Chapter 1, Getting Started with Computer Forensics Using FTK

Software	
Operation System	Server 2008 R2 / Windows7 (64-bit)
Hardware	
Processor	Intel® i7, Dual Quad Core Xeon, or AMD equivalent
Memory	32 GB (or more)
OS / Application drive	7200 RPM drive with 64MB cache or SSD drive
Storage for PostgreSQL database	160GB Solid State Drive (SSD) dedicated exclusively to PostgreSQL.
Network Card	Gigabit
HW RAID Controller	Highly recommended if hosting PostgreSQL database. Configure with RAID 5, 6, or 10 avoid RAID0
Temporary Folder Location	SSD drive or RAID0 partition w/ write-through
Drive Configuration	Drive 1: OS Drive 2: PostgreSQL Database (SSD or HW RAID) Drive 3: Case Folder and HD Image Drive 4: Temp Directory (SSD or RAID0)



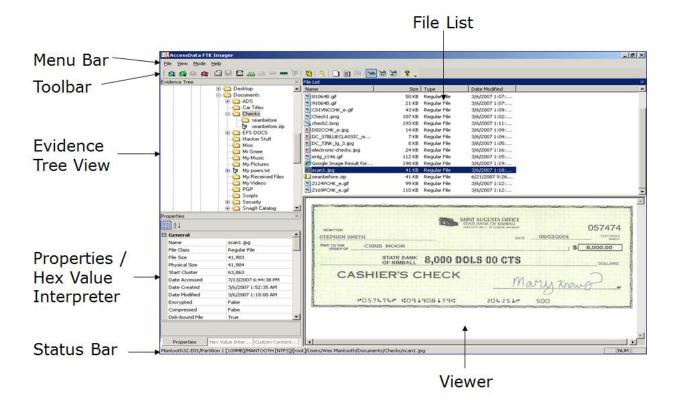
🚾 AccessData Fo	rensic Toolkit Version: 5.0.1.39			
File Database	Case Tools Manage Help			
Cases				
Name	Date Modified		Case ID	n/a
		(Case Owner	n/a
		F	Reference	n/a
			Date Modified	n/a
		(Da Add New User	
		0 [[Da Ca Trusted Us Full Name: De Full Name: Password: Password: Verify Password: Role(s): Application Adminis Assign Roles.	istrator

Chapter 2, Working with FTK Imager

ETABLE/		
eSATA Forensic	Bridge	
DC IN		
* ° * 800		
		SAT.
* * 800		
** 400	Power	
400	IDE Detect	
USB 2.0	SATA Detect	
	Host Detect	
	Write Block	
esata	Activity	
		- 80

All Files (*.*)

E01 Images (*.e01) SMART Images (*.s01) Advanced Forensic Format Images (*.aff) Virtual Hard Disk (*.vhd) ICS Images (*.101) SafeBack / SnapBack Images (*.001) Tar Archive (*.tar) Zip Archive (*.zip) AccessData Logical Image (*.AD1) VMDK Virtual Drive (*.vmdk) Ghost Raw Image (*.gho) Raw CD/DVD image (*.iso; *.img; *.bin; *.tao; *.dao) Alcohol CD image (*.mds) DiscJuggler image (*.cdi) CloneCD image (*.ccd) Gear CD Image (*.p01) IsoBuster CD image (*.cue) Nero CD image (*.nrg) Philips/OptImage CD image (*.cd) Pinnacle CD image (*.pdi) Plextools CD image (*.pxi) Prassi CD Right Image Plus (*.gcd) Prassi PrimoDVD Image (*.gi) Roxio CD Creator Image (*.cif) Virtual CD image (*.vc4) WinOnCD image (*.c2d) Apple Disk Images (*.dmg)



- 😭 Add Evidence Item
- Add All Attached Devices
- Image Mounting
- Remove Evidence Item
- a Remove All Evidence Items
- Create Disk Image
- Export Disk Image
- Export Logical Image (AD1)
- Add to Custom Content Image (AD1)
- Create Custom Content Image (AD1)
- Verify Drive/Image
- Capture Memory
- Dotain Protected Files
- Q Detect EFS Encryption
- Export Files
- Export File Hash List
- Export Directory Listing
- 🌤 Choose IE, text, or hex viewer automatically
- Here in plain text
- New files in hex format
- Open FTK Imager User Guide

AccessData FTK Imager 3.1.1.8		Address Address	
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp			
🔒 🙀 🗣 🛳 🚖 🔂 🖬 🛱 🚛 프 🗉		* 👬 📆 🦿	
Evidence Tree	× File List		×
	Name	Size Type Date M	odified
	Select Source	X	
	Please Select the Source Ev	Idence Type	
	Physical Drive		
	C Logical Drive		
	C Image File		
	C Contents of a Folder		
	(logical file-level analy	sis only; excludes deleted, unallocated, etc.)	
Hex Value Interpreter			
Type Size Value			
signed integer 1-8 unsigned integer 1-8			
FILETIME (UTC) 8 FILETIME (local) 8			
DOS date 2			
DOS time 2 time_t (UTC) 4	< Back	Next > Cancel Help	
time_t (local) 4			
<	•		
Byte order:	dian		
Properties Hex Value Int Custom C	onte		
For User Guide, press F1			
Q AccessData FTK Imager 3.1.1.8			
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp			
🔒 🎎 🗣 🛳 🛳 🖂 🖬 🖬 🗛 🗛 🕸	🔁 🔍 🗋 🖬 🔤	• सेसे सेहे 💡 🖕	
Evidence Tree	× File List		×
	Name	Size Type Date M	odified
	Select Drive	~	
	Source Drive Selection		
	Please select from the follo	wing available drives:	
		ITACHI HTS725050A7E630 [500GB I	
	\\.\PHYSICALDRIVE0 - H	ITACHI HTS725050A7E630 [500GB IDE]	
		ingston DataTraveler 2.0 USB Device [8G]	
Hex Value Interpreter			
Type Size Value			
signed integer 1-8 unsigned integer 1-8			
FILETIME (UTC) 8 FILETIME (local) 8			
DOS date 2			
DOS time 2 time_t (UTC) 4	< Back	Finish Cancel Help	
time_t (local) 4			
	• • •		
Byte order: • Little endian C Big end	lian		
Properties Hex Value Int Custom C	onte		

Q AccessData FTK Imager 3.1.1.8	
<u>File View M</u> ode <u>H</u> elp	
🛯 🏩 🏩 😂 🚘 🖾 🖶 🔚 🗮 🚑 💷 🚥 🚥	🔋 🍕 🗋 🗎 📾 🐱 📽 🍷 🖕
Evidence Tree	File List ×
□ 🔄 \\.\PHYSICALDRIVE0	Name Size Type Date Modified
Partition 1 [476938MB]	Unallocated space] 0 Unallocated Sp
⊡"t≇ System [NTFS]	MBR 1 Filesystem Met
□ [root] □ SBadClus	
E SExtend	1
🗄 🛅 \$Recycle.Bin	
te \$Secure	
🗄 🧰 ACL Data	
AssuranceHelp	
⊡ Auranool	
Custom	
Documents and Settings	
Hex Value Interpreter	
Type Size Value	
signed integer 1-8	
unsigned integer 1-8 FILETIME (UTC) 8	000 FA EB 23 53 61 66 65 42-6F 6F 74 20 00 06 01 00 úë#SafeBoot ····
FILETIME (local) 8	010 00 00 00 00 18 2A D8 01-00 00 00 02 CC 59 00 ·····*Ø······ÌY· 020 00 00 00 00 00 00 9C 0E-68 00 7C 60 1E 06 0E 1F ·······h· `····
DOS date 2 DOS time 2	030 0E 07 FC BB AE 7D B9 04−00 8D 5F 10 80 3F 80 E0 ···ix∞9}*····??·à
DOStime 2 time t (UTC) 4	040 F8 75 62 80 7F 04 12 75-SC BE 5E 7C BF 00 06 57 gub ····u*[]; ···W
time_t (local) 4	050 B9 09 00 F3 A4 8B 17 8B-4F 02 BB 00 7C C3 B8 01 ¹ · · 6¤ · · · O·≫ · Ã, ·
	060 02 CD 13 07 1F 61 CF 8A-C4 80 E4 0F 80 FC 09 7E ·í···aï·Ä·ä··ü·~ 070 03 80 C4 27 B1 04 D2 E8-3C 09 7E 02 04 27 01 06 ··Ä'±·Òè<·~··'··
	070 03 80 C4 27 B1 04 D2 E8-3C 09 7E 02 04 27 01 06 ··A*±·Oe<·~··· 080 9B 7D AC 0A C0 75 06 AC-98 03 F0 EB F5 79 06 4E ·}¬.Åu·¬··δēŏy·N
Byte order: 💽 Little endian 🔿 Big endian	090 C6 04 20 F6 D8 B4 0E BB-07 00 CD 10 EB E4 B4 92 E· öØ'·»··Í·ëä'·
Properties Hex Value Int Custom Conte	Cursor pos = 0; phy sec = 0
\\.\PHYSICALDRIVE0/Unpartitioned Space [basic dis]/MBR

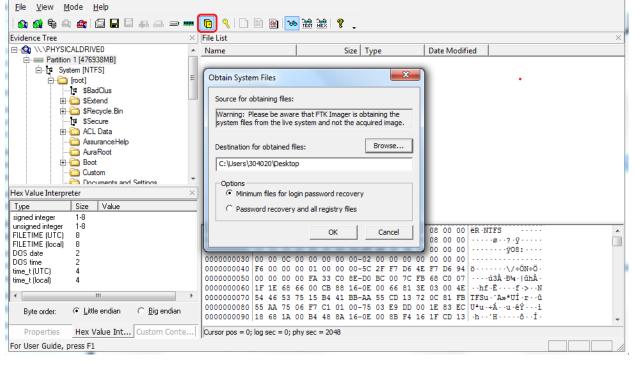
AccessData FTK Imager 3.1.1.8 File View Mode Help	
□-ŵ \\.\PHYSICALDRIVE0	Size Type Date Modified
Create Image	23
	Select Image Type
Partition 1 [476938MB]	Please Select the Destination Image Type
Starting Evidence Number: 0 Image Destination(s)	C Raw (dd) C SMART C E01 C AFF
unsigned Add Edit Remove FILETIM Verify images after they are created Precalculate Progress Statistics DOS time Create directory listings of all files in the image after they are created Image after they are created U time_t (lo Start Cancel	< Back Next > Cancel Help
	6 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC U ² u→Á··u→ÉÝ···Ì 0 B4 48 8A 16-0E 00 8B F4 16 1F CD 13 ·h··'H····ô··Í·
Properties Hex Value Int Custom Conte Cursor pos = 0; log sec = 0; ph	y sec = 2048
For User Guide, press F1	

Evidence Item Infor	mation X
Case Number:	
Evidence Number	· .
Unique Descriptio	n:
Examiner:	
Notes:	
	< Back Next > Cancel Help

Select Image Destination
Image Destination Folder
C:\Users\304020\Desktop Browse
Image Filename (Excluding Extension)
evidence
Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment 1500
Compression (0=None, 1=Fastest,, 9=Smallest) 6
Use AD Encryption
< Back Finish Cancel Help

	ve						
dd Image							
Image File:							
_)\Desktop\Mantooth.E01						
] ((
Mount Type: Physical & Logical							
Drive Letter:	Next Available (H:)	•	-				
	Block Device / Read Only						
	Iblock Device / Read Only	·					
Write Cache Fol	der:						
C:\Users\30402	0\Desktop						
] ((
			Mount				
Anned Image Lis	+						
Napped Image Lis	t						
1apped Image Lis Mapped Images:	t						
	t Method	Partition	Image				
Mapped Images: Drive PhysicalDrive2	Method Block Device/Read	Image	C:\Users\304020\Desktop\Mantooth.E01				
Mapped Images: Drive PhysicalDrive2 F:	Method Block Device/Read Block Device/Read	Image Partition 1 [109M	C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01				
Mapped Images: Drive PhysicalDrive2	Method Block Device/Read	Image	C:\Users\304020\Desktop\Mantooth.E01				
Mapped Images: Drive PhysicalDrive2 F:	Method Block Device/Read Block Device/Read	Image Partition 1 [109M	C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01				
Mapped Images: Drive PhysicalDrive2 F:	Method Block Device/Read Block Device/Read	Image Partition 1 [109M	C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01				
Mapped Images: Drive PhysicalDrive2 F:	Method Block Device/Read Block Device/Read	Image Partition 1 [109M	C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01				
Mapped Images: Drive PhysicalDrive2 F:	Method Block Device/Read Block Device/Read	Image Partition 1 [109M Partition 2 [7MB]	C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01				
Mapped Images: Drive PhysicalDrive2 F:	Method Block Device/Read Block Device/Read	Image Partition 1 [109M	C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01				
Mapped Images: Drive PhysicalDrive2 F:	Method Block Device/Read Block Device/Read	Image Partition 1 [109M Partition 2 [7MB]	C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01				
Mapped Images: Drive PhysicalDrive2 F:	Method Block Device/Read Block Device/Read	Image Partition 1 [109M Partition 2 [7MB]	C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01				
Mapped Images: Drive PhysicalDrive2 F:	Method Block Device/Read Block Device/Read	Image Partition 1 [109M Partition 2 [7MB]	C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01 C:\Users\304020\Desktop\Mantooth.E01				

🔍 AccessData FTK Imager 3.1.1.8			hallo ha	Box which	
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp					
🛯 🏩 🎕 🎕 🚘 🗇 🖬 🖬 🚑 🛲 💻 🚃	🔁 🥄 🗋 🗎 🖬 🐱	रेट्रेने मेटेरे 💡 🖕			
Evidence Tree	File List				×
	Name	Size T	ype	Date Modified	
Partition 1 [476938MB]					
⊡ r System [NTFS]				D	
⊡ froot] □ 1 sBadClus	Memory Capture		×		
Er • € States and	Destination path:				
🕀 🗀 \$Recycle.Bin	C:\Users\304020\Desktor		Browse		
\$Secure	C: Users (304020 (Deskto)	P	browse		
🕀 🧰 ACL Data	Destination filename:				
	memdump.mem				
	I				
Custom	Include pagefile				
Documents and Settings	pagefile.sys				
Hex Value Interpreter ×	pagemenaya				
Type Size Value	Create AD1 file				
signed integer 1-8	memcapture.ad1				
unsigned integer 1-8 FILETIME (UTC) 8	1			08 00 00 ëR·NTFS ····	
FILETIME (OTC) 8	Capture Memory	Cancel		D8 00 00 ····ø··?·ÿ···	
DOS date 2				00 00 00 ······ÿ08:··	
DOS time 2	0000000040 F6 00 00	00 01 00 00 00-50	C 2E E7 D6 4E	00 00 00 ·······//+ÖN+0	 ö.
time_t (UTC) 4 time_t (local) 4				68 C0 07 ····ú3À·Đ¾· ûhi	
				03 00 4E · · hf · Ë · · · · f · > ·	
۰				OC 81 FB TFSu·'A»*UÍ·r·	
Byte order: 📀 Little endian 🔿 Big endian				1E 83 EC U ^a u·÷Á··u·éÝ··	
	0000000090 18 68 1A	00 B4 48 8A 16-0B	E 00 8B F4 16	1F CD 13 . h · · · H · · · · ô · ·	I · •
Properties Hex Value Int Custom Conte	Cursor pos = 0; log sec = 0; p	ohy sec = 2048			
For User Guide, press F1					



Q AccessData FTK Imager 3.1.1.8

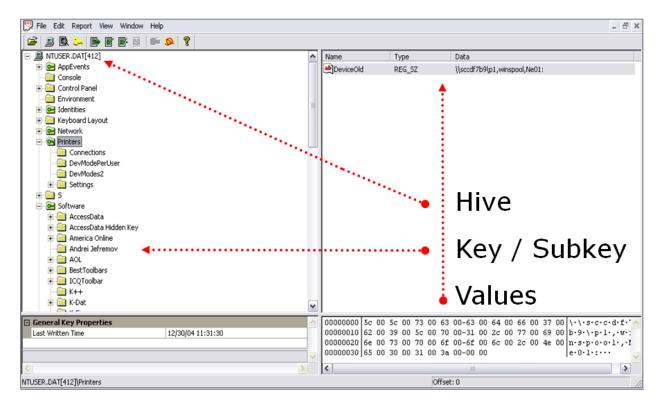
Q AccessData FTK Imager 3.1.1.8	Addir Addir Addir Addir Addir	
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp		
🔒 🏩 🎭 🛳 🚖 🖾 🖬 🖬 🛃 🚙 💷 🚥	🖪 🕙 🗋 🔤 😹 盤 🔋 🧅	
Evidence Tree >	File List	×
□··· 😫 \\.\PHYSICALDRIVE0	Name Size Type Date Modified	
Partition 1 [476938MB]	Extend 1 Directory 07/06/2013 22:	
⊡…[System [NTFS]	SRecycle.Bin 1 Directory 13/06/2013 18:	E
in [root] □ \$BadClus	ACL Data 1 Directory 07/06/2013 18:	
⊡us ⊡⊡ \$Extend	AssuranceHelp 1 Reparse Point 07/06/2013 18:	
	AuraRoot 1 Renarse Point 07/06/2013 18:	
T \$Secure	Detect Encryption Progress Dry 07/06/2013 23:	
ACL Data	pry 13/06/2013 18:	
	Please wait while FTK Imager scans the evidence in Point 14/07/2009 05:	
🛅 AuraRoot	to detect encryption. Depending on the size of the evidence, this may take several minutes.	
🕀 💼 Boot	pry 17/10/2012 01:	
Custom	pry 07/06/2013 19:	
Documents and Settings	pry 16/10/2012 22:	
Hex Value Interpreter >	Cancel pry 23/08/2013 18:	
Type Size Value	pry 14/07/2009 03:	
signed integer 1-8	bry 13/12/2013 13:	*
unsigned integer 1-8 FILETIME (UTC) 8	000 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0	A
FILETIME (local) 8	010 10 00 00 00 98 01 00 00-98 01 00 00 01 00 00 00	
DOS date 2	020 BF 54 00 00 00 00 01 00-88 00 6E 00 01 00 00 00 ¿T······n···· 030 05 00 00 00 00 00 05 00-F2 90 72 30 41 04 CA 01 ·······ò·r0A·Ê·	=
DOS time 2	040 F2 90 72 30 41 04 CA 01-BF C9 9F DD B2 63 CE 01 ò·r0A·Ê·;É·ý*cη	
time_t (UTC) 4 time_t (local) 4	050 F2 90 72 30 41 04 CA 01-00 00 00 00 00 00 00 00 00 0 0 0 01 0 10 0 0	
	060 00 00 00 00 00 00 00 00-06 24 00 10 03 00 00 A0 ·······\$·····	
< •	070 16 01 44 00 6F 00 63 00-75 00 6D 00 65 00 6E 00 ··D·o·c·u·m·e·n·	
Byte order: 💽 Little endian 🔿 Big endian	080 74 00 73 00 20 00 61 00-6E 00 64 00 20 00 53 00 t·s· ·a·n·d· ·S· 090 65 00 74 00 74 00 69 00-6E 00 67 00 73 00 CD 01 e·t·t·i·n·g·s·Í·	-
Properties Hex Value Int Custom Conte	Cursor pos = 0	
For User Guide, press F1		

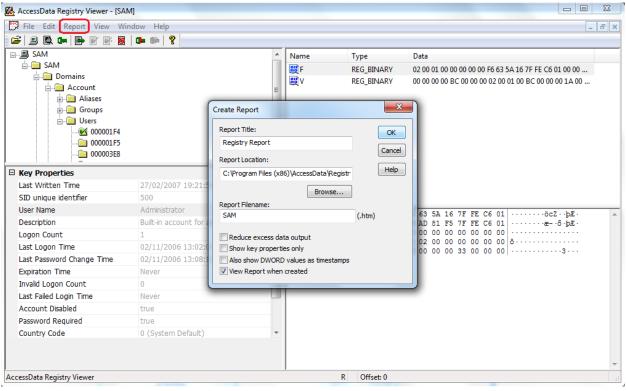
Chapter 3, Working with Registry View

			6 h f	
System (C:) ▶ Windows ▶ System32 ▶ config ▶	▼ € ₂	Search config	
Organize 🔻 Include in	· · · · · · · · · · · · · · · · · · ·	New folder		iii 🔹 🗔 🔞
🔆 Favorites	Name	Date modified	Туре	Size
🧾 Desktop	퉬 Journal	13/07/2009 23:34	File folder	
鷆 Downloads	\mu RegBack	31/10/2013 11:50	File folder	
🖳 Recent Places	퉬 systemprofile	13/06/2013 15:14	File folder	
	\mu TxR	16/10/2012 21:12	File folder	
🤭 Libraries	BCD-Template	07/06/2013 20:03	File	28 KB
Documents		15/12/2013 19:41	File	43.008 KB
🌙 Music	DEFAULT	15/12/2013 17:30	File	512 KB
📔 Pictures	a netlogon.ftl	15/12/2013 21:49	FTL File	1 KB
📑 Videos	SAM	13/12/2013 11:41	File	256 KB
	SECURITY	13/12/2013 18:51	File	256 KB
👰 Computer	SOFTWARE	15/12/2013 22:03	File	88.320 KB
🏭 System (C:)		15/12/2013 22:02	File	19.968 KB
ENDRIVE (E:)				
🕎 VOL1\$ (\\BR-SAOFIL				
CODEMETER (G:)				
🕎 304020\$ (\\BR-SAOF				
👽 Network				
12 items				

Name Date modified Type Size Image: Desktop Image: Oracle 17/11/2013 22:22 File folder Image: Downloads Image: Oracle 13/06/2013 15:14 File folder Image: Downloads Image: Oracle Image: Oracle Image: Oracle Image: Downloads Image: Oracle Image: Oracle Image: Oracle Image: Downloads Image: Oracle Image: Oracle Image: Oracle Image: Oracle Image: Downloads Image: Oracle Ima	Computer	System (C:) Users June 20 System (C:)	- - - + - - - + - - - - - - - - - -	Search 304020)
★ FavoritesNameDate modifiedTypeSize■ Desktop● Oracle17/11/2013 22:22File folder● Downloads● PrintHood13/06/2013 15:14File folder● Recent Places● Recent13/06/2013 15:14File folder● Saved Games13/06/2013 15:15File folder● Documents● Searches22/09/2013 22:09File folder● Nusic● Statt Menu13/06/2013 15:14File folder● Videos● Templates13/06/2013 15:14File folder● Videos● CmDust-Result.log12/12/2013 16:12Text Document● PENDRIVE (E)● Intuser.dat.LOG115/12/2013 22:07DAT File● VOL1S (\\BR-SAOFI● NTUSER.DAT15/12/2013 15:14BLF File● NTUSER.DAT[016888bd-6c6f-11de-8d1d13/06/2013 15:14BLF File64 KB● NTUSER.DAT[016888bd-6c6f-11de-8d1d13/06/2013 15:14REGTRANS-MS File512 KB	Organize 🔻 📄 Open	Burn New folder			•	?
 Downloads PrintHood I3/06/2013 15:14 File folder Recent I3/06/2013 15:14 File folder Saved Games I3/06/2013 15:15 File folder Saved Games I3/06/2013 15:15 File folder Saved Games I3/06/2013 15:14 File folder Searches Searches Searches Searches Searches Start Menu I3/06/2013 15:14 File folder Templates Templates IS/12/2013 16:12 Text Document St KB MTUSER.DAT IS/12/2013 22:07 LOG1 File Se KB NTUSER.DAT(016888bd-6c6f-11de-8d1d I3/06/2013 15:14 BLF File KB NTUSER.DAT(016888bd-6c6f-11de-8d1d I3/06/2013 15:14 REGTRANS-MS File S12 KB 		Name Nethood	10/00/2010 10:14	rile loider	Size	
□ Libraries □ Libraries □ Libraries □ Libraries □ Libraries □ Documents □ Music □ SendTo □ 3/06/2013 15:14 File folder □ Music □ Start Menu □ 3/06/2013 15:14 File folder □ Videos □ Templates □ 3/06/2013 15:14 File folder □ Videos □ CmDust-Result.log □ 2/12/2013 16:12 Text Document 116 KB □ NTUSER.DAT □ 15/12/2013 22:07 DAT File 4.096 KB □ NTUSER.DAT □ 15/12/2013 15:14 LOG2 File 0 KB □ CODEMETER (G:) □ NTUSER.DAT{016888bd-6c6f-11de-8d1d 13/06/2013 15:14 BLF File 64 KB □ NTUSER.DAT{016888bd-6c6f-11de-8d1d □ 3/06/2013 15:14 REGTRANS-MS File 512 KB			13/06/2013 15:14			
 Music Start Menu 13/06/2013 15:14 File folder Yideos CmDust-Result.log 12/12/2013 16:12 Text Document 116 KB ML Document S1 KB Computer System (C:) PENDRIVE (E:) NTUSER.DAT S1/12/2013 22:07 DAT File A.096 KB Intuser.dat.LOG1 S1/12/2013 22:07 LOG1 File 256 KB NTUSER.DAT(016888bd-6c6f-11de-8d1d 13/06/2013 15:14 BLF File KB NTUSER.DAT(016888bd-6c6f-11de-8d1d 13/06/2013 15:14 REGTRANS-MS File S12 KB 		Searches	22/09/2013 22:09	File folder		
Image: Computer Image: Computer	Pictures	Start Menu	13/06/2013 15:14	File folder		
System (C:) Intuser.dat.LOG1 15/12/2013 22:07 DAT File 4.090 KB PENDRIVE (E:) Intuser.dat.LOG2 13/06/2013 15:14 LOG2 File 0 KB VOL1S (\\BR-SAOFIL NTUSER.DAT{016888bd-6c6f-11de-8d1d 13/06/2013 15:14 BLF File 64 KB CODEMETER (G:) NTUSER.DAT{016888bd-6c6f-11de-8d1d 13/06/2013 15:14 BLF File 64 KB		🖹 install.xml	16/10/2012 19:39	XML Document	51 KB	
CODEMETER (G:) NTUSER.DAT{016888bd-6c6f-11de-8d1d 13/06/2013 15:14 REGTRANS-MS File 512 KB	System (C:)	ntuser.dat.LOG1	15/12/2013 22:07	LOG1 File	256 KB	
TUSER.DAT 016888bd-6c6f-11de-8d1d 13/06/2013 15:14 REGTRANS-MS File 512 KB		· ·				
Image: Network Image: Network 16/10/2012 18:16 Configuration sett 1 KB Image: Network Image: Network 13/12/2013 14:26 POL File 64 KB Image: Network 13/11/2013 21:00 Text Document 1 KB	🗣 Network	ntuser.ini	16/10/2012 18:16 13/12/2013 14:26	Configuration sett POL File	1 KB 64 KB	

🔀 AccessData Registry Viewer			
File View Help			
 ≥ 2 0 ≥ 2 € 3 	0- 0- ?		
	🔏 Open		
	O ♥ ↓ Registry Files	 ✓ 4 Search Registry Files 	
	Organize 🔻 New folder	8≡ - □ @	
	Documents Name	Date modified Type Size	
	Music	12/02/2008 18:13 File 256 KB	
	Videos		
	1톤 Computer 쫉 System (C:)		
	PENDRIVE (E:)		
	👽 VOL1S (\\BR-SAC		
	CODEMETER (G:) [■]		
	😴 304020\$ (\\BR-S4		
	100 C C C C C C C C C C C C C C C C C C		
	🗣 Network		
	-		
	File name: SAM	✓ All Files (*.*)	
		Open Cancel	
		Cancer	
AccessData Registry Viewer			di
AccessData Registry Viewer			





🔍 AccessData FI	TK Imager 3.1.1.8						
	Iode <u>H</u> elp						
🏔 🆓 🗣 🗠) 🔄 🖬 🖬 🗳 🚛 🛥 🤊						
Evidence Tree		×	File List				
	⊡ · 🛅 System32	*	Name	Size Ty	уре	Date Modified	
	⊕ • 🛅 Boot • • 🛅 catroot		퉬 Journal		irectory	02/11/2006 10:	
			📕 RegBack		irectory	07/07/2007 20:	
	GroupPolicy		TxR		irectory	02/11/2006 12:	
			SIB0 COMPONENTS.LOG		TFS Index All egular File	14/07/2007 18: 02/11/2006 10:	
	⊡ ⊡ LogFiles		DEFAULT.LOG		egular File	02/11/2006 15:	_
	Microsoft	-	DEFAULT.LOG1		egular File	12/07/2007 19:	=
	networklist	Ξ	DEFAULT.SAV		egular File	02/11/2006 10:	
			SAM		equilar File	1 2 /0 2 / 2008 20.	
	⊞ - 🛅 spool		SAM.LOG	Export Files			
	i∃…i⊇ winevt 	-	SAM.LOG1	Export File Has	h List		
Hex Value Interpre		×	SECURITY SECURITY.LOG	🕰 Add to Custom	n Content Imag	e (AD <u>1</u>)	
Туре	Size Value	_	SECURITY.LOG1	256 Re	egular File	12/07/2007 19:	
signed integer	1-8		SOFTWARE	22.272 Re	egular File	12/02/2008 20:	-
unsigned integer FILETIME (UTC)	1-8 8		00000 72 65 67 66 CE	00 00 00-CF 00 0	0 00 6B 03 5	4 B4 regfÏ···Ï···k·T′	A
FILETIME (local)	8					0 00 ³ mÈ	
DOS date	2					0 00 2 00 \.S.y.s.t.e.m.R.	
DOS time time t (UTC)	2					4 00 0.0.t.\.S.y.s.t.	
time_t (local)	4		00050 65 00 6D 00 33			E 00 e·m·3·2·∖·C·o·n·	
•	III	b.	00060 66 00 69 00 67			0 00 f·i·g·\·S·A·M···	
		,					
Byte order:	€ Little endian		00090 B8 1A 50 D5 00				-
Properties	Hex Value Int Custom Conte		Cursor pos = 0; dus = 21221	; log sec = 21221; phy se	ec = 21284		
Exports files from	n the image to a local folder						
-							

* Ac													
<u>F</u> ile	<u>E</u> dit	View	Evi <u>d</u> ence	e F <u>i</u> lter	<u>T</u> ools	<u>M</u> anage	<u>H</u> elp)					
-	F	ilter: -	unfiltered -				•	Filter Ma	anager	1			
Ex	plore	Overvie	w Email	Graphics	Video	Internet/	Chat	Bookmarks	Live Search	Index S	earch Volat	ile	
_	Evider	nce Item	c					4 0	File Content				
_	LVIGG	ice icem	∎ É						Hex Text	Filtered	Natural		
								^		Fillereu			
			_	system					63 🗗				
				System32									
				🛅 Boot									
				🛅 catroo	t								
				config									
				GroupF									
				GroupF		rs							
				Micros				_					
				DI NDF				=					
					klist			н					
				DF	klist			=					
				DF networ Speech	klist 1			=					
			00000	DF hetwor Speech pool	klist 1			E	File Conto	ent Pro	operties	Hex Interpre	eter
ile Lie	st		00000	NDF networ Speed spool winevt	klist 1				File Conte	ent Pro	operties	Hex Interpre	eter
				NDF networ Speed spool winevt	klist 1			•	File Contr		operties y Time Zone: 1		
£ (78	Name		NDF networ Speed spool winevt	klist 1			•	File Cont		y Time Zone: I		
5 - 5	<i> </i>	Name		NDF networ Speed Spool in winevt Tasks	klist	m# Ex		Normal Path	File Conto	Displa Catego	y Time Zone: I ry P-Size	E. South Amer	ica D
2 2 0	₽ <i> </i> ▲ \$130	Name		NDF networ Speed Spool in winevt Tasks	klist	m # Ex	t	Normal Path Mantooth		Displa Catego Index .	y Time Zone: I ry P-Size 4096 B	E. South Amer	ica D
2 2 0 0 0	₽ ₽ ▲ \$130 COM	Name		NDF networ Speed Spool in winevt Tasks	klist	m # Ex 13 14 log	t J	Normal Path Mantooth Mantooth	.E01/Partition .	Displa Catego Index . Unknov	ry Time Zone: I ry P-Size 4096 B vn 1024 B	E. South Amer L-Size 4096 B	ica D
	\$130 COM	Name) 1PONENTS		NDF networ Speed Spool in winevt Tasks	klist I Iter 191 191	m # Ex 13 14 log 15 log	t J	Normal Path Mantooth Mantooth Mantooth	.E01/Partition . .E01/Partition .	Displa Catego Index . Unknov Unknov	y Time Zone: I ry P-Size 4096 B vn 1024 B vn 1024 B	E. South Amer L-Size 4096 B 1024 B 1024 B	ica D
	\$130 COM DEF	Name) 1PONENTS AULT.LOG		NDF networ Speed Spool in winevt Tasks	klist I Iter 191 191 191	m # Ex 13 14 log 15 log 16 log	t 9 9 91	Normal Path Mantooth Mantooth Mantooth Mantooth	.E01/Partition . .E01/Partition . .E01/Partition .	Displa Catego Index . Unknov Unknov Unknov	y Time Zone: I ry P-Size 4096 B vn 1024 B vn 1024 B vn 256,0 KB	E. South Amer 4096 B 1024 B 1024 B 256,0 KB	ica D
	\$I30 COM DEF	Name IPONENTS AULT.LOG AULT.LOG AULT.SAV		NDF networ Speed Spool in winevt Tasks	klist I Iter 191 191 191 191	m # Ex 13 14 log 15 log 16 log 17 sa	t 9 9 91	Normal Path Mantooth Mantooth Mantooth Mantooth Mantooth	.E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition .	Displa Catego Index . Unknov Unknov Unknov Unknov	y Time Zone: I ry P-Size 4096 B vn 1024 B vn 1024 B vn 256,0 KB	E. South Amer 4096 B 1024 B 1024 B 256,0 KB	ica D
	Size Straight Straigh	Name) IPONENTS AULT.LOG AULT.SAV nal		NDF networ Speed Spool in winevt Tasks	klist I Iter 191 191 191 191 191	m # Ex 13 14 log 15 log 16 log 17 sa 28	t 9 9 91	Normal Path Mantooth Mantooth Mantooth Mantooth Mantooth	.E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition .	Displa Catego Catego Index . Unknow Unknow Unknow Unknow Unknow Folder	y Time Zone: I ry P-Size 4096 B vn 1024 B vn 1024 B vn 256,0 KB vn 20,00 KB	E. South Amer 4096 B 1024 B 1024 B 256,0 KB 20,00 KB	ica D
	SI30 SI30 COM DEF/ DEF/ Jour Regi	Name) 1PONENTS AULT.LOG AULT.SAV nal Back		NDF networ Speed Spool in winevt Tasks	klist I ter 191 191 191 191 191 192	m # Ex 13 14 log 15 log 16 log 17 sa 28 29	t 9 9 91	Normal Path Mantooth Mantooth Mantooth Mantooth Mantooth Mantooth	.E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition .	Displa Catego Catego Index . Unknow Unknow Unknow Unknow Folder Folder	y Time Zone: I ry P-Size 4096 B vn 1024 B vn 1024 B vn 256,0 KB vn 20,00 KB 48 B 48 B	E. South Amer 4096 B 1024 B 1024 B 256,0 KB 20,00 KB 48 B 48 B	ica D
	SAM	Name) 1PONENTS AULT.LOG AULT.SAV nal Back		NDF networ Speed Spool in winevt Tasks	klist 191 191 191 191 191 192 192	m # Ex 13 14 log 15 log 16 log 17 sa 28 29 18 <n< td=""><td>t J J J1 v</td><td>Normal Path Mantooth Mantooth Mantooth Mantooth Mantooth Mantooth Mantooth</td><td>.E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition .</td><td>Displa Catego Index . Unknow Unknow Unknow Unknow Folder Folder Folder</td><td>ry Time Zone: 1 ry P-Size 4096 B vn 1024 B vn 1024 B vn 256,0 KB vn 256,0 KB 48 B 48 B vn 256,0 KB</td><td>E. South Amer 4096 B 1024 B 1024 B 256,0 KB 20,00 KB 48 B 48 B</td><td>ica D</td></n<>	t J J J1 v	Normal Path Mantooth Mantooth Mantooth Mantooth Mantooth Mantooth Mantooth	.E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition . .E01/Partition .	Displa Catego Index . Unknow Unknow Unknow Unknow Folder Folder Folder	ry Time Zone: 1 ry P-Size 4096 B vn 1024 B vn 1024 B vn 256,0 KB vn 256,0 KB 48 B 48 B vn 256,0 KB	E. South Amer 4096 B 1024 B 1024 B 256,0 KB 20,00 KB 48 B 48 B	ica D
	\$I30 COM DEF DEF Jour Regi SAM SAM	Name IPONENTS AULT.LOG AULT.LOG AULT.SAV nal Back		NDF networ Speed Spool in winevt Tasks	klist 191 191 191 191 191 192 192 192	m # Ex 13 14 log 15 log 16 log 17 sa 28 29 18 <n 19 log</n 	t))1 v	Normal Path Mantooth Mantooth Mantooth Mantooth Mantooth Mantooth Mantooth	E01/Partition . E01/Partition . E01/Partition . E01/Partition . E01/Partition . E01/Partition . E01/Partition .	Displa Catego Catego Index . Unknov Unknov Unknov Folder Folder Unknov Unknov	ry Time Zone: 1 ry P-Size 4096 B vn 1024 B vn 1024 B vn 256,0 KB vn 256,0 KB vn 256,0 KB vn 256,0 KB vn 256,0 KB vn 1024 B	E. South Amer L-Size 4096 B 1024 B 1024 B 256,0 KB 256,0 KB 48 B 48 B 48 B 256,0 KB 1024 B	ica D
	SAM	Name) IPONENTS AULT.LOG AULT.SAV mal Back I.LOG		NDF networ Speed Spool in winevt Tasks	klist Iter 191 191 191 191 192 192 192 191	m # Ex 13 14 log 15 log 16 log 17 sa 28 29 18 <n 19 log 20 log</n 	t))1 v	Normal Path Mantooth Mantooth Mantooth Mantooth Mantooth Mantooth Mantooth Mantooth	E01/Partition . E01/Partition . E01/Partition . E01/Partition . E01/Partition . E01/Partition . E01/Partition .	Displa Catego Gatego Index . Unknow Unknow Unknow Unknow Unknow Folder Folder Unknow Unknow Unknow	y Time Zone: 1 ry P-Size 1024 B vn 1024 B vn 256,0 KB 48 B 48 B vn 256,0 KB vn 1024 B vn 256,0 KB vn 1024 B vn 256,0 KB	E. South Amer L-Size 4096 B 1024 B 1024 B 256,0 KB 48 B 48 B 256,0 KB 1024 B 1024 B 256,0 KB	ica D

Open Launch in Content Viewer Open With Create Bookmark Add to Bookmark	
Open With Create Bookmark Add to Bookmark	
Open With Create Bookmark Add to Bookmark	
Create Bookmark Add to Bookmark	_
Add to Bookmark	
	_
Remove from Bookmark	
Nemove nom bookmark	
Labels	
Review Labels	
Mount Image to Drive	
Add Decrypted File	
Perform Cerberus Analysis	
Visualize Browser History	
Export Browser History to CSV	
Export browser history to esvil.	_
View File Sectors	
Find on Disk	
Add to Fuzzy Hash Library ssed Modified	Ι
Find Similar Files 7/2008 18: 14/07/2007 15:	
Add to PhotoDNA Library 1/2006 07: 02/11/2006 07:	
1/2006 12: 02/11/2006 12:	
Open in Registry Viewer 7/2007 18: 12/07/2007 16:	
1/2006 07: 02/11/2006 07:	
Export 7/2008 18: 02/11/2006 07:	
Export to Image 7/2008 18: 07/07/2007 17:	
2/2008 18: 12/02/2008 18: Acquire to disk image 7/2007 18: 02/11/2006 07:	
Acquire to disk image 7/2007 18: 02/11/2006 07: Export File List Info 7/2007 18: 12/07/2007 16:	
7/2007 18: 12/07/2007 18:	
Copy Special 1/2006 07: 02/11/2006 07:	

Manage Evidence						X
Display Name	State	P	Path: C:V	lsers\304020\[Desktop\Mantooth.E01	
Mantooth.E01 Add Remove Case KFF Options	+	ID / Na Descrip Evidence Gr Time Z	oup: one: Ame Ame East Cent Cent Mour Pacit Pacit	ern Time witho ral Time with D ral Time withou ntain Time with ntain Time with ntain Time with Da		je
🛃 AccessData Registry Viewer - [SYSTEM] 💬 File Edit Report View Window	Help					• ×
Standard Start Date	6/03/2007 15:04:03 UTC irst dom in nov at 2:00:00 econd dom in mar at 2:01		Bias StandardNa StandardBias StandardStart DaylightName DaylightBias DaylightStart FimeZoneKe DynamicDay	REG_DWORD REG_BINARY REG_SZ REG_DWORD REG_BINARY	Data 0x000001A4 (420) @tzres.dll,-192 0x0000000 (0) 00 00 08 00 01 00 02 00 00 00 00 00 00 00 00 00 00 0xFFFFC4 (4294967236) 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00	
Standard Bias 0 Daylight Bias 4	50		4 01 00 00		¥	

🗧 📖 🗟 📭 📑 🗃 🖬						8
- 🛄 SAM		*	Name	Туре	Data	-
SAM			BE F	REG_BINARY	02 00 01 00 00 00 00 00 F6 63 5A 16 7F FE C6 01 00 00	
Domains Account Groups Users 000001F5 000001F5 00000188		ш	wer ₩V	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00	
Last Written Time	27/02/2007 19:21:54 UTC	-				
SID unique identifier	500					
User Name	Administrator					
Description	Built-in account for administering the	c	00 02 00 01	00 00 00 00 00	-F6 63 5A 16 7F FE C6 01öcZbE.	_
Logon Count	1				-E6 AD 81 F5 7F FE C6 01æõ.þÆ.	
Last Logon Time	02/11/2006 13:02:01 UTC				-00 00 00 00 00 00 00 00	
Last Password Change Time	02/11/2006 13:08:15 UTC	Ξ			-11 02 00 00 00 00 00 00 00 ô	
Expiration Time	Never		1			
Invalid Logon Count	0					
Last Failed Login Time	Never					
Account Disabled	true					
Password Required	true					
Country Code	0 (System Default)					
Hours Allowed	Anytime	Ŧ				
er Name is is the user name of the user	with this SID.					

Chapter 4, Working with FTK Forensics

Pre	eparation	Acquisition and Preservation	
_	ssData Forensic Toolkit Version: 5.0 atabase Case Tools Manage		
Cas	Log Out Change password Administer Users Session Management Configure	Case ID n/a Case Owner n/a Case Owner n/a Reference n/a Date Modified n/a Administer Users User Name Full Name Role(s) Itcarbone flcarbone Application Administrator	
		Create User Disable User Change Password Set Role(s) Show disabled users Close	

Administer Users	Partners at	-	23
User Name	Full Name	Role(s)	
flcarbone	ficarbone	Application Administrator	
	Add New User	×	
	Trusted Full Name:	User Name:	
	Password:		
	Verify Password	:	
Create User.			
Show disabled	users Assign Role	s OK Cancel	Close

Initial Role(s) for:		×
Roles:		
Name	Description	
Application Administrator	This role has all privileges.	
Case Administrator	This role has all case privileges.	
Case Reviewer	This role has review rights only, modification of the evidence data is not permit	ted
		OK Cancel
		UK Cancer
	Password:	
	Verify Password:	
	Role(s):	
Create User		
	Assign Roles OK Cancel	Close
Show disabled users		

Jser Name	Full Name Role(s)	
Icarbone	flcarbor Change Password Current password for flcarbone (flcarbone) New password Re-enter OK Cancel	
Create User.	Disable User Change Password Set Role	(c)

	prensic Toolkit Version: 5.0.1.39 Da	abase: lo	localhost			
	Case Tools Manage Help	,				
Cases	New					
Name	Open			n/a		
	Assign Users		Case Owner	n/a		
	Backup		Reference	n/a		
	Restore		Date Modified	n/a		
	Delete		Date Accessed	n/a		
	Copy Previous Case		New Case Options		×	
	Remove Generated Index Refresh Case List	F5	Owner: Case Name: Reference:		FTK	
			Reference:			<u>^</u>
			Description		۵ ۲	
			Description File:			
			Case Folder Directory:	C:\Cases		
			Database Directory:	<casefolder>/DB</casefolder>		
				In the case folder		
			Processing Profile:	AD Standard	▼ Custom	
				✓ Open the case	OK Cancel	
						·

AccessData Forensic Toolkit Version: 5.0.1.39 Database: localhost Case:	FTK	and that
<u>Eile E</u> dit <u>V</u> iew Evi <u>d</u> ence Filter <u>T</u> ools <u>M</u> anage <u>H</u> elp		
Filter: - unfiltered -	r Manager 🛛 📘 🖶	
Explore Overview Email Graphics Video Internet/Chat Bookma		
	File Content	
	Hex Text Filtered Natural	
	Nanage Evidence	
		C:\Users\ficarbone\Desktop\Mantooth.E01
	Mantooth.E01 +	_
	ID / Name:	
	Description:	
	Evidence Group:	Manage
	Time Zone:	America/Denver
		Merge case index Use UNC Paths
	Add Remove	Refinement Options Language Setting
	Case KFF Options	OK Cancel

AccessData Forensic Toolkit Version: 5.0.1.39 Database: localhost Cas	: FTK 🔤					
<u>Eile Edit. V</u> iew Evi <u>d</u> ence Fijter <u>T</u> ools <u>M</u> anage <u>H</u> elp	1					
👻 Fiter: -unfittered - 👻 Fiter Manager						
Explore Overview Email Graphics Video Internet/Chat Bookr						
Evidence Items 4 b						
	Hex Text Filtered Natural					
E-C Q Mantooth.E01	Dear NEW Sweetie.					
B-C Partition 1 3	5 5					
B-C/[• Maxioon [virs] ⊞-C/⊡ [orphan]	I did it! I wrote her and told her it was OFF! I didn't lie or anything.					
	It is all you and me now babe!					
B-C) a \$Recycle.Bin	I printed it and mailed it today so she should get it later this week.					
2 \$Secure ⊕ Boot	i prince it and maned it today so she should get it later this week.					
	How about a date this weekend?					
⊕-□⊃ MSOCache						
🕀 🗁 🧰 Program Files	I met my dad last weekend. He got released and we are trying to patch things up. Here is a picture of him.					
FC> ProgramData C> Super Secret Stuff						
😐 🗁 System Volume Information	What a looker!					
B-D G Users						
🕀 🖵 🛅 Default	File Content Properties Hex Interpreter					
	He Content Propercies Hex interpreter					
File List	🖕 🕞 Display Time Zone: E. South America Daylight Time (From local machine) 🕒 💽 🧟 🗶					
Label Item # Ext Patr	Category P-Size L-Size MD5 SHA1 SHA256 Created Accessed Modified					
	ooth.501/Partition					
	poth.E01/Partition GIF 7168 B 6892 B 12/04/2007 21: 13/07/2007 15: 11/04/2007 17:					
	oshi.50 /Partition Folder 408 8 408 6 05/03/2007 23 02/07/2008 18 07/07/2007 20 oshi.50 /Partition Folder 56 8 56 8 05/03/2007 23 02/07/2008 72 02/07/2007 20					
	ooth.EU.Partition GIF 38,00 KB 37,57 KB 05/03/2007 22: 13/07/2007 15: 05/03/2007 22:					
	ooth.E01/Partition Unknown 1024 KB 1024 KB 1024 KB 1024 KB 10/04/2007 22: 20/06/2008 12: 10/04/2007 19:					
	ooh:D01/PethonMaroso65,0148 65,0148 120/2007 20130/72007 15140/72007 15 D01:D01/PethonUninovan 496 496 8 27/02/2007 15020/72000 15					
EFS DOCS 1683 Man	ooth.E01/Partition Folder 56 B 56 B 05/03/2007 23: 02/07/2008 17: 07/07/2007 20:					
	ooht.B01/Partison PHG 66,00 KB 65,70 KB 05,70 KB 05,70 KB 05,70 KB 05,70 KB 05,70 KB 05,70 KB 12,70 KB 12,7					
	ooh:B1/Partison PEGE_L. 17,50 K8 17,48 K8 05/03/2007 22 13/07/20007 15 05/03/2007 22 ooh:B1/Partison PEGE_L. 17,50 K8 17,48 K8 05/03/2007 25 03/07/2008 17 03/07/2008 17					
🗌 📓 Itunes.jpg Man	ooth.E01/Partition JPEG E 18,00 KB 17,96 KB 05/03/2007 22: 13/07/2007 15: 05/03/2007 22:					
Loaded: 34 Filtered: 34 Total: 34 Highlight	och Entidention Existence 48 48 48 0 0 Elinizione 2 25 0 2017/2009 19 0 Elinizione 2 25 0 2017/2009 2 25					
Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mant	oth/Documents/Dear Sweetie.doc					
Ready	Evolute Tab Filter: [None]					

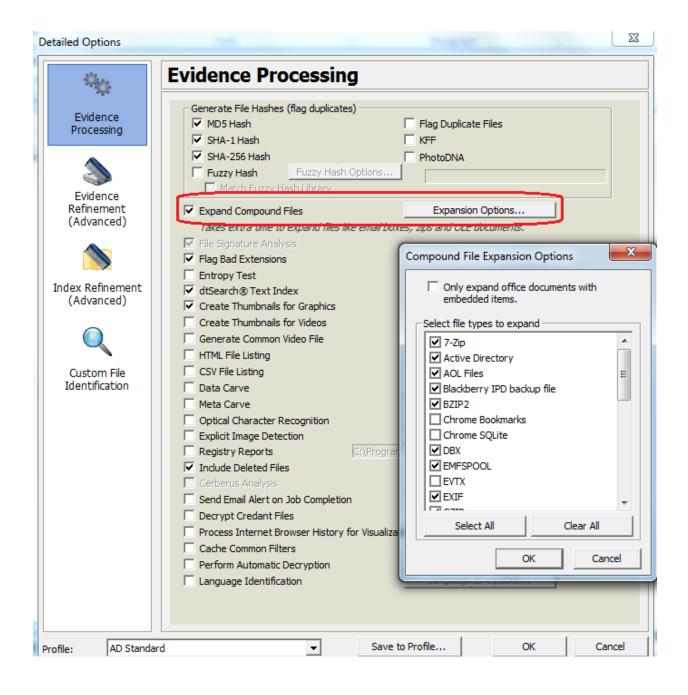
Detailed Options		Contraction of the local division of the loc	×
4 ₀	Evidence Processing		
Evidence Processing	Generate File Hashes (flag duplicates)	Flag Duplicate Files	
Evidence	SHA-256 Hash Fuzzy Hash Fuzzy Hash Options Match Fuzzy Hash Library	PhotoDNA	
Refinement (Advanced)	Expand Compound Files	Expansion Options	
(Advanced)	Takes extra time to expand files like email be File Signature Analysis Flag Bad Extensions Entropy Test	oxes, zips and OLE documents.	
Index Refinement	✓ dtSearch® Text Index	Indexing Options	
(Advanced)	Create Thumbnails for Graphics		
	Create Thumbnails for Videos	Thumbnail Options,	
	Generate Common Video File	Video Options	
Custom File	CSV File Listing		
Identification	Data Carve	Carving Options	
	Meta Carve		
	Optical Character Recognition	OCR Options	
	Explicit Image Detection	EID Options	
		am Files\Acces\RSR Templates	
	Cerberus Analysis	Cerberus Options	
	Send Email Alert on Job Completion Decrypt Credant Files	Credant Server Settings	
	 Process Internet Browser History for Visualiz 		
	Cache Common Filters		
	Perform Automatic Decryption	Passwords	
	Language Identification	Language ID Options	
Profile: AD Standard	▼ Save	e to Profile OK	Cancel

Detailed Options	×
°0	Evidence Refinement (Advanced)
Evidence Processing	Refine by File Status/Type Refine by File Date/Size Inclusion/exclusion settings that will apply to evidence items that are added to the case.
Evidence Refinement (Advanced) Index Refinement (Advanced) Custom File Identification	Include File Slack □ Don't Expand Embedded Graphics Include File Slack □ Don't Expand Embedded Graphics Include OLE Streams: All File Status Ignore status Deleted Ignore status From Email Ignore status Only add items that match both File Status AND File Types criteria
Profile: AD Stand	ard Save to Profile OK Cancel

Detailed Options	×
ф.	Evidence Refinement (Advanced)
Evidence Processing	Refine by File Status/Type Refine by File Date/Size
Evidence Refinement (Advanced) Index Refinement (Advanced) Custom File Identification	Created From Last Modified From 26/12/2013 Last Accessed From 26/12/2013 To AND At least O Bytes At least O Bytes At least O Bytes
Profile: AD Standard	Save to Profile OK Cancel

Chapter 5, Processing the Case

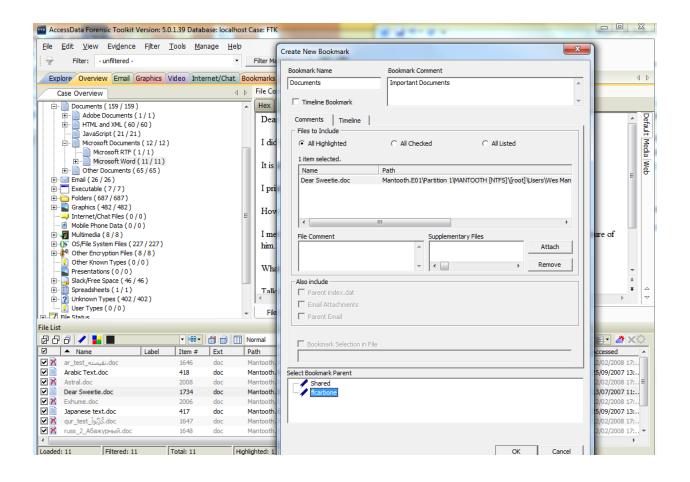
м	anage Evidence			X
	Display Name Mantooth.E01	State	Path:	C:\Users\304020\Desktop\Outline preparation kit. Zipped\Washer.I
	Washer.E01	+		
			ID / Name:	
			Description:	^
				-
			Evidence Group:	- Manage
			Time Zone:	America/Denver
				Merge case index Use UNC Paths
	Add Remove			Refinement Options Language Setting
	Case KFF Options			OK Cancel



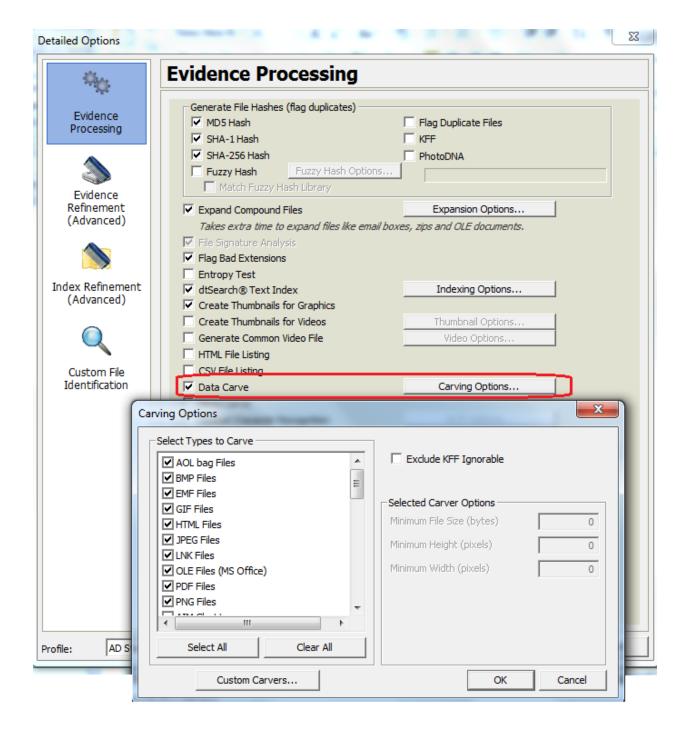
AccessData Forensic Toolkit Version: 5.0.1.3		1000		
File Edit View Evidence Filter Too	Export			
Filter: - unfiltered - Open	- File Options			
anneed Launc	h Append item number to filename		Export emails as MSG	
Explore Overview Email G	Append extension to filename if t	oad/absent	Export emails to PST	
Case Overview	Export children		Preserve folder structure	
Create	Exclude slack space children f	iles	Organization: Separate PST per evidence	
Add to			joeparate i of per evidence	
🕀 🗊 Databases (12 / 12) Remov		name	Export messages from email archives to PS	T
Documents (159 / 159)		name	Include thumbnails of video files	
Adobe Documents (1 Labels			Include common video format	
JavaScript (21/21)	Create manifest files		1 Include common video format	
Microsoft Documents Moun				
Microsoft RTF (1	Include original path			
E··· Other Documents (6:	e			
Executable (7/7)	C All Checked (38)		All Highlighted (1)	
E Goders (687 / 687) Visuali	^{iz} C All Listed (11)		C All	
Graphics (482 / 482) Internet/Chat Files (0 / 0	(Whole disk images, logical images, a	and partitions are always excluded	d)	
File List View F	Destination base path:			
	1			
	C. Osers			
Add to	5			
Arabic Text.doc Find S	ir			
Add to				
Dear Sweetie.doc			OK	Cancel
Exhume.doc Open	ir			
Japanese text.doc			10 00 KP	12/02/2000 17
	to Image	tion Microso 19,00 KB tion Microso 19,00 KB	19,00 KB 19,00 KB	12/02/2008 17: 12/02/2008 17:
4		15,00 KD	20,00 10	12/02/2000 17
Loaded: 11 Eiltered: 11	re to disk image	Checked: 38 Total LSi:	ze: 413,0 KB	
Mantooth.E01/Partition 1/MANT	File List Info	nts/Dear Sweetie.doc		
	Special	Overview Tab Filter: [No	one]	

₽ [Available Columns			Column Templa	ta Nama]	
Expk	Available Columns			Normal (1)	te Name				4
C				1					
<u>.</u>				Selected Colum	ns Short Name	Description	-		
[[Entropy Stats File Status Features File Status Features File System Features Zip-specific Features Custom Columns Office-specific Features	s	Add >> Remove	Name Label Item Number Extension Path File Type	Name Label Item # Ext Path Category	Label asso A number Extension The full pa	of the object (f ociated with an assigned to the ath to an object type ID (or a cu	adata	*
	 ⊕ Cerberus Static Analysi ⊕ Microsoft IIS Internet S ⊕ Log2t ⊕ Internet Data ⊕ All Features 		Move Up Move Down	Physical Size Logical Size MD5 Hash SHA1 Hash SHA256 Hash Created Date Accessed D Modified Date	P-Size L-Size MD5 SHA1 SHA256 Created Accessed	The physic The logical The MD5 H The SHA1 The SHA2 The date to The date to	al size (size on I size of the object nash of the obje hash of the obj 56 hash of the the object was the object was the object was		÷ ÷
⊕							Remove All	SHA1	🕒 💽 🎽 🗙
					Ok	<	Cancel		Column Settings
	Extend	26	Mantooth	.E01/Partition	Folder 4	H8 B 4	148 B	<u></u>	√ Name
_	Recycle.Bin	1813		.E01/Partition			56 B		✓ Label
🛅 Ś	REZFRY8	1830		.E01/Partition			i6 B		√ Item #
. :	RmMetadata	31		.E01/Partition			336 B		✓ Ext
		41	Mantooth	.E01/Partition	Folder 4	18 B 4	18 B		-
	Txf								✓ Path

Aanage Column Setti	ngs		×
Settings Template Cerberus Results EID Email File Listing Internet History Normal Normal +Filters Reports: File Path Reports: Standard eDiscovery eDiscovery Email	s		
New Import	Edit	Copy Selected Make Shared	Delete
		Apply	Close



Additional Analysis	X
Hashing / Job Options Indexing / Tools Miscellaneous	
File Hashes MD5 Hash SHA-256 Hash SHA-1 Hash Fuzzy hash Flag Duplicate Files KFF	PhotoDNA PhotoDNA Refinement
KFF Groups	Include OLE Streams: All
Recheck previously processed items	
Fuzzy hash Match fuzzy hash library Recheck previously processed items Fuzzy hash options	
Target Items	Job Options
C Highlighted Items C Checked Items	Send Email Alert on Job Completion
C Currently Listed Items	
© All Items	
	OK Cancel



AccessDat	ta Forensic Toolkit Version: 5.0.1.39 Datab	ase: localhost Case: FTK	X 4 **	**	
<u>File</u> dit	<u>View Evidence Filter Tools Mar</u>	age <u>H</u> elp	16		
i 🖓 Filt	Iter: - unfiltered -	▼ Filter Manager	2		
Explore	16 01 11	met/Chat Bookmarks Live Search Index	Search Volatile		4 Þ
		File Content Hex Text Filtered Natural			
🕀 💀 File Iter		北朝鮮のミサイル発射の対抗措	置として、日本政府が国民に北朝	脯への渡航自粛を要請した	ことを受 🔺 🖁
	Admin Case: FTK				ことを受 · Default Media Web
Đ Đ Đế	efined Groups		Defined Sets		ledia
	Name Status	Default Closed	Name	Status Source Vendor	Web
			KFF.csv	Alert In House	-
					• ~
.					
File List					
요요					Acce
					12/0
					25/0
	Set As Defaults New	Edit Delete			13/0 12/0
					25/0
	losed KFF groups and sets cannot be edited or	deleted.			07/0
	Import Export Groups				Done 12/0 20/0
	JIFE/GOL 2010	uoc manuoun.conyraruuun micro	50 72,00 Kb 72,00 Kb 110571551506555	3010e410/	12/0
•		m			۲
Loaded: 11	Filtered: 11 Total: 11	Highlighted: 0 Checked: 38	Total LSize: 407,8 KB		

AccessData Forensic Toolkit Versi	ion: 5.0.1.39 Database: localhost Case: FTK	8 4 7 - 0 - C					
File Edit. View Evidence Filter Tools Manage Help							
Filter: - unfiltered -							
W There Guindered		<u>•</u>					
Explore Overview Email Grap	hics Video Internet/Chat Bookmarks Live Search Inde	x Search Volatile	4 ⊳				
Case Overview	↓ File Content						
Evidence Groups (71.468 / 71	(Univ Test Strend Natural		D				
🗄 🖬 🖬 File Items	Additional Analysis	X	要請したことを受 → 🛛				
E	Hashing / Job Options Indexing / Tools Miscellaneous		要請したことを受 Default Media Web				
File Category (2.069 / 2.069)	File Hashes	PhotoDNA					
	MD5 Hash SHA-256 Hash	PhotoDNA	edia				
🖻 📄 Documents (209 / 209)	SHA-1 Hash Fuzzy hash		w later w				
Adobe Documents (1,	Flag Duplicate Files		ら重なり、新たな 8				
HTML and XML (73 / 7 Microsoft Documents (Refinement	ビ対応に追われて・				
Other Documents (12)	KFF	Include OLE Streams: All	±				
	KFF		¥ △				
	Recheck previously processed items		▶ ▽				
Folders (687 / 687) Graphics (451 / 451)	-Fuzzy hash						
File List	Match fuzzy hash library						
8877 / 1	Recheck previously processed items		🍅 🗐 - 🏄 X 🔿				
☑ ▲ Name	Fuzzy hash options		HA256 Created Acce				
doc.نقيصته_ar_test.نقيصته			12/02/2008 17: 12/0				
Arabic Text.doc	Target Items	Job Options	25/09/2007 13: 25/0				
Astral.doc	C Highlighted Items	Send Email Alert on Job Completion	12/02/2008 17: 12/0				
Dear Sweetie.doc	C Checked Items		12/07/2007 16: 13/0				
Japanese text.doc	C Currently Listed Items All Items		12/02/2008 17: 12/0 25/09/2007 13: 25/0				
Normal.dot	· Air temis		07/07/2007 15 07/0				
doc.کَذِيَواdurtest			12/02/2008 17: 12/0				
🗹 🕅 russ_2_Абажурный.doc			12/02/2008 17: 12/0				
Something interesting.rtf			08/03/2007 19: 20/0				
Vampire.doc		OK Cancel	12/02/2008 17: 12/0				
l (l			1)				
			Þ				
Loaded: 11 Filtered: 11	Total: 11 Highlighted: 0 Checked: 38	Total LSize: 407,8 KB					

AccessData Forensic Toolkit Version:	5.0.1.39 Database: localhos	t Case: FTK	a 30	at Associate in			
<u>File Edit View Evidence Filter</u>	<u>T</u> ools <u>M</u> anage <u>H</u> elp						
Filter: - unfiltered -							
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Volatile							
Text Pattern Hex					Live Search (Prefilter:(- unfiltered -) Query:("Mantooth")) (ID:		
mantooth		<u>A</u>	dd Clear	Export Import	Text Query: "Mantooth" <ansi, case="" insensitive=""> 821</ansi,>		
ANSI 🗆 Unicode 🕨 🗌 Other Coo	Allocated Space 814 hit(s) in 125 file(s)						
Search Terms Type	200 hit(s) Item 839 [index.dat] Mantooth.E01/P						
Mantooth ANSI(Case Insensitive)							
					⊞ 56 hit(s) Item 12 [\$MFT] Mantooth.E01/Partition =		
					38 hit(s) Item 1372 [index.dat] Mantooth.E01/P		
					⊕-31 hit(s) Item 593 [index.dat] Mantooth.E01/Pa ⊕-27 hit(s) Item 588 [index.dat] Mantooth.E01/Pa		
	earch Filter: - unfiltered -	•		<u>S</u> earch			
File Content					1 hit(s) Item 427 [NTUSER.DAT] Mantooth.E01		
Hex Text Filtered Natural					20 hit(s) Item 1936 [SOFTWARE] Mantooth.E01		
					It hit(s) Item 428 [ntuser.dat.LOG1] Mantooth. It hit(s) Item 595 [index.dat] Mantooth.E01/Pa		
					B hit(s) Item 451 [edb0000C.log] Mantooth.E01,		
	T hit(s) Item 452 [WindowsMail.MSMessageStore						
	🕀 6 hit(s) Item 485 [2A29541D-0000000E.eml] Ma						
	6 hit(s) Item 1582 [downloads.rdf] Mantooth.E0						
					⊕ 4 hit(s) Item 446 [edb.chk] Mantooth.E01/Partit ⊕ 4 hit(s) Item 489 [3376666D-0000000A.eml] Ma		
No file	H + 1 htts) Item 491 [40A511AF-0000008.em] Ma H → 4 htts) Item 491 [40A511AF-0000008.em] Ma						
File Content Properties Hex	Interpreter						
File Concenc Propercies Hex	Interpreter				B 3 hit(s) Item 262 [mantooth2007.ARL] Mantooth		
File List					⊡ 3 hit(s) Item 460 [165D65F6-00000004.eml] Mai		
@887 / ▙ ■	• 💷 💼 🔲	Normal	Display Time Z	🗐 🔹 👗 X 🔅	. 3 hit(s) Item 495 [458C76A0-0000000C.em]] Ma		
☑ ▲ Name Label	Item # Ext	Path	Category P-Size	L-Size MD5	⊕ 3 hit(s) Item 508 [09EE4522-00000004.em] Mar ⊕ 3 hit(s) Item 1566 [~ar1730.xar] Mantooth.E01		
SMFT	12 <missin< td=""><td>Mantooth.E01/Partition</td><td>Unknown 9344 KB</td><td>9344 KB e17b14</td><td></td></missin<>	Mantooth.E01/Partition	Unknown 9344 KB	9344 KB e17b14			
🗌 🕐 ~ar1730.xar	1566 xar	Mantooth.E01/Partition	Unknown 6656 B	6656 B 258af4			
~ar1730.xar.lnk	1499 lnk	Mantooth.E01/Partition	Windo 488 B	488 B 21f68d	2 hit(s) Item 1430 [08-15-05_arkansas_check.gi		
018270	1978	Mantooth.E01/Partition	Unalloc 512,0 KB	512,0 KB			
04f24080836c56509cab	1294 <missin< td=""><td>Mantooth.E01/Partition</td><td>Unknown 512 B</td><td>53 B 6a7939</td><td> 2 hit(s) Item 1435 [91064B.gif.lnk] Mantooth.E0 2 hit(s) Item 1436 [Ape_20shoot.gif.lnk] Mantoo </td></missin<>	Mantooth.E01/Partition	Unknown 512 B	53 B 6a7939	 2 hit(s) Item 1435 [91064B.gif.lnk] Mantooth.E0 2 hit(s) Item 1436 [Ape_20shoot.gif.lnk] Mantoo 		
062746 08-15-05 arkansas che	1981 1430 Ink	Mantooth.E01/Partition	Unalloc 32,50 KB Windo 1024 B	32,50 KB 743 B 9a9b8d			
		Mantooth.E01/Partition	Windo 1024 B	743 B 989080			
·				P.	🗈 2 hit(s) Item 1443 [C01VNCCHK_e.gif.lnk] Manta 🔻		
Loaded: 128 Filtered: 128	Total: 128 Hid	phlighted: 0 Checked	d: 38 Total LS	ize: 45,42 MB	4 III +		

AccessData Forensic Toolkit Version: 5.0.1.39 Database: localhost Case: FTK							
Ele Edit View Evidence Filter Iools Manage Help							
Filter: - unfiltered -							
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search Volatile	4 Þ						
dtSearch@ Index 4	Index Search Results						
Terms Search Criteria	⊡. dtSearch® Indexed Search {Prefilter:(all files) Qu						
Operators Terms Clear	Allocated Space 6966 hit(s) in 1975 file(s)						
Mantooth Add G And C Or G All C Selected G Accumulate Results	Documents 736 hit(s) in 207 file(s) Spreadsheets 10 hit(s) in 2 file(s)						
Indexed Words Total Hits Search Terms Total Hits	Databases 22 hit(s) in 3 file(s)						
mantain 1 mantooth 6996 Export	Graphics 1398 hit(s) in 447 file(s) Multimedia 15 hit(s) in 5 file(s)						
mantooth 6996 Options	Email 121 hit(s) in 26 file(s) Email 121 hit(s) in 26 file(s)						
mantoothU 6 mantooth1 9Search Now	⊕ Executable 18 hit(s) in 6 file(s)						
mantooth1_23545 1	Archives 36 hit(s) in 12 file(s)						
mantooth1_85050 1 mantooth2000 1	Folders 1591 hit(s) in 657 file(s) Other Encryption Files 74 hit(s) in 17 file						
mantooth2007 27	Internet/Chat Files 354 hit(s) in 19 file(
mantooth20071 3 mantooth2007@aol 22 v	OS/File System Files 1136 hit(s) in 256 t						
	 Other Known Types 8 hit(s) in 2 file(s) Unknown Types 1447 hit(s) in 316 file(s) 						
	Unallocated Space 30 hit(s) in 30 file(s) Unallocated Space 30 hit(s) in 30 file(s)						
File Content							
Hex Text Filtered Natural							
Hit # of Prev Next Go to: Go							
Meda							
* 1							
۲. () () () () () () () () () (
File Content Properties Hex Interpreter							
File List							
🖓 🖓 🖉 🥒 🖊 🔛 🔹 👘 👘 🛄 Normal 🗸 Display Time Zone: America/Ph							
☑ ▲ Name Label Item # Ext Path Category P-Size L-Size MD5 ▲							
Image: #local 1283 Mantooth.E01/Partition Folder 160 B 160 B							
Image: Security 1271 Mantooth.E01/Partition Folder 272 B 272 B Image: Security 1271 Mantooth.E01/Partition Folder 272 B 272 B							
#SharedObjects 1274 Mantooth.E01/Partition Folder 152 B 152 B							
Loaded: 2.005 Filtered: 2.005 Total: 2.005 Highlighted: 0 Checked: 38 Total LSize: 110.2 MB	۲						

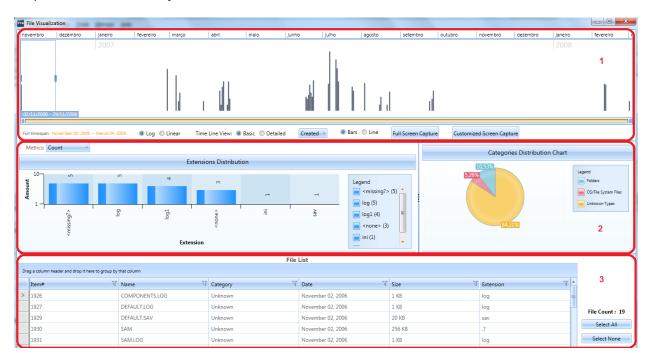
AccessData Forensic Toolkit	t Version: 5.0.1.39 Database: localhost Case: FTK	-	and Among the Compt Comparising Multiple Mean Property	- • ×
<u>File E</u> dit <u>V</u> iew Evi <u>d</u> enc	e Filter <u>T</u> ools <u>M</u> anage <u>H</u> elp			
Filter: - unfiltered -	▼ Filter Manager	. 💼 🕁		
Explore Overview Email	Graphics Video Internet/Chat Bookmarks Live S			4 Þ
		earch index Search vo	↓ Live Search Results	V V
Text Pattern	Hex			
			Clear Export Import	
ANSI Unicode	any character		MAC Address	
Search Terms Type	\t - tab	Code Pages	URL {http, https, ftp, ftps}	
	\s - whitespace character	N P	OKL {http://ttps//ttps/	
	\d - decimal digit - same as [0-9]		mailto:	
	\u - upper case character - same as [A-Z]			
Max Hits Per File: 200	\I - lower case character - same as [a-z]			
File Content	\w - word character - same as [a-zA-Z0-9_]			
Hex Text Filtered Na	\n - newline character		org	
	\r - return character			
	\b - at word boundary		museum	
	\B - not at word boundary		tv	
	\< - at start of word		<any></any>	
	() destate of word		@com	
	^ - at start of line		@edu	
•	S - at end of line		@	
File Content Proper	\` - at start of file		@net	
File List	\' - at end of file	Diselas Tires	@org	
8881 #	? - match previous 0 or 1 times	Display Time	@	
Name	* - match previous 0 or more times	Category P-	All Leaves	
	+ - match previous 1 or more times		All Issuers AMEX	
	{n} - match previous n times		AMEX Visa	
	{n,} - match previous n or more times		Visa Mastercard 1	
	{m,n} - match previous m to n times		Discover	
			Credit Card Standard	
•	[[:alpha:]] - alpha character		Web Credit Card Transaction Receipt with X or #	
Loaded: 0 Filtere	[[:alnum:]] - alpha-numeric character	hecked: 38		

🔤 AccessData Forensic Toolkit Version: 5.0.1.39 Database: localhost Case: FTK	
File Edit View Evidence Filter Tools Manage Help	
Filter: - unfiltered -	
- compound -	4 ⊳
dtSearch® Actual Files	
lerms Archive Files / Name / A	
mantooth Bad Extension Files Actual Files Alternate Data Streams	
Bookmarked Archive Files >>>	
Indexed Words Tantain Cerberus Score Bookmarked	
mantoo Cerberus Static Analysis Carved Files	
mantooth Checked Files	
Checked Files	
Decrypted Files C AND C C R Clear	
File Content Deleted Files	
Hex Text Filtered Natural eDiscovery Refinement w/o OCR Exclude	
Hit # of Prev Next Email Attachments Prave Name /	
Email Files	
Email Files and Attachments	
Evidence Items	
Excluded eDiscovery Refinement w Explicit images folder (high score)	
Explicit images folder (medium score)	
File Category	
File Created Time	
File Content Properties Hex Interpreter	
FileList	
Per P P F Cose	
☑ Name Label Item ≠ Ext Path Category P-Size L-Size MDS	
Loaded: 0 Filtered: 0 Total: 0 Highlighted: 0 Checked: 38 Total LSize: 0	

AccessData Forensic Toolkit Version: 5.0.1.39 Database: localhost Case: FTK	Contraction (1997) (19977) (19977) (1997) (1997) (1997) (1997) (1997) (1997)	
Elle Edit View Evidence Filter Icols Manage Help Image: Second	anager 📗 🔂	
Explore Overview Email Graphics Video Internet/Chat Bookmarks	Live Search Index Search Volatile	4 ⊳
dtSearch® Index	↓ Index Search Results	
	Terms Gear Gear Import	
Indexed Words Total Hits A Search Terms Manage Filters	Total Hits	×
mantoo	Piter Dennition: temp	
mantooth	Properties:	
Actual Files	Name: Temp Description:	
File Content Archive Files Bad Extension Files	Rules:	
Hex Text Bookmarked Hit # Carved Files		
Cerberus Score	Properties Operators Criteria -+ IV Filter 	_
Cerberus Static Analysis Checked Files		
Decrypted Files Deleted Files		
Duplicate Files		
eDiscovery Refinement w/o OCR Email Attachments		
Email Delivery Time		
	C Match Any C Match All Save Close	
File Cont New Edit, Copy, Delete	Close Close	:i
File List Import Export Copy to Shared	Display Time Zone: America/Ph	
	Display Time Zone: America/Ph Display Time Zone: America/Ph Category P-Size L-Size MD5	
Close		
Loaded: 0 Filtered: 0 Total: 0 Highlighted: 0	Checked: 38 Total LSize: 0	

AccessData Forensic Toolkit Version: 5	5.0.1.39 Database: localhost Case: FTK	-	and particular sections.	
<u>File E</u> dit <u>V</u> iew Evi <u>d</u> ence Filter	<u>T</u> ools <u>M</u> anage <u>H</u> elp			
Export	 Filter Mana 	ager 📄 🖶		
Export to Image	Yest 1			
Export File List Info	Video Internet/Chat Bookmarks I	Live Search Index Search Vol	atile	4 1
Export Word List	↓ b File Content			
Report	Hex Text Filtered	Vatural		
Timeline Report	Report Options			
Volatile Data Report				
Job Summary Report	Report Outline	Default entries		
Close	Case Information	La	bel Value	
Exit	Graphics	Agency/Company 🔽 A	gency/Company	
Ežic	Videos	Investigator's Name 🔽 In	vestigator's Nam	
	File Paths	Address 🔽 A	ddress	
	Registry Selections	Phone 🔽 Ph	none	
	Screen Capture	Fax 🔽 Fa	ix	,
		Email 🔽 Er	mail	
File List		Comments 🔽 Co	omments	
₫₽₫ / ▙ ■				📥 🗠 🗠
✓ A Name Label				
The focal				14:
Security #SharedObjects				14:
\$AttrDef				16:
2 \$Bad				16:
\$BadClus	Import			16:
\$Bitmap \$Boot	· · · · · · · · · · · · · · · · · · ·	Include File Extensions		Add Remove 16:
\$Config	Export			14:
⊈∳° \$EFS				19:
SEFS				0K [Cancel] 19:
■ I SEFS ■ I SEFS				OK Cancel 19: 19:
Service Servic	26 Mantooth.E0	1/Partition Folder 448 B	448 B	06/07/2007 16: 06/07/2007 16:
\$12M7A26.jpg		1/Partition Unknown 544 B	544 B 73ed7a	26/07/2007 16: 26/07/2007 16:
□ () \$130		1/Partition Index 4096 B		07/07/2007 14: 02/07/2008 13:
<		III III	toocin di la	1
Loaded: 1.964 Filtered: 1.964	Total: 1.964 Highlighted: 0	Checked: 38 Total	LSize: 102.7 MB	

Report Output		×
Report Folder		
Formats PDF RTF HTML WML XML DOCX ODT	Export Options Use object identification number for filename Append extension to filename if bad/absent HTML Report Customization Use custom logo graphic Use custom CSS	× v
	OK	Cancel



Agent Installation	
Machines to install	
192.168.0.182	
	Add
Remove Import	Export
🗌 Uninstall agent	
Use custom agent name	
Service name: AgentService	
Executable name: agentcore.exe	
Update the agent if it is present	
Allow manual uninstall	
ОК	Cancel

Chapter 6, New Features of FTK 5

Credentials							
Domain Testes	Username flcarbone						
, Domain:	Testes						
Username:	ficarbone						
Password:	******						
Confirm Password:	******						
Add Remove							
	OK Cancel						

AccessData Foren	sic Toolkit Version:	5.0.1.39 Databa	ise: localhos	t Case: F	тк	-		1.00								
<u>F</u> ile <u>E</u> dit <u>V</u> iew	Evidence Filter	Tools Man	age <u>H</u> elp													
Elter:	Add/Remove			Filter	Manager		₽									
	Add <u>R</u> emote	Data							_							
Explore Overvie	Additional Ar		B	lookmar	ks Live Sear	ch Ind	ex Sear	ch Volatile								
Evidence Item	_			↓ ▶ F	File Content											
Evidence	Process Man	ually Carved Ite	ms		Hex Text	Filtered	Natu	ral								
E Mantoot	<u>M</u> anage Evid	ence Groups		ŀ				00 00 00	00-	00 0	0 00	00 0	00 00	00 01	n	
🗄 🕁 💭 🏹 memdun	Import Mem	ory Dump					00 00	00 00 00	00-	00 0	0 00		0 00	00 0	-	
		· · · ·			000000090	00 00	00 00	00 00 00	00-	00 0	0 00	00 0	00 00	00 00	o	
	Import Custo	om Column File.					00 00	00 00 00	00-			00 0	00 00	00 00	-	
	Delete Custo	im Column Data	a		0000000000	00 00	00 00	00 00 00	00-	00 0 00 00			00 00	00 00	-	
	Merge Case 1	Index		FTK Age	ent				~		0 00			00 0		
						-			-	0 00	0 00	00 0	00 00	00 00		
					Remote Add	ress: 1	92.168.0	. 182						00 00	-	
					Remote	Port: 3	000	_		0 00 0 00			00 00	00 00	-	
					i cento ce i	0.0 13							00 00		-	
				O Ins	stall Temporary	Agent									- 1	
				🛈 Us	e Existing Ager	nt										
										prete	ar					
-						ОК		Cancel		prece	-					
File List									-							
₽ ₽ ₽ ∕ 🔒		•	i di 🔟	Normal		• [isplay T	ime Zone: E.	Sout	n Ame	rica Da	aylight	:Time (From lo	ocal machine)
🗹 🔺 Name	Label	Item #	Ext	Path		Ca	tegory	P-Size	L-Si	ze	MD	5	SHA	1	SHA256	Created
= #local		1283		Mantoo	th.E01/Partitio	n Fo	lder	160 B	160	В						07/07/2007 19:
#Security		1271		Mantoo	th.E01/Partitio		lder	272 B	272	В						07/07/2007 19:
#SharedObje	ts	1274			th.E01/Partitio		lder	152 B	152	-						07/07/2007 19:
AttrDef		16	<missin< td=""><td></td><td>th.E01/Partitio</td><td></td><td></td><td>2560 B</td><td>256</td><td>0 B</td><td></td><td></td><td></td><td></td><td></td><td>06/07/2007 20:</td></missin<>		th.E01/Partitio			2560 B	256	0 B						06/07/2007 20:
Sad 🕄 🕄		20		Mantoo	th.E01/Partitio	n No	t Yet	0 B	0 B							06/07/2007 20:

Classification Contraction Contraction Contraction Contractions	* FTK	a fee among as the			
Ele Edit View Evidence Filter Tools Manage Help	er Manager				
Explore Overview Email Graphics Video Internet/Chat Bookm Snapshot Find Difference 4 b					4 ♭
≥ €		Start Time Working Directory	/ Command Line PID	Has Searc Parent PID Us	er MD5 St ^
□-	SearchProtocol postgres.exe C:\Program Files\AccessD	18/01/2014 20:35: 18/01/2014 20:36: C:\pgData91\	"C:/Program Fil 10808	N 0 N 0	
□ → 18/01/2014 18:38:51 (UTC)	c.vprogram Files (x86) (Int c.vprogram Files (x86) (Int mcshield.exe C: (Program Files (Common	15/01/2014 17:40: C:\WINDOWS\		N 0 N 0	000000000000000000000000000000000
Carbone (dump)	AcroRd32.exe C:\Program Files (x86)\Ad	18/01/2014 19:15: C:\WINDOWS\ 15/01/2014 17:40: C:\WINDOWS\	"C:\Program Fil 11868 "C:\Program Fil 11188	N 0 N 0	000000000000000000000000000000000000000
E-6 18/01/2014 18:38:51 (UTC)	splwow64.exe C:\WINDOWS\splwow64	18/01/2014 18:52: C:\WINDOWS\ 18/01/2014 19:15: C:\WINDOWS\	C:\WINDOWS\s 8576 "C:\Program Fil 11868	N 0 N 0	00000000000000000000000000000000000000
E-▲ S Driver List □-▲ 38/01/2014 18:38:51 (UTC) ▲ S Carbone (dump)	AcroRd32.exe C:\Program Files (x86)\Ad	16/01/2014 20:57: C:\WINDOWS\ 18/01/2014 19:15: C:\WINDOWS\	"C:\Program Fil 9336 "C:\Program Fil 1188	N 0 N 0	000000000000000000000000000000000000000
□- □	AcroRd32.exe C:\Program Files (x86)\Ad	16/01/2014 20:57: C:\WINDOWS\ 18/01/2014 19:15: C:\WINDOWS\ 16/01/2014 20:57: C:\WINDOWS\	"C:\Program Fil 9336 "C:\Program Fil 1188 "C:\Program Fil 9336	N 0 N 0 N 0	
		18/01/2014 12:52: C:\WINDOWS\	"C:\Program Fil 12988	N O	000000000000000000000000000000000000000
System Descriptor Table	Total: 149 Highlighted: 1 Checked: 0	KFF: Unlisted, Important, Unimport	ant		
□ (a) 18/01/2014 18:38:51 (UTC) Carbone (dump)	Detailed Information DLLs TCP/IP Handles Fuzzy Hash Search Hits SDT	VAD			
	Name Description	Path Has Searc C:\Program Files (x86)\Int N	Version	Creation Time Process Nam 15/01/2014 17:40: iexplore.exe	11188 000000000000000000000000000000000
	ntdl.dl www64.dl	C:\WINDOWS\\$YSTEM32\ N C:\WINDOWS\\$YSTEM32\ N		15/01/2014 17:40: iexplore.exe 15/01/2014 17:40: iexplore.exe	11188 000000000000000000000000000000000
	wow64win.dl	C:\WINDOWS\SYSTEM32\ N C:\WINDOWS\SYSTEM32\ N		15/01/2014 17:40: iexplore.exe 15/01/2014 17:40: iexplore.exe	11188 000000000000000000000000000000000
	iexplore.exe ntdl.dl kernel32.dl	C:\Program Files (x86)\Int N C:\WINDOWS\SysWOW6 N C:\WINDOWS\syswow64\ N		15/01/2014 17:40: iexplore.exe 15/01/2014 17:40: iexplore.exe 15/01/2014 17:40: iexplore.exe	11188 000000000000000000000000000000000
	KERNELBASE.dl	C:\WINDOWS\syswow64\ N C:\WINDOWS\syswow64\ N		15/01/2014 17:40: iexplore.exe 15/01/2014 17:40: iexplore.exe	
	msvcrt.dll sechost.dl	C:\WINDOWS\syswow64\ N C:\WINDOWS\SysWOW6 N		15/01/2014 17:40: iexplore.exe 15/01/2014 17:40: iexplore.exe	
l	RPCRT4.dl	C:\WINDOWS\syswow64\ N C:\WINDOWS\syswow64\ N		15/01/2014 17:40: iexplore.exe 15/01/2014 17:40: iexplore.exe	11188 000000000000000000000000000000000
		-	_		X
Additional Analysis		10.0			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Hashing / Job Options Indexing	/Tools Miscellaneous				
-Indexed Search			ols		
dtSearch® Text Index			tical Character	Recognition	OCR Options,.,
Process File Slack Space			olicit Image Det	-	EID Options
Process Drive Free Space	e	C Reg	gistry Reports		RSR Directory,
 Entropy Test (do not index compressed of 	or encrypted items)	Cer	rberus Analysis		Cerberus Options
Do not include document m	etadata in filtered text	🗌 Lan	nguage Identifio	cation	Lang ID Options,.,
Merge case index when fini	shed				
Decryption		Ev	olicit Image D	etection Options	x
Decrypt Credant Files	Credant Server Settings		Shere introge D	etection options	
Perform Automatic Decrypti	on Passwords,.,	F	X-DFT (defa	ult)	
		[X-FST (faste	er)	
		L L L	X-ZFN (more	e accurate)	
				ОК	Cancel
				ОК	Cancel

Additional Analysis			23
Hashing / Job Options Indexing / Tools Miscellaneous			
_Indexed Search	Other Tools		
🗖 dtSearch® Text Index	Optical Character Recognition	00	R Options
Process File Slack Space	Explicit Image Detection	EII	O Options,,,
Process Drive Free Space	Registry Reports	RSF	Directory
 Entropy Test (do not index compressed or encrypted items) 	🗖 Cerberus Analysis	Cerbs	erus Options
Do not include document metadata in filtered text	Language Identification	Lang	ID Options
Merge case index when finished			
Decryption			
Decrypt Credant Files Credant Server Settings			
Perform Automatic Decryption Passwords			
		ок	Cancel

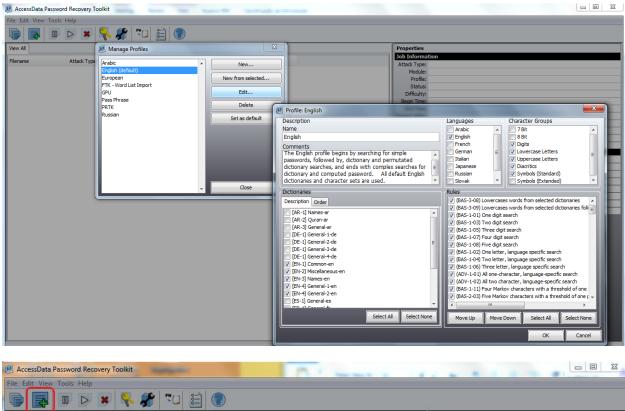
File Content Hex Text Filtered Natural				T	
EXAMPLE.EXE Score: 49 +/- Cerberus Score	CA9E66C59	92100D3BD7[DOB47BF3F9D4C	1	Default Web
Function Call Summary ±/- File Access DeleteFileA(<unknown>) CreateFileA(<unknown>, < CreateFileA(<unknown>, < CreateFileA(<unknown>, < CreateFileA(<unknown>, < Loads a driver Low-Level Access Network Functionality Process Manipulation Security Access ±/- Subverts API Surveilliance Uses Cryptography Windows Registry Function Call Detail</unknown></unknown></unknown></unknown></unknown>	∶unknown>, <unknow< th=""><th></th><th></th><th>-</th><th></th></unknow<>			-	
	Argument(s)			•	
ContinueDebugEvent 5488498	Name dwProcessId dwThreadId dwContinueStatus	Type DWORD DWORD DWORD	Value <unknown> <unknown> <unknown></unknown></unknown></unknown>		
DebugActiveProcess 5488474	Name	Туре	Value	-	~
File Content Properties Hex Inte	rpreter				

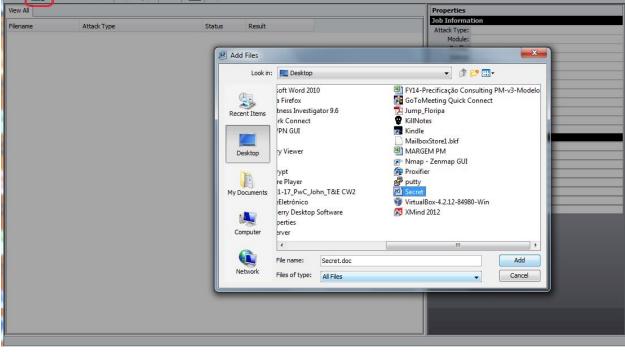
Device Time Analysis Enformation Data Visualization Files		100 24 1752 Calendar ony Calendar	Cookies Web	1 Notes	31 5 App Data Applications					
System Application Data X										
A Dropbox (dropbox)			-	1						•
 Google Voice (googlevoice) LinkedIn (linkedin) 			20333	245	Fri Mar 04 21:23:11 +0000 2011	0	545	1	Welcome to official twitter page for United. We look forward to connecting with you.	260907612
Osfoora (twitter) accounts			2116	280	Thu Apr 30 11:28:02 +0000 2009	0	430	0	ForensicFocus.com - computer forensics portal for digital forensics and ediscovery practitioners	36641167
drafts friends storedDMs		Southern California	654	107	Mon Aug 31 14:59:57 +0000 2009	7	3818	0	Police/Medical Technical Advisor for The Mentalist	70412647
storedDMsSent storedtweets		NY	205	31	Tue May 25 16:59:09 +0000 2010	0	115	0	Apple OS X & iOS Digital Forensics	148025431
 storedmentions Skype (skype) Accounts 		Lindon, UT	1660	567	Fri Sep 04 15:09:57 +0000 2009	0	1954	0	See new videos, resources & industry news from AccessData, a leading provider of E-Discovery, Forensics & Cyber Security software.	71557070
 CallMembers Calls ChatMembers 	m	Oxford	312237	0	Fri Sep 11 14:57:38 +0000 2009	0	474	0	C. S. Lewis Quotes Everyday	73402979
ChatMembers Chats Contacts		Dallas, TX	1617240	15	Tue Jan 30 22:14:50 +0000 2007	3114	3781	0	Woot : One Day, One Deal. See followers for additional Woot feeds.	734493
 Conversations Messages SMSes 		For USA customers	1589818	35	Tue May 01 15:46:16 +0000 2007	35	1544	1	Refurbished Dell [™] computers, electronics. Questions/comments? Contact Chris Beutnagel @ChrisCBAtDell or Elise Osborn @EliseAtDell.	5688592
	wilson	Los Angeles- ish	2384295	225	Wed Jan 28 05:28:45 +0000 2009	1226	5515	1	I am an actor and a writer and I co- created SoulPancake and my son, Walter.	19637934
	ices.shtml	NYC - On tour this summer	590958	455	Sun Jun 03 11:09:19 +0000 2007	35	1673	1	Husband to hot wife, father of 4, comedian, actor, writer, former sleeper http://favstar.fm/users/JimGaffigan Itunes = http://tinyurl.com/65z4dfy	6539592

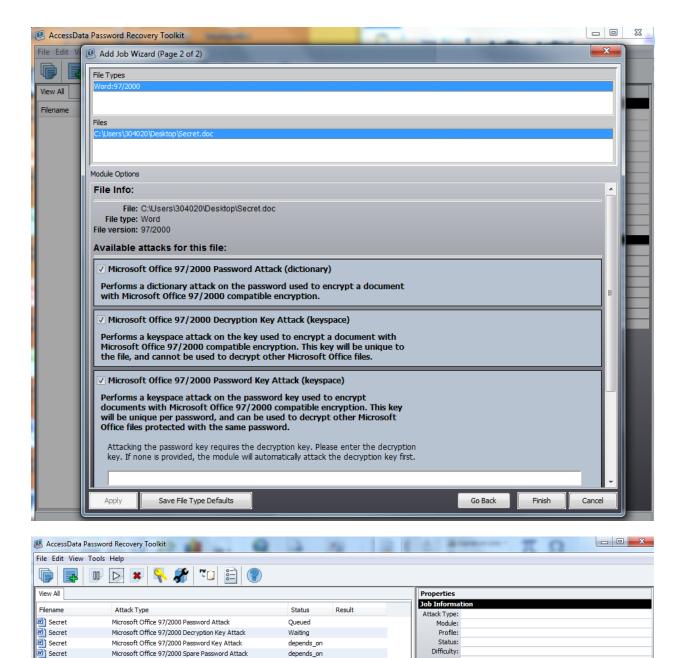
Chapter 7, Working with PRTK

Module Name	Display Name	Attack Types	Supported Products
ABICoder	ABICoder Password Module	dictionary	Product Name: ABI Coder Versions supported: 3.5.7.4 - 3.6.1.4
Access	MS Access Password Module	decryption dictionary	Product Name: Microsoft Access Versions supported: Through 2013
ACT	ACT! Password Module	decryption	Product Name: ACT! Versions supported: 1 - 4 2000 5 - 6
AdvancedFileLock	AdvancedFileLock Password Module	dictionary	Product Name: Advanced File Lock Versions supported: 6 - 7.1
AIM	AIM Password Module	decryption dictionary	Product Name: AOL Instant Messenger Versions supported: Through 7.5 Product Name: AIM Triton Versions supported: Through 1.5 Product Name: AIM For Windows Versions supported: Through
AmiPro	AmiPro Password Module	dictionary	Product Name: Ami Pro Versions supported: <i>Unknown</i>

AccessData Passwo	ord Recovery Toolkit	A			-	
File Edit View Tools	Help					
	🖻 🕱 Қ 🧩	PW 🗀 🖹 🍘				
View All						Properties
Filename	Attack Type		Status	Result		Job Information Attack Type: Module: Profile: Status: Difficulty: Begin Time: End Time: Derryptable: Result Type: Comments: File Information Filename: Type: Version: Size: MD5: SHA-1: Created: Modified:







depends_on

Difficulty:

Begin Time: End Time Timeout After: Decryptable Result Type Results: File Informati Filename Туре Version Size MD5 SHA-1: Created Modified:

Microsoft Office 97/2000 Spare Password Attack