:22 EEST	2008-02-13 21:37:40 EET	2008-02-13 21:37:40 EET	2007-07-25 22:06:22 EEST	593	Allocated	Allocated	unknown	/img_Washer (5).E0
z-11[1].png			1	2007-07-25 22:06:21 EEST	2008-02-13 21:37:40 EET	2008-02-13 21:37:40 EET	2007-07-25 22:06:21 EEST	601	Allocated	Allocated	unknown	/img_Washer (5).E0
z-14[1].png			1	2007-07-25 22:06:21 EEST	2008-02-13 21:37:40 EET	2008-02-13 21:37:40 EET	2007-07-25 22:06:21 EEST	591	Allocated	Allocated	unknown	/img_Washer (5).E0
z-3[1].png			0	2007-07-25 22:06:21 EEST	2008-02-13 21:37:39 EET	2008-02-13 21:37:39 EET	2007-07-25 22:06:21 EEST	578	Allocated	Allocated	unknown	/img_Washer (5).E0
lojban_icon.png			0	2004-02-22 03:14:37 EET	2008-02-13 02:34:40 EET	2008-02-13 07:28:01 EET	2008-02-13 07:28:01 EET	1121	Allocated	Allocated	unknown	/img_Washer (5).E0
pee limit.jpg			1	2007-07-25 23:24:52 EEST	0000-00-00 00:00:00	2008-02-13 03:01:26 EET	2007-07-25 23:23:09 EEST	349948	Allocated	Allocated	unknown	/img_Washer (5).E0
blocks_image_0_1.png			1	2008-02-13 02:43:04 EET	0000-00-00 00:00:00	2008-02-13 02:43:12 EET	2008-02-13 02:43:12 EET	164279	Allocated	Allocated	unknown	/img_Washer (5).E0
pee limit.jpg			1	2007-07-25 23:24:52 EEST	0000-00-00 00:00:00	2008-02-13 03:01:26 EET	2007-07-25 23:23:09 EEST	349948	Allocated	Allocated	unknown	/img_Washer (5).E0
220[1].jpg			1	2007-01-12 21:59:00 EET	2008-02-13 03:23:28 EET	2008-02-13 07:24:49 EET	2008-02-13 07:24:49 EET	411003	Unallocated	Allocated	unknown	/img_Washer (5).E0
43366488_75[1].jpg				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_Washer (5).E0
icon18_wrench_allbkg[1].png				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_Washer (5).E0
SK10[1].jpg				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_Washer (5).E0
drig[1].jpg				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_Washer (5).E0
SK01[1].jpg				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_Washer (5).E0
101[1].jpg				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_Washer (5).E0
102[1].jpg			1	2008-02-13 04:22:09 EET	2008-02-13 07:22:54 EET	2008-02-13 07:23:16 EET	2008-02-13 04:22:09 EET	783	Unallocated	Allocated	unknown	/img_Washer (5).E0
103[1].jpg			1	2008-02-13 04:15:54 EET	2008-02-13 07:22:54 EET	2008-02-13 07:23:17 EET	2008-02-13 04:15:54 EET	684	Unallocated	Allocated	unknown	/img_Washer (5).E0
103[2].jpg			1	2008-02-13 04:15:51 EET	2008-02-13 07:22:54 EET	2008-02-13 07:23:16 EET	2008-02-13 04:15:51 EET	550	Unallocated	Allocated	unknown	/img_Washer (5).E0
103[3].jpg				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_Washer (5).E0

Videos

Table | Thumbnail | Summary

33 Results

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Loc
1202410556[1].swf			0	2008-02-13 02:57:44 EET	2008-02-13 07:31:25 EET	2008-02-13 02:57:44 EET	2008-02-13 02:57:44 EET	25019	Allocated	Allocated	unknown	/img
CAQT4J07.swf			0	2008-02-13 02:58:24 EET	2008-02-13 22:50:33 EET	2008-02-13 22:50:33 EET	2008-02-13 02:58:24 EET	30557	Allocated	Allocated	unknown	/img
tell_me[1].swf			1	2008-02-13 03:16:02 EET	2008-02-13 07:31:38 EET	2008-02-13 03:16:02 EET	2008-02-13 03:16:02 EET	28744	Allocated	Allocated	unknown	/img
fuid[1].swf			1	2008-02-13 04:23:13 EET	2008-02-13 22:50:32 EET	2008-02-13 22:50:32 EET	2008-02-13 04:23:13 EET	1522	Allocated	Allocated	unknown	/img
world_map_05[1].swf			1	2008-02-13 03:51:38 EET	2008-02-13 07:31:39 EET	2008-02-13 03:51:38 EET	2008-02-13 03:51:38 EET	139810	Allocated	Allocated	unknown	/img
CA8HALNO.swf			0	2007-07-25 21:19:08 EEST	2007-07-25 23:39:46 EEST	2007-07-25 21:19:08 EEST	2007-07-25 21:19:08 EEST	9791	Allocated	Allocated	unknown	/img
CAAVA7UX.swf			0	2007-07-25 22:06:22 EEST	2007-07-25 23:39:46 EEST	2007-07-25 22:06:22 EEST	2007-07-25 22:06:22 EEST	19427	Allocated	Allocated	unknown	/img
CAETSDCY.swf			0	2007-07-25 23:20:12 EEST	2008-02-13 21:29:18 EET	2008-02-13 21:29:18 EET	2007-07-25 23:20:12 EEST	4696	Allocated	Allocated	unknown	/img
imgad[1].swf			0	2007-07-25 21:19:49 EEST	2008-02-13 22:09:58 EET	2008-02-13 22:09:58 EET	2007-07-25 21:19:49 EEST	11744	Allocated	Allocated	unknown	/img
CA49E1B4.swf			0	2007-07-25 21:23:57 EEST	2007-07-25 23:40:36 EEST	2007-07-25 21:23:57 EEST	2007-07-25 21:23:57 EEST	29731	Allocated	Allocated	unknown	/img
CA67KFPQ.swf			0	2007-07-25 20:51:45 EEST	2007-07-25 23:40:36 EEST	2007-07-25 20:51:45 EEST	2007-07-25 20:51:45 EEST	54946	Allocated	Allocated	unknown	/img
flash2[1].swf			0	2007-07-25 23:20:33 EEST	2007-07-25 23:40:42 EEST	2007-07-25 23:20:33 EEST	2007-07-25 23:20:32 EEST	82321	Allocated	Allocated	unknown	/img
FXDamages_300x250_Bnr_072007[1].swf			0	2007-07-25 21:23:52 EEST	2008-02-13 21:34:45 EET	2008-02-13 21:34:45 EET	2007-07-25 21:23:52 EEST	15499	Allocated	Allocated	unknown	/img
AOL_500x300user_FL8[1].swf			0	2007-07-25 21:19:09 EEST	2007-07-25 23:41:19 EEST	2007-07-25 21:19:09 EEST	2007-07-25 21:19:09 EEST	155996	Allocated	Allocated	unknown	/img
lmb_lre_PassStRtCredLPMCnectDrawhseCalc15sec_MC6			0	2007-07-25 22:10:33 EEST	2007-07-25 23:41:27 EEST	2007-07-25 22:10:33 EEST	2007-07-25 22:10:33 EEST	53622	Allocated	Allocated	unknown	/img
jp[1].swf			1	2007-07-25 23:22:55 EEST	2007-07-25 23:41:27 EEST	2007-07-25 23:22:55 EEST	2007-07-25 23:22:55 EEST	41655	Allocated	Allocated	unknown	/img
women1[1].swf			0	2007-07-25 23:22:56 EEST	2007-07-25 23:41:33 EEST	2007-07-25 23:22:56 EEST	2007-07-25 23:22:48 EEST	108285	Allocated	Allocated	unknown	/img
bwtest[1].swf			0	2007-07-25 21:19:11 EEST	2007-07-25 23:42:01 EEST	2007-07-25 21:19:11 EEST	2007-07-25 21:19:11 EEST	37997	Allocated	Allocated	unknown	/img
CAIJWXMZ.swf			0	2007-07-25 20:51:00 EEST	2007-07-25 23:42:02 EEST	2007-07-25 20:51:00 EEST	2007-07-25 20:51:00 EEST	85326	Allocated	Allocated	unknown	/img
CAXGK315.swf			0	2007-07-25 20:51:33 EEST	2007-07-25 23:42:03 EEST	2007-07-25 20:51:33 EEST	2007-07-25 20:51:33 EEST	34300	Allocated	Allocated	unknown	/img
CAZUORFL.swf			0	2007-07-25 20:53:31 EEST	2007-07-25 23:42:03 EEST	2007-07-25 20:53:31 EEST	2007-07-25 20:53:31 EEST	6003	Allocated	Allocated	unknown	/img
jp[1].swf			1	2007-07-25 23:20:29 EEST	2007-07-25 23:42:20 EEST	2007-07-25 23:20:29 EEST	2007-07-25 23:20:29 EEST	41655	Allocated	Allocated	unknown	/img
jp[2].swf			1	2007-07-25 23:22:48 EEST	2007-07-25 23:42:20 EEST	2007-07-25 23:22:48 EEST	2007-07-25 23:22:48 EEST	41655	Allocated	Allocated	unknown	/img
NAP_UNLsigns_120x90L1_10k_US1[1].swf			0	2007-07-25 20:51:59 EEST	2007-07-25 23:42:23 EEST	2007-07-25 20:51:59 EEST	2007-07-25 20:51:59 EEST	7311	Allocated	Allocated	unknown	/img
RipaPhone_300_med[1].flv			0	2007-07-25 22:05:57 EEST	2007-07-25 23:42:24 EEST	2007-07-25 22:05:57 EEST	2007-07-25 22:05:56 EEST	751824	Allocated	Allocated	unknown	/img
tell_me[1].swf				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
CA67KFPQ.swf				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

CA8HALNO.swf

Audio

Table | Thumbnail | Summary

5 Results

Save Table as CSV

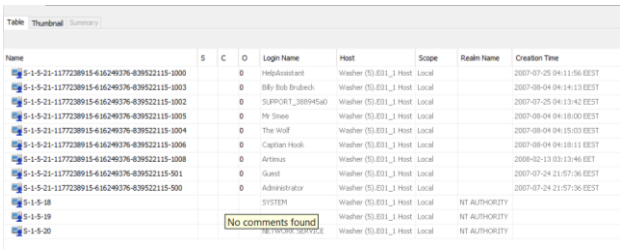
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
ygm[1].wav			0	2007-07-25 20:51:30 EEST	2007-07-25 23:41:33 EEST	2007-07-25 20:51:30 EEST	2007-07-25 20:51:30 EEST	9946	Allocated	Allocated	unknown	/img_Washer (5).E01/vol_vol2/Documents and S
sndrec.wav			2	2001-08-23 15:00:00 EEST	2007-08-04 04:22:44 EEST	2007-08-04 04:18:23 EEST	2007-08-04 04:18:23 EEST	58	Allocated	Allocated	unknown	/img_Washer (5).E01/vol_vol2/Documents and S
sndrec.wav			2	2001-08-23 15:00:00 EEST	2007-08-04 04:22:57 EEST	2007-08-04 04:19:14 EEST	2007-08-04 04:19:14 EEST	58	Allocated	Allocated	unknown	/img_Washer (5).E01/vol_vol2/Documents and S
sndrec.wav			2	2001-08-23 15:00:00 EEST	2007-08-04 04:23:29 EEST	2007-08-04 04:19:30 EEST	2007-08-04 04:19:30 EEST	58	Allocated	Allocated	unknown	/img_Washer (5).E01/vol_vol2/Documents and S
sndrec.wav			2	2001-08-23 15:00:00 EEST	2007-08-04 04:23:13 EEST	2007-08-04 04:19:44 EEST	2007-08-04 04:19:44 EEST	58	Allocated	Allocated	unknown	/img_Washer (5).E01/vol_vol2/Documents and S

Documents

Table | Thumbnail | Summary

File Type	File Extensions
HTML (246)	.htm, .html
Office (27)	.doc, .docx, .odt, .xls, .xlsx, .ppt, .pptx
PDF (1)	.pdf
Plain Text (106)	.txt
Rich Text (2)	.rtf

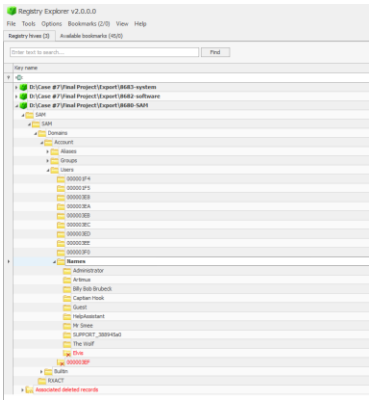
5. Users information



Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-1177238915-616249376-839522115-1000			0	HelpAssistant	Washer (5).E01_1 Host	Local		2007-07-25 04:11:56 EEST
S-1-5-21-1177238915-616249376-839522115-1003			0	Billy Bob Brubeck	Washer (5).E01_1 Host	Local		2007-08-04 04:14:13 EEST
S-1-5-21-1177238915-616249376-839522115-1002			0	SUPPORT_388945a0	Washer (5).E01_1 Host	Local		2007-07-25 04:13:42 EEST
S-1-5-21-1177238915-616249376-839522115-1005			0	Mr Sneee	Washer (5).E01_1 Host	Local		2007-08-04 04:18:00 EEST
S-1-5-21-1177238915-616249376-839522115-1004			0	The Wolf	Washer (5).E01_1 Host	Local		2007-08-04 04:15:03 EEST
S-1-5-21-1177238915-616249376-839522115-1006			0	Captian Hook	Washer (5).E01_1 Host	Local		2007-08-04 04:18:11 EEST
S-1-5-21-1177238915-616249376-839522115-1008			0	Artimus	Washer (5).E01_1 Host	Local		2008-02-13 03:13:46 EET
S-1-5-21-1177238915-616249376-839522115-501			0	Guest	Washer (5).E01_1 Host	Local		2007-07-24 21:57:36 EEST
S-1-5-21-1177238915-616249376-839522115-500			0	Administrator	Washer (5).E01_1 Host	Local		2007-07-24 21:57:36 EEST
S-1-5-18				SYSTEM	Washer (5).E01_1 Host	Local	NT AUTHORITY	
S-1-5-19					Washer (5).E01_1 Host	Local	NT AUTHORITY	
S-1-5-20					Washer (5).E01_1 Host	Local	NT AUTHORITY	

No comments found

Deleted User: Elvis



6. Devices Attached:

Listing

USB Device Attached

Table | Thumbnail | Summary

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
system			0	2008-03-10 10:11:21 EET		ROOT_HUB	4&22481edd&0	Washer (5).E01
system			0	2008-03-10 10:11:25 EET		ROOT_HUB	4&28ea0b8a&0	Washer (5).E01
system			0	2008-03-10 10:11:25 EET		ROOT_HUB	4&30f8eea4&0	Washer (5).E01
system			0	2008-03-10 10:11:25 EET		ROOT_HUB	4&31714c48&0	Washer (5).E01
system			0	2008-02-13 07:33:30 EET	Silicon Integrated Systems Corp.	Super Flash 1GB / GXT 64MB Flash Drive	0000000000C9BA	Washer (5).E01
system			0	2008-02-13 04:16:24 EET	Apple, Inc.	iPod Video	000A270014B302AB	Washer (5).E01
system			0	2008-02-13 07:22:08 EET	SanDisk Corp.	SDCZ2 Cruzer Mini Flash Drive (thin)	20041101101b4bc0091b	Washer (5).E01
system			0	2008-03-10 10:39:49 EET	SanDisk Corp.	SDCZ2 Cruzer Mini Flash Drive (thin)	20043512300C4E62C465	Washer (5).E01
system			0	2007-07-25 21:22:29 EEST	SanDisk Corp.	SDCZ2 Cruzer Mini Flash Drive (thin)	20043513310C7A22D0C8	Washer (5).E01
system			0	2008-03-10 10:07:30 EET	Trek Technology (S) PTE, Ltd	Product: 9005	10120515511949	Washer (5).E01
system			0	2008-03-10 10:11:22 EET	Linksys	WUSB54G v4 802.11g Adapter [Ralink RT2500USB]	5&2013f42e&0&2	Washer (5).E01

7. Encrypted Files:

Encryption Detected

Table | Thumbnail | Summary

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment
X marks the spot.doc			0	File	Notable			Password protection detected.	Password protection detected.
ALLSTATE CREDIT AGENCY.pdf			0	File	Notable			Password protection detected.	Password protection detected.
How To Steal Credit Numbers.doc			0	File	Notable			Password protection detected.	Password protection detected.
SLIST.doc			0	File	Notable			Password protection detected.	Password protection detected.

Online Behavior

Web Search

Term: credit card printer
Time: 2007-08-02 20:05:39 EEST
Domain: tele-pak.com
Program Name: Internet Explorer Analyzer

Source

Host: Washer (5).E01_1 Host
Data Source: Washer (5).E01
File: /img_Washer (5).E01/vol_vol2/Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/index.dat

Message0004

Subject:	**Re: New Venture**
From:	"John Washer" <chkwasher@comcast.net>
Date:	Wed, 11 Jul 2007 14:27:15 -0600
To:	"Wes Mantooth" <dollarhyde86@comcast.net>, "Mr Smee" <smee.rox@gmail.com>

Message Body

Sweet!

If that turns out to be too risky, a budy of mine showed me how to rig the machines to keep the cards... Then we shoulder surf the pin and get the card when they leave!

Message0020

Subject:	**I may have what you want.**
From:	"Rasco Badguy" <txkidd@swbell.net>
Date:	Wed, 1 Aug 2007 12:40:54 -0500
To:	<chkwasher@comcast.net>

Message Body

Skimmerman just called me to see if I had access to a card printer. Here is a photo of the one I have. It makes great licenses and ID cards. I just so happen to have 2 of these. You want one?

Message0018	
Subject:	**Re: Me and my woman**
From:	"John Washer" <chkwasher@comcast.net>
Date:	Thu, 2 Aug 2007 14:13:27 -0600
To:	"David Thomas" <skimmerman27@hotmail.com>

Message Body

Cool Man!

I scored this tech brief on debit card printing. I am working a new source for printers and mag writers...

Do you have any good sources for those?

Executive Summary:

In the course of the digital forensics investigation into the Washer case, we utilized two powerful tools, Autopsy and Registry Explorer, to analyze the digital evidence retrieved from the Washer.E01 image. The investigation focused on crucial aspects, including the time zone, operating system information, installed programs, documents and media, users' information, and emails.

Findings:

Time Zone: Through in-depth analysis, we determined the time zone settings of the seized hard drive, providing valuable insights into the geographical location and potential patterns of activity.

Operating System Information: Detailed information about the operating system allowed us to understand the system's configuration, which played a significant role in the investigation.

Installed Programs: We identified and documented the list of installed programs, shedding light on the tools and applications available to the user.

Documents and Media: Our investigation uncovered a wealth of documents and media files, offering potential evidence related to the case.

Users' Information: By examining user profiles, we gained critical information about the individuals involved in the activities under scrutiny.

Emails: The examination of emails led to significant discoveries related to the case, exposing communication patterns and potential connections.

Investigation Summary:

The investigation has yielded substantial evidence implicating John Washer in illegal activities. The digital evidence uncovered has linked him to the production of counterfeit credit cards. Through meticulous analysis of the retrieved data, we have identified communication with an associate known as "Rasco," revealing their involvement in the illicit activities.

Additional Insights:

One of the key findings from the investigation is the mode of communication utilized by John Washer with his associates. AOL instant messaging was identified as a prominent platform for communication, adding a critical layer of information to the case.

Associate: "Rasco"

In the course of our investigation, we managed to establish the identity of one of John Washer's associates, known by the name "Rasco." This individual's connection to the case suggests their involvement in the criminal activities under investigation.

Vehicle Identification:

Through our comprehensive analysis of media files, we were able to identify photos of "Rasco's" vehicle, providing potential leads for further investigation.

Conclusion

The digital forensics investigation into the Washer case, leveraging the potent capabilities of Autopsy and FTK, has led to a comprehensive and significant conclusion. Through the systematic analysis of critical digital evidence, including time zone details, operating system information, installed programs, documents and media, users' information, and emails, a compelling narrative has emerged, pointing to the involvement of John Washer in illegal activities related to the production of counterfeit credit cards.

Our analysis of the time zone settings provided valuable geographical insights, contributing to the reconstruction of events and potential locations of activity. Detailed documentation of the operating system information allowed us to grasp the system's configuration, providing crucial context for understanding the case.

The inventory of installed programs unveiled the tools and applications at the user's disposal, shedding light on their potential involvement in illicit activities. The plethora of documents and media files recovered during the investigation proved to be a vital source of potential evidence, adding depth to the investigation.

Meticulously examining user profiles allowed us to identify the individuals implicated in the activities under scrutiny, strengthening the case against John Washer. The examination of emails served as a pivotal element in unearthing critical evidence, establishing communication patterns and connections with associates, particularly with "Rasco."

Our investigation conclusively implicates John Washer in the production of counterfeit credit cards. The digital trails left behind provide irrefutable evidence of his active participation in these illicit activities. The discovery of "Rasco's" identity and insights into their vehicle further enrich the investigation, presenting potential leads for deeper probes into their involvement.

An intriguing aspect uncovered in our analysis is the use of AOL instant messaging as a primary communication platform among the individuals involved, offering critical insights into their modus operandi and communication dynamics.

The adherence to standard operating procedures (SOPs) throughout the investigation ensured the integrity and admissibility of the digital evidence, fortifying the reliability of our findings and conclusions.

Recommendations

Decrypt Encrypted Files:

One of the critical areas for further investigation is the decryption of any encrypted files or data encountered during the examination. Encrypted files may contain valuable information relevant to the case, and deciphering them could unveil additional evidence or shed light on the extent of John Washer's involvement in the production of counterfeit credit cards. Utilizing specialized decryption tools and techniques, the investigation team should prioritize the decryption process to uncover hidden details that could be crucial for a comprehensive understanding of the criminal activities.

Financial Transactions Analysis:

A comprehensive analysis of financial transactions, including bank records, online payment platforms, and credit card usage, is crucial to tracing the flow of funds and identifying potential money laundering activities associated with the criminal enterprise. Such analysis could provide vital clues linking financial transactions to the production and distribution of counterfeit credit cards. Utilizing specialized financial investigation tools and collaboration with financial institutions may aid in identifying suspicious transactions and uncovering the financial infrastructure of the operation.

Forensic Mobile Device Analysis:

Incorporating the examination of mobile devices linked to the suspects can offer essential insights into their activities beyond the confines of the computer systems. Forensic mobile device analysis may reveal conversations, location data, and call logs that could be instrumental in corroborating existing evidence and identifying additional associates or accomplices. This step can significantly enhance the investigation's depth and scope, providing a more comprehensive picture of the individuals' involvement and connections.

By implementing these recommendations, the digital forensics investigation can further its depth and breadth, uncovering additional evidence and potential associations crucial to building a strong case against the individuals involved in the production of counterfeit credit cards. The pursuit of decryption, in-depth communication analysis, financial transactions scrutiny, mobile device examination, collaborative efforts, and expert testimony preparation will

collectively contribute to a robust investigation and strengthen the chances of a successful prosecution, delivering justice and deterring future criminal activities.