## 시작 시 AMP 문제를 해결하기 위해 ProcMon 로 그를 수집하는 방법

## 목차

<u>소개</u> <u>절차:</u>

## 소개

시스템 관리자는 프로세스 모니터(procmon.exe)를 사용하여 컴퓨터 시작 프로세스 중에 FireAMP 커넥터 환경이 중단되는지 여부를 확인하는 자세한 로그를 얻을 수 있습니다.이러한 로그는 Cisco TAC에서 이러한 문제를 해결하기 위해 요청합니다.Process Monitor는 여기에서 도움이 되는 무료 유틸리티입니다.이 파일은 https://docs.microsoft.com/en-us/sysinternals/downloads/procmon에서 무료로 다운로드할 수 있습니다.

이 문서에서는 시스템 부팅 프로세스 중에 문제가 발생할 경우(부팅 시 BSOD를 생성하는 중임) ProcMon 로그 및 메모리 덤프를 수집하는 방법에 대해 설명합니다. 이러한 로그는 부팅 중에 발생 하는 시스템 이벤트를 캡처하는 데 필요합니다.

## 절차:

1. 문제가 쉽게 재현될 수 있도록 시험장치를 설정하는 방법

2. 관리자로 ProcMon 도구를 다운로드하여 실행합니다.File(**파일) -> Process Monitor Backing** Files(프로세스 모니터 백업 파일)로 이동하고 경로를 선택합니다.

Precess Meniter - C//D	sani/win7464-nau/Deakte	p/process_output/text_ped								
Did tvert filter	Tools Cysters Help									
	20 Orantos	Tublic Links		free d	Dated					
Searchindear     Searchindear     Searchindear     Searchindear     Searchindear     Searchineise     Searchineise	232 A Ma System Care 232 A Ma System Care 233 A System Care 234 D Provid Care 234 D Provid Care 234 D Reg Care Nov 234 D Reg Care Nov	HC H		AUCCESS AUCCESS AUCCESS AUCCESS AUCCESS AUCCESS AUCCESS AUCCESS AUCCESS AUCCESS	Carted FSC Corted FSC Carted FSC Thread D: 2 Guary Name Guary Hand Centred Acce Guary Name	L.G. L.R. M4 Fag Fag				
Process Manite	r Becking Film									
These backing file of	Aljects are being used to sto	re event data:								
i. Nave		Event Court	Event Bytes Para	ing Events	Process Gourt	Octoney Court	keen Count	Connelled		
所 利品 起品 起品 起品 一品 一品 一品 一品 一品 一品 一品 一品 一品 一										
6. Process Hartler ce 6	natore events in virtual mer	nary (inited by the system corest ini	C), or in a file you specify	protect by free o	fek spece). Which	de you prefer?				
O Use vitual new	try (0,7024 analohis)									
Car fa named	C. Sarripit 7d Ann	"Desites/process_subpd"(set 1.prd								-
Pro/Hanibadi E. 4	Ph. () () (r/m panding)									Garcel
N Spine DE N Spine DE N Spine DE	2383 RegCoarKey 2383 RegCoarKey 2383 RegCoarKey 2383 RegCoartier	WCR Applications' vehicual and WCR Applications' vehicual and WCR Applications' vehicual and		RUCCESS RUCCESS	Deared Acce Guary Name	# Ř.				

3. Process Tool에서 Options(옵션) -> Enable Boot Logging(부팅 로깅 활성화)으로 이동합니다.

🗳 Pr	DORES 1	Monitor	r - C:\Uh	ani/wini	7x64-rww\Deskto	piprocmon_output/text1.pml					
File	Edit	Event	Riter	Tools	Options Help						
L and A			C 1.4		41						
		< 18	67   Y	7 🗛 🤉	Always on	1 op					
Time	. Po	cere Na		PID	Fort			Rend	Detail		
12.36:	. 115	earthin	deser	2252	Market and			SUCCESS	Cantrol: F	SCTL Q.	
12.36:		earth in	deser	2252	regeogen	Loons_		SUCCESS	Cantrol: F	SCTL R.	
12:36:	175	earchity	deser	2252	Configure	Sumbola		SUCCESS	Cantrol: F.	SCTL_R.	
12.36:		earch R	terHos	2072	congae			SUCCESS	Thread ID	2884	
12:36:	- <u>_</u> E	ispicarer i	DE	2988 (	Select Col	amna		SUCCESS	Query: Na	are a	
12:36:	- 62	apiorer i	EXE	2968	10.0			SUCCESS	Query: Ha	andleTag	
12:36:	- Gat	1000	XE	2968 (	Platory De	pth		SUCCESS	Query: Ha	inde Tag	
12.36:		SCROLEN	-	2968	Profiling E	vente		SUCCESS	Desired A	COMMENT OF T	
12.36	- 98	SCROWE !	EXE .	2				SUCCESS	Guery: Na		
12.06	- 23	ACCOUNT OF		2900	Enable Bo	et Logging		9000E99	Guery: He	snole rag	
12.36	- X.	locitorer i	CARL CONT	2200				SUPPERE	Date: DD	CCR88 PL.	
12.36		and states in	EVE .	2488	✓ Show Rest	ilved Network Addresses Chri-N		SUCCESS	19896.1989	0_36.W.	
12.36	1	with the l	FXE	2548	Hex File O	firets and Lengths		SUCCESS			
12:36	The second	with the l	EXE	2588		17.00		SUCCESS	Query Ne	1.1	
12.35	1	Sellow P	EXE	2968	Pies Proce	is and Thread ID's		SUCCESS	Query Ha	ordeTag	
12:36		inderer l	DE	2568	RegQueryKey	HKEU/Software/Classes		SUCCESS	Query: He	ande Teg.	
12:36:		Spiorer B	EXE:	2968	RegOpenKey	HKCU\Software\Classes\.pnf\OpenWithPro	oids	NAME NOT FOUND	Desired A	coess: R.	
12:36:	📬 E	ipiorer l	DE	2988	RegOpenKey	HKCR\pm\OpenWithProgide		NAME NOT FOUND	Desired A	CORRER R.	
12:35:	. 👍	Spiorer B	EXE	2968	RegQueryKey	HKCU/Software/Classes		SUCCESS	Query: Na	ene	
12:36:	📬 E	ipiore l	DE	2568	RegiumyKey	HKCU/Software/Cleases		SUCCESS	Query: He	ndeTeg	
12.36:	油	lipiorer l	EXE:	2968	RegQueryKey	HKCU//Software/Classes		SUCCESS	Query: Ha	andleTag	
12:36	- 🦕	iquiorer l	DE	2568 (	RegOpenKey	HICU/Software/Classes/Software/Microsoft	Windows\Curr	NAME NOT FOUND	Destred A	COMP. R.	
12.36:	🏔	spiorer I	EXE:	2968	RegOpenKey	HKCR\Software\Microsoft\Windows\Current	Version (Explore.	NAME NOT FOUND	Desired A	ccess: R.,	
12:36	- 📬	opiorer l	EXE:	2568 (	RegiouryKey	HICU/Software/Classes		SUCCESS	Query: Na	174	
12.36:	- 🚘	spiner i	DE	2968	RegQueryKey	HKEU/Software/Classes		SUCCESS	Query: Ha	andleTag	
12:36:	- 94	opiorer 1	EXE	2568	RegularyRay	HREU/Software/Classes		SUCCESS	Query: Ha	ande Tag	
12.36:	- 25	SCROLET B	EXE	2968	HegOpenkey	HKCU/Software/Classes/pnil	10 - NT - 1	SUCCESS	Desired A	coess: R	
12:36:	- 98	againer i	EAE	2300	rieguueytay	HALU/Software Wichsite (Windows (Luners)	Werson Voolore	SUCCESS	Cuery: Ha	indie lag	
12.36		spore i	EAC	2300	Regulation	HALO SOTWATE MICROSOL OWNDOWS KUPPET	Version Explore.	3000535	Desired A	COESS PL.	
12:30	122	Sectorer 1	CARC .	2300	BagloonKey	HALL CONVERT ORDER OF PERMIT	Manion Explore	SILLESS	Desired &	cost D	
12.36		indexes [	DIE .	2568	Bandumiter	HICLD Software Microard (Wedners) Correct	Manatara Evaluation	SUCCESS	Query He	ande Ten	
12:36	1	leiner I	DE	2968	BagOpanKey	HIC: ID: Software/Microsoft/Windows/Current	Version' Explore	SUCCESS	Desired A	COMMY D	
12:36		applorar I	Dat	2568	RegQueryValue	HICLUSoftware/Microanh/Windows/Current	Version Lipping	SUCCESS	Type: RD	0.5Z.Le	
12:36	100	lickow/	EXE	2968	RegCloseKey	HK2U/Software/Microsoft/Windows/Current	Version' Explore	SUCCESS		all a second	
12:36	. 📬 E	ipiow l	DIE	2568	RegCloseKey	HKCU/Software/Microsoft/Windows/Current	Version Explore	SUCCESS			
12.36:	🚍 E	Spiorer B	BE	2968	RegCloseKey	HKEU/Software/Microsoft/Windows/Current	Version' Explore.	SUCCESS			
12:36:	📬 E	ipion i	DE	2568	RegQueryKey	HKEU/Software/Classes		SUCCESS	Query: Na	AT 4	
12:36:	🕞 E	Siplarer B	EXE	2968	RegQueryKey	HKEU/Software/Classes		SUCCESS	Query: Ha	andleTag	
12:36:	📷 E	içilərər İ	DE	2988 (	RegQueryKey	HREU/Software/Classes		SUCCESS	Query: He	ndeTeg	
12:35:		Spiorer B	EXE	2968	RegOpenKey	HRCU/Software/Classes/Applications/inotep	ad eve	NAME NOT FOUND	Desired A	ccess: R	
12:36	- 🖓 E	içilarır i	ÐE	2968 (	RegOpenKey	HKCR\Applications\notepad ass		SUCCESS	Desired A	CORRER R.	
12.36	- 04	SCIONER	3K	2968 (	RegCloseKey	HRCR Applications Instepad eve		SUCCESS			
12.36	- 98	appearse i	EXE	2968	Regularyfay	HALU/Software/Classes		SUCCESS	Guery: Na		
12.35		ACCOUNT N	344	2966	Hegaveykey	HALU-Software Classes		SUCCESS	QURY: Ha	andle Tag	
12.35	1	ALC: NO.	CVC	2300	Bagalagy and	WWWWWWWWWWWWWWWWWWWWWWWWWWWWW	ad and	NUME NOT DOUBLE	Desired 1	contract.	
12.36		ADOR!	CVC	2900	Barloontey	HAL CHOOTHATE LIDESES VEDECALORS VIERD	00.000	SUCCESS	Cesred A	CCCSS R.	
12.36	12	ing a series of a	EVE:	2940	Barlantay	HIT TO Applications' unternal auto		SILLESS	Duese Ma	ALLER PL.	
12.96		interes (	E E	2988	Bandaumter	HILE R Applications Insterned ass		SUCCESS	Ocentry, No	ande Ten	
12.35	1	letine i	EVE:	2900	Plan Don Fer	UPTID Schurge/Theses/Linetershooten	when T days be	NAME NOT ON IND	Desired &	control D	

4. Generate threat profiling events(위협 프로파일링 이벤트 생성) 및 Every second를 선택합니다.

🎒 Proc	ess Monitor - C/	Users\win7x64-new\Desktop	p\procmon_output\test1.pm	1			
File Ed	fit Event Filte	r Tools Options Help					
-2 E		- A - A - A - A - A - A					
	1 2 8 21	A 🐨 🗛 🖉 🖬 🖬					
Time	Process Name	PID Operation	Path		Result	Detail	
12:36	Searchindexer	2252 ReSystemContro	NC:		SUCCESS	Control: FSCTL_Q_	
12:36	Searchindexer		IC:		SUCCESS	Control: FSCTL_R	
12:36	S Cashle Day	at Looping		)	SUCCESS	Control: FSCTL_R	
12:36:	P.S. Chable bot	ot cogging			SUCCESS	Thread ID: 2884	
12:36	10 E		these seconds the barrels are		SUCCESS	Query: Name	
12:36	E the state	onitor can generate tryead pro	and ar interval		SUCCESS	Query: HandleTag	
12:36	Call Call		eyola meria.		SUCCESS	Query: Handle Tag	
12:36	Ger 🖉 Ger	erate thread profiling events			SUCCESS	Desired Access: Q	
12:36	E				SUCCESS	Query: Name	
12:36	<b>1</b>	Every second			SUCCESS	Query: Handle Tag	
12:36	E E	Every 100 milliseconds			SUCCESS	Desired Access: M	
12:36	E E	_		(Default)	SUCCESS	Type: REG_SZ, Le	
12:36	<b>6</b>		OK Cancel		SUCCESS		
12:36	<b>E</b>		-		SUCCESS		
12:36	Explorer EXE	2988 KRegQueryKey	HKCU/Saltrage/Classes		SUCCESS	Query: Name	
12:36	Eplorer EXE	2988 KRegQueryKey	HKCU/Software Wasses		SUCCESS	Query: HandleTag	
12:36	Eplorer EXE	2988 KRegQueryKey	HKCU/Software/Classe		SUCCESS	Query: HandleTag	
12:36	Explorer.EXE	2988 KRegOpenKey	HKCU/Software/Classes/pml/	OpenWithProgids	NAME NOT FOUND	Desired Access: R	
12:36	Epplorer EXE	2988 KegOpenKey	HKCR\pml\OpenWithProgids		NAME NOT FOUND	Desired Access: R	
12:36	Explorer EXE	2988 KRegQueryKey	HKCU\Software\Classes		SUCCESS	Query: Name	
12:36	Explorer EXE	2988 KRegQueryKey	HKCU\Software\Classes		SUCCESS	Query: HandleTag	
12:36	Epplorer EXE	2988 KRegQueryKey	HKCU/Software/Classes		SUCCESS	Query: Handle Tag	
12:36	Explorer EXE	2988 KRegOpenKey	HKCU\Software\Classes\Softv	rare \Mcrosoft \Windows \Curr	NAME NOT FOUND	Desired Access: R	
12:36	Explorer EXE	2988 KRegOpenKey	HKCR\Software\Mcrosoft\W/	ndows/Current/Version/Explore.	NAME NOT FOUND	Desired Access: R	
12:36	Diplorer EXE	2968 KegGueryKey	HKCU Software Classes		SUCCESS	Query: Name	
12.35	Explorer EXE	2966 RegQueryKey	HRLU/Software/Classes		SUCCESS	Query: Handle Tag	
12.35	Explorer EXE	2365 Kineguseykey	HALU/Software Classes		SUCCESS	Query: Handle Lag	
12.36	Diplorer EXE	2505 Regupenkey	HKLU/Software/Classes/pmi		SUCCESS	Desired Access: N	
12.36	Explorer EXE	2555 Kineguueykey	HKLU/Software/Microsoft/We	dows (Lurrent Version (Explore)	SUCCESS	Query: Handle Tag	
12.36	Explorer EXE	2966 Regupenkey	HALU Software Microsoft We	dows Current Version (Explore.	SUCCESS	Desired Access: R	
12.35	Diplover.EXE	2300 Regulation Ney	HINLU Software Vecrosoft / We	dows (Lutrent Version (Explore)	50002555	Query: Handle Lag	
12.35	Explorer EXE	2300 Regupenkey	HKLU (Software (Necrosoft / We	dows Current Version (Explore)	5000255	Desired Access: R	
12.35	EDDIOLAL EXE	2365 Reguleyney	HALU Software Microsoft / we	dows Current Version Explore.	3000633	Guery: Hande Lag	
12.30	Copierre EXE	2000 Photo includes	LWCLD Coltrainte Uncrosoft (Wer	down Current Version (2000)	SUCCESS	Tune: DEG_57_1-	
12.00	Evelow EVE	2500 Reguleyvalle	MACO (Software (Microsoft Were all) Microsoft Were	down Current Version (Explore)	CLOCESS	igge: hba_az, Le	
12.00	Englow EVE	2988 Regulatery	HIGHT IS Collection (Manager Manager Manag	down Content Version (Schore)	SUCCESS		
12:36	Europerer EVE	2900 Regulation	HWT17 Colturare Microsoft (We	volves current version (Coplane)	SUCCESS		
12-16-	Evolow EVE	2500 Backworkey	MICTIP Colturate Character	considererererererererererererererererererer	SUPPERE	Ourse Name	
12.36	Enjow EVE	2988 Real work	HIGHT IS Software Classes		SUCCESS	Query Handa Tan	
16.79	CODOR EXE	The state of the s	111110 COLUMN 0 COMPOSE			causely. Handle 18g	

5. 프로세스에서 모든 관련 필터를 선택하고 데이터를 수집해야 합니다.

6. 충돌을 복제할 수 없는 경우 NotMyFault64.exe 유틸리티를 사용하여 충돌 Windows를 강제로 실 행할 수 있습니다. <u>https://live.sysinternals.com/files/</u>

실행 방법에 대한 지침은 다음과 같습니다. <u>https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump</u>

	and the second	the second second second			
OR Over The	Yosh Options Tally				
A & A & A & A & A & A & A & A & A & A &	40 2 4				
- Procestere	PD Genter	Fat	Feed	Ownel	
Eldine .	100 Bulletin	Crimpen RenCennel#1011 All an Ing	9.0020	Ofer 2009-007.	
1 Marcola	170 Datablemate	C Vegen RenCennell* 215-Killering	1.0.210	WanaCeator Te.	
10.00	The Dary Bridging	C yhegen NerCass AM (1511-4) on ha	BURGH DUCK	Dedictive 151	
100.000	The second second	THE M DRIVEN PRIMARY PRIMARY IN COMPANY IN COMPANY INC.	and the state	COMPACT/COMPACT	
100	The second second	18 M Manual Manual Manual V Constantion To	100 100 100	Contract Actions 1	
1000	110 Advantage	1 August Revolution and 110 all low ba	2.01220	Accession 18	
a laterate	100 Bellandardett	C August RenCash and 11 feb are by	9.41 225	Access for 2	
1 M 40	100 Bulletin	C Prepar Renders AM 11 Sectors 10	9.00205	(Heg. (5.000.00)	
E.M. 40	170 Databarati	Crimpen RenCech 447-111-41-en 1g	9,00215	Wandowine Inc.	
1 VC 40	170 Balandaria	C Vegan Rendern ART 11 Tell ren ha	BURGE DATE:	Department 161	
10.00	The second second	18 M Selver House Street V Caretheory In	And the state	COMPACTORS N.	
	The second second	The Monte of Contract of Contract of Contractors for		COMPACT/COMPACT	
1000	The subscription	1 Annual Residence and 110 Advances in	241 100	Score in	
a laterate	100 Belling Agented	Company Rest and all \$12.5 do not be	B.41 (19)	Accessible 18	
E Martine	THE BANKIN	Company Residence and Publishers Inc.	9.41 225	Other Distances	
E Martine	100 Belanisterate	Companisher Carol AMP 111 Michael 10	9.00225	internet waters for	
E 101.000	170 Landerson	E Prepara Renda con Allen 11 fi ato ana taj	BUTTER DUTTE	Departments.	
10.00	The Section	18,9 Silver Road Shape If Caterbury In	And the Party of the	Contract Access 11	
10.00	The series	the other than a state of the s		And Acres 1.	
	International Action	A characteristic contract of the second seco	20.00	Support Access 14	
1000	ting and and a second	A change from any sight had at on he	The other states	Accession in the	
a lateral	Line Building	Company News Jack and The Public Street Street	10.00 000	The later of	
E Marian	100 Buckline	Proper NerCent All Install	9.41 225	Partiente Ina ile	
E Martine	100 Bucch	Proper NerCentral Press &	9.00815	Declaria Asse ()	Belances and an Utilization of Contract State
E Martine	100 Burnstefedrige	Proper Net George Methods &	9.00 895	18M 1875/W-8	CONTRACTOR OF CONT
1. Marcal	The second s	Companitive Case AMP Index In June	100710-007	Classif-Access P.	
1.00.00	100 Breath	Proper NerCest AM Interact	9.00895	the Allege .	instaurnajahid mashed beitrap
100.000	IN BOARTS	<ul> <li>Vegan Nerriaco all' tutos di val</li> </ul>	NAME OF TAXABLE	COMPARIANCE N.	The discount of the Particle Strength Str Strength Strength St Strength Strength
	The second second	Company New Carry and Training the	1000	State of the local division of the	The hand the start part of the start of the
	and the second second	Company Network and Party in	10000	and the second	Polana Saria) Mader in 7079-607
	The state line with the second	Company Real and April 12 Automatics	A PROPERTY.	Constanting 14	Have many aff. Or Have made Debt many declarate
1000	110 Charlestin	with M School (Reserved Westman 16) Comprisinger Ter-	sand out they	Constant Array R.	
all internet	110 Paging the	with M Schware Merseef. Westwork IT Comprises on The	NAME OF TAXABLE	Column Array R.	
E Martine	110 Paginette	HKM School Hensel Western W Commission In-	And showing the	Clanet Arrest R.	HAR HER II IF HA CHES,
E Martine	100 Blanchardert	C Propert RenCentral PC111 at case by	9,60,895	Accelerities 20.	20 (20 (202) 10 (202) 10 (202) 10 (202) 10 (202) 10 (202)
- E.M. 44	100 Blanchardert	C Vrigen Rei Ceci alle 118 et dei he	0.03995	Acute for 3.	Tribulat Different Different Different Different Different
- 500.00	INC BORNER	C Vegen RenCental Contact and Contact and the	0.43.000	one postation.	3 DEPUT 29.407.046.351 Kern free
	The second second	Compare New Jack and Control of the New York	A COLUMN TO A COLUMN	Contraction 14	Continuents and a buffet space discrimination of their interaction.
1022	100 Charlentin	of M Information of Manager VI Completence In-	sand out of the	Contract Income 18	
1000	110 Destautor	and M Information and Advances M Complement In-	and out they	Contrast Acres 18	Configuration (a find a mean device public between 10 a first backing for the contract optime 1 a structure
all information	100 PeakerHe	with M Schwart Menand Westman M Comprisioners In-	and relation	Classed Arrest R.	
1 Marcal	100 milambardett	C Prepare ResiGent all PCDD Interace by	9.0088	Accelerity 3.	Conference and find the acceleration of the product
Colores .	100 Bilanchardert	C Propert RenCent all P (151) all year by	0.00815	Acute In 3.	
100.00	IN ANY A	C Prepare RenCarol all PCD1 Renamble	1.0.001	One 2010AD	
1000	The supplements	C Propert RenCard and Cold all and the	PLACEPT	stand agen in	1
	The Dary Bridgers	A Property of the Case of the Case of the State of the St	and states	Contraction 14	1
100	THE PARTY NEWS	and in the set of the	and out of	Control Income in	1
10.00	110 Charlestin	out of Subsect Strengt Strengt WC countingers In-	and out the	Control Array 6	\
a de ser	100 million/heritest	C Property Rest Carol all PC 211 all una ha	P.ACTER	decate-line 20	1
<ul> <li>Manual</li> </ul>	100 Million Arrient	C Propert RenCennal#1018 all unches	<b>BLOOPIN</b>	Receiption 28.	1
<ul> <li>Marco</li> </ul>	100 Advin	C Proper RenCental#1018 at sector	PLOCENT	Ofer 2008.01	1
1 March 199	170 Campionate	C Propert RenCeccular/2018 at cescing	PLOCEN:	Ware/agin Te.	1
1.00.000	W Carylingers	2 Proper RenCennative 318 all and he	BUNDH DHOWL	Department 16	1
1000	The Pay Services	HE, M. Different Romand, Minutes VC Construment Ter-	And ACT YOR	Contrast Access 10	1
	The Part Section	on the second decade the second to compare the	and set for	Contract Access 10.	1
	The second	A design from the second second to be a second seco	B.CO.T.	Rent of the Party	1
10.00	1107 Albertheiter	Colorante Real And and Add 12.0 di ser la	2.0000	Respondence in	
al laterate	100 Advis	C Propert RenCard all Cold and Inc. Inc.	0.0000	(Net 25/80.00)	
Contrada and	153 Countie	C Proper Cate / West Officers Tests tests conf.	weet not now	Control Arrest R.	
<ul> <li>International</li> </ul>	200 Children free	HEN .	PLOCETT	Core Arritella	
<ul> <li>International</li> </ul>	200 Challenter	HEAL SOFTWARE ASSAULT ASSAULT ASSAULT	1000011	Change Access 10.	
a subscription and	200 Challenshe	HEAVING PROVIDE ADDRESS ADDRES ADDRESS ADDRESS br>ADDRESS ADDRESS br>ADDRESS ADDRESS	PLOCET	Grey NA Same	
100000000000000000000000000000000000000	CTT Children Auf	ALCO DO FRANCE ACCOUNT ACCOUNTS	POWER NOO BY	A	
Conditional data	CRI Philosofielas	ALCONTRACT ACCOUNT ACCOUNTINGING	PLOCEIN	Tax PELSE in	
and the second second	THE R. LOW CO.	THE REPORT OF THE PARTY OF THE	100.00	her subhr	
Company of the	THE PROPERTY.	THE R. LEWIS CO., NAMES AND ADDRESS OF TAXABLE	The state of the s	Canada Array 1	
a second second	THE PROPERTY.	THE MOST PARTY AND ADDRESS AND	2.0122	Deep NA Long	
Compression and	(10 Challenbert	HEAL STATING AND ADDIVINED	BUTTEN TOO IN		
No. of Concession, name	200 Challentrates	INCOMENTATION AND ADDRESS OF TAXABLE	PLOCEN	Tax PELSE In	
		and he shares and an an another that as	the second second		

7. 기계를 망가뜨리는 행위

8. 시스템을 안전 모드로 부팅하고 Procmon**.pmb** 및 **MEMORY.DMP를** 수동으로 수집합니다. 두 파 일은 모두 C:\Windows folder에 있습니다.이러한 파일은 Cisco TAC와 공유됩니다.

Computer	▼ Local Disk (C:) ▼ Win	dows 🔻	× (7)	Search Windows		
Organize • Open •	New folder				H • 0	
★ Favorites	Name A		Date modified	Type	Size	
<ul> <li>Libraries</li> <li>Documents</li> <li>Music</li> <li>Pictures</li> </ul>	<ul> <li>fveupdate.exe</li> <li>HelpPane.exe</li> <li>hh.exe</li> <li>IE11_main.log</li> </ul>		7/14/2009 3:39 AM 6/2/2017 10:10 AM 4/18/2018 5:41 PM 1/30/2018 3:52 PM	Application Application Application Text Document	15 KB 717 KB 17 KB 14 KB	
Computer	MEMORY.DMP     mib.bin     msdfmap.ini     notepad.exe		1/6/2020 12:41 PM 7/14/2009 1:06 AM 6/10/2009 10:36 PM 7/9/2015 7:57 PM	DMP File BIN File Configuration sett Application	331,914 KB 43 KB 2 KB 189 KB	
CD Drive (D:) Shared Folders (\\vn	ntbtlog.txt     PFRO.log     Procmon.pmb		1/6/2020 12:41 PM 1/6/2020 12:30 PM 1/6/2020 12:41 PM	Text Document Text Document PMB File	83 KB 576 KB 320,740 KB	
🗣 Network	ProfessionalN.xml regedit.exe setupact.log setuperr.log splwow64.exe StarterN.xml	Type: XML Document Size: 52.3 KB Date modified: 6/10/20	6/10/2009 10:30 PM :39 AM :30 PM :30 PM :30 PM :30 PM :30 PM :30 PM :30 PM :31 PM :31 PM :32 PM :32 PM :33 PM :30 PM :31 PM :31 PM :31 PM :32 PM :32 PM :33 PM :30	XML Document Application Text Document Text Document Application XML Document	53 KB 417 KB 29 KB 0 KB 66 KB 48 KB	

7. 선택적으로, C:\Windows folder폴더에 PMB 파일이 생성된 경우 "일반 모드"로 부팅할 수 있는 경 우 ProcMon을 다시 시작하면 다음 로그가 표시됩니다.여기에서 Save(저장) 버튼을 클릭하여 이벤 트를 다시 저장할 수 있습니다.

Process Monitor - Sylintemails: www.splintemail.com			
File Edit Event Filter Tools Options Help			
Image: State (State (State))			
The Research Market Real Provider And	 Part of		



_
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 E Load Image	C:\Windows\System32\amss.exe	SUCCESS	Image Base: 0x479
2.41: Pamas exe	292 ar Load Image	C:\Windows\System32vitdl.dll	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 KRegQueryValue	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 RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	
41: Pamas exe	292 Koreate File	C://Windows	SUCCESS	Desired Access: E
41 Smss.exe	292 ReadFile	C:\\Windows\System32\amas.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:\Windows\System32\amsa.exe	SUCCESS	Offset: 107,008, Le
41: Resmos.exe	292 MeadFie	C:\Windows\System32\amas.exe	SUCCESS	Offset: 104,448, Le
41 smss.exe	292 See Thread Create		SUCCESS	Thread ID: 300
41: Romas exe	292 ReadFile	C:\Windows\System32\amas.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 RegOpenKey	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 KRegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	0
41: Pamos 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 KRepQueryValue	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 RegQueryValue	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: Elamos exe	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: emes.exe	232 RegQueryValue	HKLM System/CurrentControlSet/Control/SESSION MANA	NAME NOT FOUN	D Length: 4,094
41 Smiss.exe	232 ReguleryValue	HKLM System CurrentControlSet Control SESSION MANA.	NAME NOT FOUN	D Length: 4,094
41: erismes.exe	232 ReguleryValue	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 Preguleyvaue	HKLM 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 Preguleyvaue	HKLM System Current on the Control SESSION MANA.	50006555	Type: HEG_HOLT
41 Smos.exe	252 Repuese value	HKLM (System CurrentControlSet Control (SESSION MANA	SUCCESS	
41	202 Preguoseney	HALM System Current on book Control SESSION MANA.	2000622	Desired Assess M
41	202 Reguperkey	INCM Gystem Current Control Set Control SESSION MANA.	CUCCESS	Index O Name A
A1 Brance and	202 PasEn militar	LVI M Custon Custon Custon Caston Control COCCOM MANA	0000633	Index 5 Name M
41	292 RecEnceValue	HALM CYREM LUTERLOTED SELLOTED SELLOTED SESSION MANA	SUCCESS	Index 3 Name M
A1 Brends and	292 ResEnceValue	LVI M Crater Crater Control Set Control (CCCCCA) MANA	CLUCEDO	Index 3 Name Of
di amos exe	202 Regenunivaue	HALM Gyster Lutter Lore Dist Lore Disc 53504 MANA.	CUCCESS	Index 4 Name 8
A1 Press eve	292 ResEnceValue	LIVE ME System Control Set Control SESSION MANA	0000633	Index 5 Name 11
41	202 Progenum value	HALM Gyster LUTERLOTED SR. LOTED SESSION MANA.	NO MODE ENTER	Index: 6 Lanoth: 4
A1 Brance and	292 Regenuit value	HALM System Control Set Control SESSION MANA.	SUCCESS	
A1: Dames and	292 ResOurceMay	HIGH Grand Control Control Control CERCICAL MARKA	CUCCESS	Daried Access M
supercise	eve meguperney	INTER OVER COLORDON FORD SE22YON WARK.	3000633	VEHEV /VVEH. P