Sammeln von ProcMon-Protokollen zur Fehlerbehebung bei AMP-Problemen beim Systemstart

Inhalt

Einführung Verfahren:

Einführung

Als Systemadministrator können Sie mithilfe von Process Monitor (procmon.exe) detaillierte Protokolle abrufen, um festzustellen, ob der FireAMP-Anschluss beim Systemstart hängen bleibt. Diese Protokolle werden auch vom Cisco TAC angefordert, um solche Probleme zu beheben. Process Monitor ist ein kostenloses Dienstprogramm, das uns hier helfen kann. Diese können Sie kostenlos unter <u>https://docs.microsoft.com/en-us/sysinternals/downloads/procmon</u> herunterladen.

In diesem Dokument werden die Schritte zum Sammeln von ProcMon-Protokollen und Speicherabbildern beschrieben, wenn das Problem während eines Systemstartprozesses auftritt (d. h., es generiert beim Booten BSODs). Diese Protokolle sind erforderlich, um die Systemereignisse zu erfassen, die während des Bootvorgangs auftreten.

Verfahren:

1. Richten Sie die Testgeräte so ein, dass das Problem leicht reproduziert werden kann.

2. Laden Sie das ProcMon-Programm herunter und führen Sie es als Administrator aus. Gehen Sie zu **Datei -> Sicherungsdateien verarbeiten** und wählen Sie einen **Pfad aus**.

nona Monitor - C/(De	ani/win7.64 new/Deakto	phprocessor_putput/setC.pml								
the best file	Tools Options Help									
	A & I I A A									
Pocess Name Search Indexer Search Indexer Search Indexer Search Indexer Equiver DI E	PD Connector 2010 A file System Care 2012 A file System Care 2012 A file System Care 2012 A file System Care 2013 A file System Care 2014 A file Care Se 2014 A file C	Path IC IC IC IC INCU Software Classes INCU Software Classes		Panal SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS	Detail Control FISC Control FISC Control FISC Thread ID: 21 Cuarty Name Cuarty Name County Name County Name County Name	LQ. LQR. LQR. BM				
· Process Manitor	r Backing Film									
These backing file of	biech are being used to sho	en event data								
New		Fast Cast	Event Bater	Pandro Frants	Property Court	Orderen Court	Inter Court	Constant		
C'Ueniwn344	iree" Deektop (pooren_ou	purf (HealTiperi 106.123)	40.911.38	5	50	1994	73	Ro		
Process Hartlar car	stare events in vitual ner	nory (inited by the system consult in	t), or in a file you is	pecify (initial by free	del spece). Which	de you prefer t				
· Une fin named	C Line (and Address	Contractor output that Lord								
*	-									
Pro/Panioad: 0.49	(priorequery) (10 0 40								X	Cancel
Distore EXE Distore EXE EXE worked	2988 AugCourNay 2988 RegCourNay 2988 RegCourNay	HICR Applications' votepaid and HICR Applications' votepaid and HICR Applications' votepaid and		SUCCESS SUCCESS SUCCESS	Duared Acce Query Name	= Ř.				

3. Gehen Sie im Procmon Tool zu **Options -> Enable Boot Logging**.

🚑 Pro	caus Monit	er - C:\Us	ani/wini	7x64-rww\Deskto	piprocmon_output/text1.pml			
File I	Edit Event	Filter	Tools	Options Help				
1 1 1		E .	• A 4	Always on	Tee			
			-					
Time	Process 7	are .	PID	Fort		FanA	Detail	
12:36:	#?Search	hdeer	2252	Highlight	Colors	SUCCESS	Cantrol: FSCTL_Q	
12.36:	E Search	indexer	2252			SUCCESS	Carbol: FSC1L_R_	
12:36:	#15earch	PCKeer	2252	Configure	Symbols	SUCCESS	Cantral: FSCTL_PC.	
12.36.	 Sealor 	NEWHOS	20/2 /	Salart Cali		SUCCESS	Trivead ID: 2004	
12:36	California	EXE	2300	annes water		SUCCESS	Duesy Hande Teo	
12.36	E Carlos	EVE	2988	History De	ath.	SUCCESS	Query Hande Tag.	
12:35	Eclar	(Exc.	2968	Destring		SUCCESS	Desired Access: Q	
12.36	Eplow	DE	- 11	Proteing E	and	SUCCESS	Query: Name	
12.36:	Epplore	B	2010	Enable Rev	e Lossina	SUCCESS	Query: HandleTag	
12.36	Epion	3G v	2568	Line but	a sogging	SUCCESS.	Desired Access: N	
12.36:	California California	NEXE:	2968 (V Show Rest	Ived Network Addresses Chi+N	SUCCESS	Type: REG_SZ, Le	
12:36:	Epian	• DE	2568 (SUCCESS		
12.36:	Bolot	3GN	2968	Plac Pile Cr	fields and Langths	SUCCESS		
12:36:	Epion	EXE	2568 (Hex Proces	a and Thread IDs	SUCCESS	Query: Name	
12.36:.	- Diplore	SIGN	2968	An A M	100010.0.0.100	SUCCESS	Query: HandleTag	
12:36:	Diplore	EXE	2368	riegulueryfwy	HKEU/Software/Classes	SUCCESS	Query: Handle Leg	
12.36.	20008	EVE -	2968	Hegupenney	HKLU-Software-Classes (print/openinitring)os	NAME NOT FOUND	Desired Access: R.	
12.30.	- Depore	EVE .	2300	regupentary	Insum pre upenwennogos	NAME NUT FUUNA	Deared Access PL.	
12.36	- Color	EVE .	2500	Barlympire	HIGH Schwarz Classes	0000000	Overs Hende Ten	
12:36	Delve	ENE	2588	Ban Lander	WT10 Schume Contract	SUPPESS	Dues HandeTas	
12.36	finites	DE.	2568	BanDoanKey	HICLD Software Classes Software Merson West	INVOIRT NAME NOT FOUND	Destrad Access R.	
12:36	Deive	EXE	2568	BagOpenKey	HICE R. Software/Microsoft/Windows/Current/Jenior	Deploye NAME NOT FOUR	Desired Access: R	
12:36	Epice	DE	2568	RegilizeryKey	HKCU/Software/Classes	SUCCESS	Query Name	
12:36:	Eclore	3G V	2968	RegQuenKey	HKEU/Software/Classes	SUCCESS	Query: HandleTag	
12:36	Epice	DE	2568	RegularyKey	HKCU/Software/Classes	SUCCESS	Query: HandleTag	
12:36:	Epiore	3G N	2968	RegOpenKey	HKCU\Software\Classes\.pnl	SUCCESS	Desired Access: R	
12:36:	Eplow	DE:	2988	RegQueryKey	HKCU/Software/Microsoft/Windows/Current/Ventor	VExplore SUCCESS	Query: Handle Tag	
12:36:	Epipe	3KE NE	2968	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion	NExplore SUCCESS	Desired Access: R.,	
12:36:	. Epice	r DE	2988	RegQueryKey	HKCU/Software/Microsoft/Windows/Current/Ventor	SUCCESS	Query: Handle Tag	
12:36:	- Dolore	SIG N	2968	RegOpenRey	HKEU/Software/Microsoft/Windows/Gunent/Version	NExplore_SUCCESS	Desired Access: R.,	
12.36	Epion	3G v	2968	RegQueryKey	HIGLU/Software/Microsoft/Windows/Current/Ventor	VExplore . SUCCESS	Query: Handle Tag	
12.36.	DEROT	BVE .	2966	Regipentay	HKCU-Software Microsoft Windows Current Version	VExplore_SUCCESS	Desired Access: Q	
12.36.	Distant	A DATE	2300	RegularyValue	HILLU-Software Microsoft Windows Current Versor	Voplee. SUCCESS	Type: PEIG_SZ, Le	
12.36.	abbox	EVE .	2200	Reg. cooney	HALO SOTWAR ONCODE OWNERS CONSTRUCTION	Colore CHOCESS		
12.36	Ective	EVE	2548	Bay Destay	1997 Th. Software, Microsoft Willowing of Instantiation	Deploy SIFTESS		
12.96	Enlos	EVE	2444	Bandauniter	Hill 10 Software Charges	SUCCESS	Ocean: Name	
12.35	Enlore	EXE	2988	BanQuenter	HICID Schwark Classes	SUCCESS	Duey HandeTan	
12:36	Eploy	DE	2988	BegQuertier	HKCU/Software/Classes	SUCCESS	Query Handle Tag.	
12:35:	Epplore	EXE :	2968	RegOpenKey	HKCU/Software/Classes/Applications/indepad.exe	NAME NOT FOUND	Desired Access: R	
12:36	Eplow	PDE	2988	RegOpenKey	HKCR'/Applications'/notepad area	SUCCESS	Destred Access: R.	
12:35:	Delore	SCE N	2968	RegDoseKey	HRCR'Applications' notepad eve	SUCCESS		
12:36	Epion	3G v	2568	RegiumyKey	HRCU/Software/Classes	SUCCESS	Query: Name	
12.36:	Delore	K EDE	2968	RegQueryKey	HKCU/Software/Classes	SUCCESS	Query: HandleTag	
12:36:	Delaw	* DE	2968 (RegiouryKay	HICU/Software/Classes	SUCCESS	Query: HandleTag	
12.36	Delore	3GN	2968	RegOpenKey	HKCU-Software/Classes Vapilications instepad eve	NAME NOT FOUND	Desired Access: R.	
12:36:	Epice	EDE	2568 (RegOpenKey	HICR'Applications (notepad ase	SUCCESS	Dealred Access: R.	
12.36:.	- Delore	EXE	2968	RegQueryRey	HRCR Applications instepad exe	SUCCESS	Query: Name	
12:36:	- Diplore	EXE	2368	riegGueryflay	HALH Veptications Violepad ase	SUCCESS	Query: Handle Tag	
1.5.15	A DOWN OF A DOWN	a la	798.0	AND DESCRIPTION OF A DE	and the second based as a second second second as a	a contract, including particular pre-	to second access? D	

4. Wählen Sie Ereignisse zur Erstellung von Bedrohungsprofilen und jede Sekunde generieren aus.

Process Monitor - C/Users\win7x64-new\Desktop\procmon_output\test1.pml								
File Ed	lit Event Filte	r Tools Options Help						
- 2 III		👄 A 🖧 🖹 🗛 🗖						
		A 🖶 ØA 🖬 🖬 🤞						
Time	Process Name	PID Operation	Path		Result	Detail		
12:36:	Searchindexer	2252 KeSystemContro	AC:		SUCCESS	Control: FSCTL_Q		
12:36	Searchindexer		NC:		SUCCESS	Control: FSCTL_R		
12:36	S Eachla Rea	ot Longing			SUCCESS	Control: FSCTL_R		
12:36	ES CHARGE DO	or coyying		SUCCESS	Thread ID: 2884			
12:36	Barrens M	with can penerate thread on	Allon events that can use		SUCCESS	Query: Name		
12:36	E the state	of all running applications at a r	equiar interval.		SUCCESS	Query: HandleTag		
12:36:	20				SUCCESS	Query: HandleTag		
12:36	📜 E 📝 Ger	verate thread profiling events			SUCCESS	Desired Access: Q		
12:36	E	(B. Every second			SUCCESS	Query: Name		
12:36:	1	 Every second 			SUCCESS	Query: Handle Tag		
12:36	E	Every 100 milliseconds			SUCCESS	Desired Access: M		
12:36:	- E			(Default)	SUCCESS	Type: REG_SZ, Le		
12:36			OK Cancel		SUCCESS			
12:36	H			1	SUCCESS	ô		
12.36	Explorer EXE	2355 Reguleykey	HNLU Calification Classes		SUCCESS	Query: Name		
12.36	Diblove, EVE	2300 ReguleryNey	HNLU Software leases		2000622	Guery: Handle Tag		
12.35	Explorer EXE	2565 Kineguuerykey	HNLU Software Classe	Country Design	SUCCESS	Query: Handle Lag		
12.05	Explorer EXE	2305 Regupenkey	HNLU (Software Classes (prin)	OpenwithProgram	NAME NOT FOUND	Desired Access: H		
12.39	Englow EVE	2900 Reguperivey	UNCLE Calculation (Classes)		CLICCECC	Oversi Name		
12.30	Englower EVE	2500 ReguleryNey	HNCO (Software Classes		SUCCESS	Query, Name		
12.00	Evolution EXE	2968 ReguleryNey	HIGHT Software Classes		SUCCESS	Query, Hande Tag		
12:36	European EXE	2988 ResConstant	HWT11 Software (Classes) Softw	The Company Manager (1999)	NAME NOT FOUND	Design Access B		
12:36	Euplow EXE	2958 BacOpenKey	HICTR\Software\Mcmadt\W/	dows\C mentVersion\Explore	NAME NOT FOUND	Desired Access: R		
12-36	Epolow EXE	2988 RecQueryKey	HKCU/Software/Classes		SUCCESS	Query: Name		
12:36	Evolover EXE	2988 RecQueryKey	HKCU/Software/Classes		SUCCESS	Query Hande Tao		
12:36	Explorer EXE	2988 RegQuer/Key	HKCU/Software/Classes		SUCCESS	Query Hande Tag		
12:36	Epplorer EXE	2988 RegOpenKey	HKCU\Software\Classes\.pml		SUCCESS	Desired Access: R		
12:36	Explorer EXE	2988 RegQueryKey	HKCU\Software\Mcrosoft\Wr	dows\CurrentVersion\Explore.	SUCCESS	Query: Handle Tag		
12:36:	Explorer EVE	2988 RegOpenKey	HKCU/Software/Mcrosoft/Wir	dows\CurrentVersion\Explore.	SUCCESS	Desired Access: R		
12:36	Eplorer EXE	2988 RegQueryKey	HKCU/Software/Mcrosoft/Wir	dows\CurrentVersion\Explore.	SUCCESS	Query: Handle Tag		
12:36	Explorer EXE	2988 RegOpenKey	HKCU\Software\Microsoft\Wir	dows/Current/Version/Explore.	SUCCESS	Desired Access: R		
12:36:	Explorer EXE	2988 KRegQueryKey	HKCU/Software/Microsoft/Wir	ndows\CurrentVersion\Explore.	SUCCESS	Query: HandleTag		
12:36	Eplorer EXE	2988 KegOpenKey	HKCU/Software/Microsoft/Win	dows\CurrentVersion\Explore.	SUCCESS	Desired Access: Q		
12:36	Explorer.EXE	2988 RegQueryValue	HKCU\Software\Microsoft\We	dows\CurrentVersion\Explore.	SUCCESS	Type: REG_SZ, Le		
12:36:	Epplorer.EXE	2988 RegCoseKey	HKCU/Software/Microsoft/Wir	ndows/Current/Version/Explore.	SUCCESS			
12:36	Biplover EXE	2988 KegCloseKey	HKCU/Software/Microsoft/Wir	dows/Current/Version/Explore.	SUCCESS			
12:36	Biplover EXE	2988 RepCoseKey	HKEU\Software\Mcrosoft\We	dows/Current/Version/Explore.	SUCCESS			
12:36	Biplover.EXE	2900 RegQueryKey	HKCU/Software/Classes		SUCCESS	Query: Name		
12:36	Explorer EXE	2388 RegQueryKey	HRCU Software Classes		SUCCESS	Query: Handle Tag		

5. Stellen Sie sicher, dass alle relevanten Filter in Procmon ausgewählt sind und Daten gesammelt werden.

6. Wenn Sie den Absturz nicht replizieren können, können Sie Windows mit dem Dienstprogramm NotMyFault64.exe, das Sie von erhalten können, zum Absturz bringen <u>https://live.sysinternals.com/files/</u>

Die folgenden Anweisungen zur Ausführung finden Sie hier: <u>https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump</u>

Process Presses - Crist	And the service of th	Charles with a set for			
A RE & RE CO.	A ALINE THE				
N N N N N N N N N N N N N N N N N N N	A & A & A				
Ins. Poper have	PD Geetter	Fat	Feed	Ownel	
23. Editer	100 British	C Proper RenCennet#10514Leeutra	140.001	Obs (2004)07.	
23. 10.00	The second secon	C Wegen Ner Can diff 111 fel av 19	1.0.20	Contraction 14	
2.2	The Paul Institute	TRUE School Street Western IF Constitution for	and set from	Consult Arrays P.	
238 KM #	170 Charlow Per	TRUM Scheme Human Western 17 Current annum Ste	NOT THE OWNER.	COMMENCED IN	
23. 14.00	The Charleston	NUM Selving Record Westwork? Contributors So	NOT THE	COntract Access 10.	
20.000	The second second	C Property Rend and Address of the State of the	100.000	Accession 12	
23. 810.00	100 Bulletin	C Proper Renders AP (111-4) and 10	9.41.221	(Ref. (5.000.00))	
23. Exter	170 Databarati	C Prepar RenCenn 487 711 Million 19	9,00215	idural sales fit.	
23. 19.00	The last working	C Wegen NerCennell* 11141-de la	S. States States 1	Department of the	
CO. Doces	The Part Section	TR.M. Schwarz (Rotand) Manhow 1712 (Institution) for	NAME OF TAXABLE	Constant Access 18	
23 EV.m	170 Charlester	TRUE Schwarz Human Westwork? Current among Str.	AND NOT THE	COMMENTATIONS PL	
23.844	170 Prinandiandard	Proper Nerclass ART 1114Low 19	100.000	Access for 2	
State Street	The second second	Property Residence and Providence by	10000	State of Street of Street	
CR. Exten	The Balancement	Company Rendered and California and Ing	9.41.005	where water in	
CH. EXten	170 Balaan/Antonia	Crimpen NerCennikP (1014) average	\$ Aven (read	Dealer Tree 141	
23. 04.00	The State of the S	15. M Schware Human Weathers 17 Curter/Sensor-To-	NAME OF TAXABLE	Contract Access 1	
2.0.0	I IN CONTRACTOR	The M Advance Manual Mendow MP L apartments for	NAME OF TAXABLE	Contract Across 10	
Cit. Eldow	100 Million Carter	E Vegen Ner Gest All 11 Statues to	9.40 (99)	Accession in	
23. EA.m	110 Belandarder	Company Revolution and Traditional State	9,41,895	Accession in	
20.00	The second second	Proper Nerces and 1154 are by	100.000	the Avenue.	
20.000	The second	Proper fact and different d	1.0.00	Partiente Anno 1	Exception 1 (Stational Action)
Cit. Eldines	In American	Company New Carol Aller Indon do	9.40 (895)	Mag 1 (15) (16) 8	
Cit. Draw	110 Pulsenfie	Companitive Carol AMP Institute Automatic	NAME OF TAXABLE	Classe Arrest R.	
28. 19.44	The second second	Wagan NerCast JAP Balls B	9.0.00	THE R. LEWIS	er daarnaals had haar al beeking
20.000	in a second	Company Net Land All Trans &	9.42 (99)	Sectoria V.	Condensative Condens Condensative Condensative Cond Condensative Condensative Condensative Condensative Condensative Co
Cit. Extran	100 Aureorfedrage	C Proper Net Cash 400" Instructs	0.00895	One 101500.8	The Same of a real of the state of the state of the state
State Street	110 Manuthman	E Proper Ren Jaco AM 111 Acres by	9.00995	Ward ages in	Hardward C. Colomba C. Martin and Society
20.000	No. Barbarbar	 Proper Ner-Case AP (11) Million 19 Million Research 10 (11) Million 19 	and other states	Construction in	
10.000	110 Automation	visited in the second strategy of Complement In-	water right when	Contract Across 16	TO THE REPORT OF A STATE STATE AND A STATE
Cit. Exten	110 Peptientes	HEALD SHOW (Renard Westwork) Commission (In-	And HER FOR	Classe Arrest R.	HAR HER HISP HE CHEL Televisia (Televis
28.844	100 Blanchardert	C Vegan Re/Ceci JMP 7118 at on he	0.03995	Accelerities 21.	at the same is its to be a series of the same serie
10.000	The second second	Compare New Card and Trans Areas in	0.0000	Other Division in which the	CONT - ARCHINE
CO. Color	100 Advantitionals	C Proper RenCent diff (1) Returns Inc.	0.0088	internal matter line.	
U.M. Kirken	100 Billion/Writers	2 Proper Net/Cent AM 711 Ref: and he	BURNER DARWE	Date Inc 15	In metacommetal information devices provide the processing of the procesing of the processing of the processing of the processing of th
10.00	The Payments	HEAD OF A CONTRACT	And the state	COMPACTACION P.	(in the entropy of the first of the entropy of the first operation of the first operation of the entropy of the first operation.
10.000	10 Parlantin	HEAL Information of Managers of Company and Information	and out that	Contract Across 18.	
10. E. M. au	100 milamberiet	C Propert RenCent (087-010 etcase by	9.400818	Acceleration 20.	Epsteen sate hit has been been a stranged at the set of
U.S. Erland	100 Mancharderi	C Prepar Rel Cash 489-718 at sea ba	0.00891	Acatella 3.	
10.000	DO BONNES	C Proyen Ner Carrister (151) at sea by	B. COMP.	One Distance.	
10.000	100 Manufactures	C Proper Rev Cent (647-117 all use her	BANKA DATES	Castor Tray 14	\
U.M. Kirkan	100 Charlestin	HEM Schwart Renault Westment If Constrianters Ter-	NOT FOR	O'Destrait Access (R)	N N
Contraction of the local division of the loc	100 Charlester	HEM School Human Western W Constitution Str.	NEW YOF YORK	O'Cashal Arras R.	1
10.00	100 million internet	Concern Resident all the second	B.CO.T.	destanting 10	\ \
10. E. M. au	100 Allemberiet	C Propert Ren Carol and Cold and any her	0.0000	Access for 31	1
1236. El-Manuel	100 Advanta	C Proper RenCennatif* (15.8 all ren ha	0.00010	Obs 2008.01	N N
Co. Column	100 Charlestonge	C Prepar Ner Carristen 151 di strate ha	9.6089	Wang Captor Te.	
10.00	100 Charlentin	NEW Advancement of the lot of the second sec	west out their	Classed Acres 18	\ \
218 B. W. mar	100 Charles No.	HEM Selected Human Windows W Conservationary Str.	And HET FOR	COntrol Arrest R.	1
1238	100 Challentin	HEM Selecter Human Western 10" Contributors Ton	NUMBER	Control Arrest PL	1
Co. Chan	170 Million Chardeni	C Prepare New Card (MRP) 75 T all des has	P.0.01	Rented to 2.	
2.2	THE BURNING	C Wagner Rev Card diffy 75 Public and Inc.	2.0.20	Other Division	
UN. Bestehlung	153 Coupling	C Proper Cata Villaget Officiale Tools tools cont	Next Hor Your	COnstant Access 10.	
C.B. Evenerate	200 Challensee	- R_M	PLOCEN1	Gary Arrite Inc.	
C.S. Congression	CONTRACTOR OF THE	ALL	P.40.001	Cashel Arises P.	
V.M. Burgersen	(10) Challender	HE M STATE WAT AND ADDITION AND	BUTTER TOO IN	and of some	
23. Compression	200 Challentation	NUMBER OF TRAFF ASSAULT ASSAULT ASSAULT ASSAULT	1.0.01	Tax PELSE in	
CH. Burgers and	200 Charles	NEW COTTAINS AND ADDICTION	P.00211		
Contraction and	CHI Charles	IN MARKED AND ADDRESS AND	P.0.00	Conv. Randa Tag.	
C.M. B. Longeroux and	(10) Challenting	THE MOST NAME ADDRESS ADDRESS ADDRESS	3.0.00	Greek Tot Same	
CH. Compression	200 Challenbert	HEALING FROM AND ADDIVING NO.	BUTTER TOO IN		
CH. Despresses	200 Challent das	NEW SOFTWARE ASSAULT ASSAULT ASSAULT	1.0.20	Tax PELSE In	
2 M	Contraction of the local distance	HOW NO WAS NOT NEED CASE	10.00		
Analog 338,333 of 452,451	0.000 /PG 8	and by Critical with the number of process and	al holigesi		
-					

7. Zerbrechen Sie den Computer.

8. Starten Sie den Computer im abgesicherten Modus, und sammeln Sie manuell **Procmon.pmb** und **MEMORY.DMP**, beide Dateien befinden sich unter C:\Windows folder. Diese Dateien sind für das Cisco TAC freizugeben.

Computer	 Local Disk (C:) Win 	dows 🕈	* <mark>19</mark>	Search Windows		
Organize 👻 📄 Open 👻	New folder				≣ • 🗖	
🔆 Favorites	Name +		Date modified	Туре	Size	
	explorer.exe		11/21/2010 4:24 AM	Application	2,805 KB	
libraries	fveupdate.exe		7/14/2009 3:39 AM	Application	15 KB	
Documents	HelpPane.exe		6/2/2017 10:10 AM	Application Application	717 KB	
A Music	👔 hh.exe		4/18/2018 5:41 PM		17 KB	
Pictures	IE11_main.log		1/30/2018 3:52 PM	Text Document	14 KB	
Videos	MEMORY.DMP		1/6/2020 12:41 PM	DMP File	331,914 KB	
	mib.bin		7/14/2009 1:06 AM	BIN File	43 KB	
Computer	msdfmap.ini		6/10/2009 10:36 PM	Configuration sett	2 KB	
Local Disk (C:)	notepad.exe		7/9/2015 7:57 PM	Application	189 KB	
CD Drive (D:)	ntbtlog.txt		1/6/2020 12:41 PM	Text Document	83 KB	
Shared Folders (\\vn	PFRO.log		1/6/2020 12:30 PM	Text Document	576 KB	
	Procmon.pmb		1/6/2020 12:41 PM	PMB File	320,740 KB	
🗣 Network	ProfessionalN.xml		6/10/2009 10:30 PM	XML Document	53 KB	
	💣 regedit.exe	Type: XML Document	:39 AM	Application	417 KB	
	setupact.log	Size: 52.3 KB	30 PM	Text Document	29 KB	
	setuperr.log	Date modified. 0/10/20	7/14/2009 6:56 AM	Text Document	0 KB	
	splwow64.exe		11/21/2010 4:24 AM	Application	66 KB	
	StarterN.xml		6/10/2009 10:31 PM	XML Document	48 KB	

7. Wenn Sie in der Lage sind, es im "normalen Modus" zu starten, wenn die PMB-Dateien im C:\Windows folder generiert werden, dann, wenn Sie ProcMon wieder starten, werden Sie die folgenden Protokolle sehen. Anschließend können Sie die Ereignisse erneut speichern, indem Sie auf die Schaltfläche Speichern klicken.





_
Genet

🔰 Process Monitor - Sysi	internals: www.sysinternals.	com		
File Edit Event Filter	Tools Options Help			
📽 🖬 🔌 🕸 🖾 🛛	🗢 🛆 🔁 🖻 🛤 🖣			
Time Process Name	PID Operation	Path	Result	Detail
12:41: Fames exe	292 🧟 Process Start		SUCCESS	Parent PID: 4, Com
2.41: Famas exe	292 ar Thread Create		SUCCESS	Thread ID: 295
2.41: Tames exe	292 ar Load Image	C:\Windows\System32\amss.exe	SUCCESS	Image Base: 0x479
2.41: Pamas exe	292 ar Load Image	C:\Wndows\System32vitdl.dl	SUCCESS	Image Base: 0x779
241: Pamas exe	292 RegOpenKey	HKLM\Software\Morosoft\Windows NT\CurrentVersion\Ima	NAME NOT FOUN	D Desired Access: Q
41: Fames exe	292 RepOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R
2.41: Pamas exe	292 KegOpenKey	HKLM'System'CurrentControlSet'Control'Session Manager	SUCCESS	Desired Access: R
41 smss.exe	292 RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	ID Length: 1.024
41: E smss.exe	292 KRepQueryValue	HKLM'System'CurrentControlSet'Control'SESSION MANA	NAME NOT FOUN	ID Length: 1,024
41 smss.exe	292 RepCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	
41: Pamas exe	292 CreateFile	C:\Windows	SUCCESS	Desired Access: E
41 Smss.exe	292 ReadFile	C:\Windows\System32\amsa.exe	SUCCESS	Offset: 74,752, Len
41: Pamas exe	292 🛃 ReadFile	C:\Windows\System32\amss.exe	SUCCESS	Offset: 1,024, Long
41 Smss.exe	292 ReadFile	C:\Wndows\System32\amsa.exe	SUCCESS	Offset: 107,008, Le
41: Resmos.exe	292 MeadFie	C:\Windows\System32\amss.exe	SUCCESS	Offset: 104,448, Le
41 smss.exe	292 Strand Create		SUCCESS	Thread ID: 300
41: Romas exe	292 ReadFile	C:\Windows\System32\amss.exe	SUCCESS	Offse Offset: 104,448
41 smss.exe	292 ReadFile	C:\\Windows\System32\amsa.exe	SUCCESS	Offse Length: 2,560
41: Ersmas exe	292 KegOpenKey	HKLM'.System\CurrentControlSet\Control\MinINT	REPARSE	Desi L/O Rags: Non-cached, Paging L/O, Synchronous Paging L/O
41: Famos exe	292 KegOpenKey	HKLM'System/CurrentControlSet/Control/MniNT	NAME NOT FOUN	D Desi Priority: Normal
41: Pamas exe	292 KegOpenKey	HKLM'.System'CurrentControlSet'Control'Session Manager\.	REPARSE	Desired Access: Al
41: I smss.exe	292 KegOpenKey	HKLM'System'CurrentControlSet'Control'Session Manager\	SUCCESS	Desired Access: Al
41: Pamas exe	292 RegDeleteValue	HKLM'System/CurrentControlSet'Control'SESSION MANA	NAME NOT FOUN	0
41: Pames exe	292 RepSetValue	HKLM'System/CurrentControlSet/Control/SESSION MANA	SUCCESS	Type: REG_SZ, Le
41: Pamas exe	292 KegOpenKey	HKLM'System'CurrentControlSet'Control'Session Manager	REPARSE	Desired Access: R
41: I amos exe	292 KegOpenKey	HKLM'System'CurrentControlSet'Control'Session Manager	SUCCESS	Desired Access: R
41: Famas exe	292 RepQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	Type: REG_DWO
41: Internet exe	292 RegQueryValue	HKLM'System'CurrentControlSet'Control'SESSION MANA	SUCCESS	Type: REG_MULT
41: Stres exe	292 RepQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	Type: REG_MULT
41: Elamos exe	292 RegQueryValue	HKLM'System'CurrentControlSet'Control'SESSION MANA	SUCCESS	Type: REG_MULT
41 Stres exe	292 RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	ID Length: 4,094
41: Image and a second	292 RegQueryValue	HKLM System CurrentControlSet Control SESSION MANA	SUCCESS	Type: REG_DWO
41: Stres exe	292 RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	D Length: 4,094
41: ense exe	232 RegQueryValue	HKLM System CurrentControlSet Control SESSION MANA	NAME NOT FOUN	D Length: 4,094
41 Smiss.exe	252 ReguleryValue	HKLM System CurrentControlSet Control SESSION MANA.	NAME NOT FOUN	D Length: 4,094
41: erismes.exe	232 PiegQueryVaue	HKLM System CurrentControlSet Control SESSION MANA	SUCCESS	Type: NEG_MULT
41. Smiss.exe	252 RegOpenkey	HKLM System CurrentControlSet Control SESSION MANA.	SUCCESS	Desred Access: M
41:	202 Peguleyiaue	HALM System Current Control SESSION MANA.	SUCCESS	Type: NEG_MULT
41 Smiss.exe	252 Reguleyvaue	HKLM System CurrentControlSet Control SESSION MANA.	NAME NOT FOUN	U Length: 4,094
41 Promosieve	202 Reguleyvaue	HALM System Current on book Control (SESSION MANA	50006555	Type: HEG_HOLT
41 Smos.exe	252 Reguesse value	HKLM System Current one of the Control SESSION MANA.	SUCCESS	
41	202 Preguoseney	HALM System Current on book Control SESSION MANA.	2000623	Desired Assess M
41. Bisnes exe	252 Regupenkey	HALM System CurrentControlSet Control SESSION MANA.	SUCCESS	Leared Access: M
41 8 9000 000	292 Performitiate	HVI M Sustan Control Control Section (Control Control	SINCESS	Index 1 Name M
41 Smaa cos	292 RecEnceValue	IN M Suter Control Set Control SECON MANA.	SUCCESS	Index 3 Name M
A1 Brends and	202 Pastin allala	LVI M Cutan Cutat Cutan Sat Cutan Control Second MANA	CINCERS	Index 2 Name Of
di amos exe	202 Progenum value	HALM Gyster Curren Control State Control SECTION MANA.	CUCCESS	Index 4 Name 8
A1 Press eve	292 ResEnceValue	HALM System Cutter Control Set Control SESSION MANA.	0000633	Index 5 Name 11
41	202 Peoperunivaue	HALM Gyster Current Control Set Control (CECCOM MANA	NO MODE ENTER	Index: 6 Lanoth: 4
A1 Brance and	292 Regenull value	HVI M Sustan Control Sat Control SESSION MANA	SUCCESS	
A1: Dames and	292 PagCostNey	HALM Gyster Curren Control Set Control SECTION MANA.	SUCCESS	Daried Access M
supercise	EVE Prepuperkey	When change council and association water	3000633	Veneto Povena. Pl