# فاشكتسال ProcMon تالجس عيمجت ةيفيك ليغشتلا ءدب دنع امحالصإو AMP ءاطخأ

تايوتحملا

<u>ةمدقملا</u> عارج<u>إلا</u>:

## ەمدقملا

ةبقارم مادختساب ةيليصفت تالجس ىلع لوصحلا ىلإ جاتحت دق ،ماظن لوؤسم كتفصب ءانثأ قيلعت ةيلمعل ضرعت دق FireAMP لصوم ناك اذا ام ديدحتل (procmon.exe) ةيلمعلا درمع دوم ناك اذا ام ديدحتل (cisco TAC in order to درمع اذه يرت عدب تي معليا معليا المعنيي المعليا التي المعني نكمي انه اندعاست نأ نكمي ةيناجم قدعاسم قادا يه تايلمعلا قبقارم .رادصإ اذه تيرحت درين معن المعليا معن المعالي المعليا مي المعال المي المعالي المي المي المي المي المعالي المعالي المعالي المعالي المعالي المعالي المعالي المعالي من المعالي الم

ةركاذلا غيرفتو ProcMon تالجس عيمجت ةيفيكب ةقلعتملا تاوطخلا دنتسملا اذه فصي دنع BSODs ءاشناب موقت اهنأ ينعي امم) ماظنلا ديهمت ةيلمع ءانثأ ةلكشملا تثدح اذإ ديهمتلا ءانثأ ثدحت يتلا ماظنلا ثادحأ طاقتلال تالجسلا هذه رفوت مزلي .(ديهمتلا

### :ءارجإلا

ةلأسملا هذه جاتناٍ ةداعاٍ اهلالخ نم لهسي ةقيرطب رابتخالا تالآ دادعإب مق .1.

2. **متي يتلا تافلملا ةجلاعم <- فلم** ىلإ لقتنا .لوؤسمك اهليغشتو ProcMon ةادأ ليزنت ر**اسم** ددحو **ضرعلا زامج ىلع ايطايتحإ اهخسن**.

<b>3</b> Pri	ons Monitor - C/(2)	ari eri	164 new/Deakto	aby because "boy	pot/soit_ped						
ie i	At thet life	Teols	Cytions Help		10.00						
-		× A 1	\$19 <b>m</b>								
1236 1236 1236 1236 1236 1236 1236 1236	Poces Name   Septimizer    Septimiz	2242 2252 2252 2252 2252 2252 2252 2252	Operator A Na SystemCore Na SystemCore Provide SystemCore NapCourty Ray RepCourty Ray RepCourty Ray RepCourty Ray RepCourt Ray	Path relC HEC HEC HECU Software HECU Software HECU Software HECU Software	Cases Cases Cases (Cases) ori (Cases), PE		Fanal SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS	Detail Control FSC1 Control FSC1 Control FSC1 Thread ID 21 County Name County Name County Name County Name County Name	L.Q. L.R. D.R. Mag. Mag.		
234	Process Manita	r Backin	g Film								
236	These backing file of	Alects #	e being used to st	ore event datas							
1236. 1236	Name				Event Court	Event Bytes	Pending Events	Process Court	Octoney Court	Icon Court Connelled	
	Counterman		960) ( 960) ( 9	dgat teks ( pre	18.1.2	*EN(.)#	5	50	129	13 16	
236	Process Haritar car	atore e	under in without me	mary (Imited by I	he system conveit lent;	, or its a file year	pecify (initial by the	del spece). Which	de you profect		
236	Clarification	-	Column Disc								
236	@ Use Renamed	0	Lary on 7484 re	· Desitapiproce	in_pulper[aut2.pn]						0
12.34		-									-
236	Pro/Honibadi E. 45	-	(printee perding)								OK Canot
1236	Distance DE Distance DE Distance DE	2948 2948 2948	RegOpentary RegOpentary RegOpentary	HER Application HER Application	ons'incleped and ons'incleped and ons'incleped and		SUCCESS SUCCESS SUCCESS	Duared Acce Query Name	. Ř.		

3. ديەمتلا ليجست نيكمت <- Options دلقتنا، Procmon قادأ يف.

🗳 Pr	poess Monit	tor - C:\)	Users/win	7x64-rww\Desktop	Pprocmon_output/text1.pml				
File	Edit Even	Filter	r Tools	Options Help					
1 mil 1		[2]	- A	Alumnum	Ten I				
			V 🗛 (	Adversion	rep				
Time .	- Process	lare	PID	Fort			Rend	Detail	
12:36:	. IF Search	indeer.	2252	Mahlaha	alar		SUCCESS	Cantrol: FSCTL_Q.	
12:36:	. It Search	indexer.	2252	riginga	ann.		SUCCESS	Cantrol: FSCTL_R	
12:36:	<ul> <li>IF/Search</li> </ul>	hckeer.	2252	Configure	umbola		SUCCESS	Cantrol: FSCTL_R.	
12.36:	Search	FiterHos	5 2072	conger			SUCCESS	Thread ID: 2884	
12:36:	- Explore	# EXE	2588	Select Colu	mnu		SUCCESS	Query: Name	
12:36:		NEXE	2968	11. 0			SUCCESS	Query: HandleTag	
12:36:	- Debo	EXE	2968	Plintory Dep	10h		SUCCESS	Query: Handle Tag	
12.36:	- Epplore	XEXE:	2968	Profiling Ex	anta		SUCCESS	Desired Access: Q	
12.36.	- Diplore	# EXE	1				SUCCESS	Query: Name	
12.36:	- DEPOT	KEAE	2968	Enable Boo	t Logging		SUCCESS	Query: Handle Tag	
12.36.	- Depay	2439	2366				SUCCESS	Deared Access N	
12.36	- abbon	EVE .	2900	🖌 Show Reso	ived Network Addresses Ctrl+N		5000E35	Type: Hebb_ac. Us	
12.36	- England	LAL LAL	2300	Hex File Of	fuets and Lenoths		SUCCESS		
12.36	- Coport	- EVE	2200				SILCERS	Overs Name	
12.36	- Enloy	EVE	2566	Hex Proces	s and Thread IDs		SILLESS	Duesy HandeTas	
12.96	Entre	EVE	2488	Burghunder	Hill ID S-theres/Classes		SUCCESS	Over: HandeTag	
12.36	Enloy	FXE	2968	BagCoanKey	HICLD Schwark Classes) and Deedlight Provi	<b>A</b>	NAME NOT FOUND	Desired Access: R	
12.36	Endor	EDE	2988	BedOpenKey	HKCR\om\OperWithProvide		NAME NOT FOUND	Desired Access: R.	
12:35	Paritor	FXE	2968	BacQueryRev	HKC1D/Software/Classes		SUCCESS	Duey Name	
12.36	Epilor	# DE	2568	Regionerster	HKCU/Software/Cleaner		SUCCESS	Query Handle Teg.	
12:36	Delor	V EXE	2968	RegQueryKey	HKEU/Software/Classes		SUCCESS	Query HandleTag	
12.36	Delor	# EXE	2568	RegOpenKey	HICU/Software/Classes/Software/Merssolt/	Windows\Curr	NAME NOT FOUND	Destred Access R.	
12:36:	Delor	N EXE	2968	RegOpenKey	HKCR\Software\Microsoft\Windows\CurrentV	ension\Explore.	NAME NOT FOUND	Desired Access: R	
12:36:	. Califician	# EXE	2568	RegiliusryKey	HICU/Software/Classes		SUCCESS	Query: Name	
12.36:	. Bokon	SC3 N	2968	RegQueryKey	HKEU/Software/Classes		SUCCESS	Query: HandleTag	
12:36:	. 🔚 Epion	# EXE	2988	RegularyKey	HKEU/Software/Classes		SUCCESS	Query: HandleTag	
12:36:	. Bolore	S EXE	2988	RegOpenKey	HKCU\Software\Classes\pnl		SUCCESS	Desired Access: R	
12:36:	. 🎧 Esploy	r EXE	2988	RegQueryKey	HKCU/Software/Microsoft/Windows/Current/V	Antion \Explore .	SUCCESS	Query: Handle Tag	
12.36:	- Epiore	SKENE	2968	RegOpenKey	HKCU/Software/Microsoft/Windows/Current/V	fersion'/Explore	SUCCESS	Desired Access: R.,	
12:36:	- Epion	r DE	2968	RegQueryKey	HKEU/Software/Microsoft/Windows/Gurrent/	fersion \Explore	SUCCESS	Query: Handle Tag	
12.36:	- Dekore	N EXE	2968	RegOpenKey	HKEU/Software/Microsoft/Windows/Current/V	Persion \Explore.	SUCCESS	Desired Access: R	
12.36	- Diplore	EXE	2968	Regioury fay	HKEU/Software/Microsoft/Windows/Current/V	Fersion \Explore.	SUCCESS	Query: Handle Tag	
12.36:	- Dekore	N EXE	2966	RegOpenikey	HKEU/Software/Morosoft/Windows/Gunent/	earen. Exblore -	SUCCESS	Desired Access: Q	
1236.	- Distant	# E.A.E.	2966	Regularyvalue	HILLU-Software Microsoft Of Holeward V	reners Vopione	SUCCESS	Type: POID_SZ, Le	
12.36.	- DEKON	N EAS	2900	Hog Josefley	HALU-Software Geotosoft Gendens Currently	earlow (Doblore -	SUCCESS		
12.30	- Colore	LAL .	2300	They Lose Tay	HALL Converse declared developed a converter	(anion) Explore	SUCCESS		
12.96	- Copore	EVE	2900	Barlunder	HICLD Scheme/Classes	ason option.	SILCERS	Overs Name	
12.36	- Delive	EVE	2968	BacQueryRey	HIT ID Schurge Change		SILLESS	Duesy HandeTas	
12.36	- Enlos	EVE	2900	Bandumiter	HICLD Scheme Classes		SUCCESS	Query HandeTag	
12.36	Delas	EXE	2968	BacCoacKey	WETD Schurge Classes) And references	d ava	NAME NOT DO NO	Desired Access: R	
12.36	Feelers	EDE	2948	Ban Doan Key	HICR Ambrations retained and	0.040	SUCCESS	Destred Acress R.	
12.35	Dela	V EXE	2968	RegCloseKey	HREFT Applications unstepad met		SUCCESS	and the reason of the	
12.36	Epion	* EXE	2968	Regiourner	HKCU'Software'Classes		SUCCESS	Query: Name	
12:35	Delor	N EXE	2968	RegQueryKey	HKEU/Software/Classes		SUCCESS	Query: HandleTag	
12:36	- Epine	# EXE	2568	RegilizeryKey	HKCU/Software/Classes		SUCCESS	Query Handle Tag	
12.36:	- Delor	3G N	2968	RegOpenitay	HKEU/Software/Classes/Applications/Instepa	d.eee	NAME NOT FOUND	Desired Access: R.	
12:36	- Califiphone	# EXE	2568	RegOpenKay	HICR'Applications Viotepad ane		SUCCESS	Desired Access: R	
12.36:	- Bolow	N EVE	2968	RegQueryKey	HKCR'Applications' notepad eve		SUCCESS	Query: Name	
12:36:	. 🔚 Explore	# EXE	2988	RegiliusryKey	HKCR\Applications\notepad ass		SUCCESS	Query: Handle Tag	
12:36	Con Deploye	N EVE	7960	Carl Coarling	USP10 Colleges (Change) Instantional college	d avail 1 of fac	NAME KINT ON BIT	Desired Access: D	

4. **ةيناث لكو تاديدەتلا طيمنت ثادحأ ءاشنإ** ددح.

🎒 Proc	Process Monitor - C/\Users\win7x64-new\Desktop\procmon_output%test1.pml							
File Ec	dit Event Filte	r Tools Options Help						
-2 E								
		A 75 A 16 W						
Time	Process Name	PID Operation	Path		Result	Detail		
12:36:	Searchindexer		IC:		SUCCESS	Control: FSCTL_Q_		
12:36	Searchindexer		IC:		SUCCESS	Control: FSCTL_R		
12:36	S Easthin Day	d Looping		)	SUCCESS	Control: FSCTL_R		
12:36:	ES Chable bot	n cogging			SUCCESS	Thread ID: 2884		
12:36	Call Descent M	where one passes in the and pro-	floor as such that can be a		SUCCESS	Query: Name		
12:36	E the state	of all running applications at a r	equiar interval.		SUCCESS	Query: Handle Tag		
12:36	20		cyne cho ren		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: HandleTag		
12:36	<b>1</b>	Every 100 milliseconds			SUCCESS	Desired Access: M		
12:36	Care I	_		(Default)	SUCCESS	Type: REG_SZ, Le		
12:36	<b>6</b>		OK Cancel		SUCCESS			
12:36	B		T	]	SUCCESS			
12:36	Explorer EXE	2988 KRegQueryKey	HKCU/Callwave/Casses		SUCCESS	Query: Name		
12:36	Epplorer EXE	2988 KRegQueryKey	HKCU/Software Westers		SUCCESS	Query: Handle Tag		
12:36	Epplorer EXE	2988 RegQueryKey	HKCU Software Classe		SUCCESS	Query: Handle Tag		
12:36	Explorer.EXE	2988 RegOpenKey	HKCU\Software\Classes\pml\	OpenWithProgids	NAME NOT FOUND	Desired Access: R		
12:36	Diplorer EXE	2988 RegOpenKey	HKCR\pm\OpenWithProgids		NAME NOT FOUND	Desired Access: R		
12:35	Diplorer EXE	2966 RegQueryKey	HRDU/Software/Classes		SUCCESS	Query: Name		
12.36	Explorer EXE	2968 RegQueryKey	HRCU/Software/Classes		SUCCESS	Query: Handle Tag		
12.36	Diblover EXE	2305 Regulatery tray	HKLU/Software/Classes		SUCCESS	Query: Handle Tag		
12.35	Explorer EXE	2505 Regupenkey	HNLU/Software Classes (Software)	rare vecrosoft windows Lurr.	NAME NOT FOUND	Desired Access: H		
12.05	EDDIONALEVE	2366 Reguperivey	HNUH GOTWARE VECTORIT VIVI	noows current version (Explore.	INVERTICAL FOUND	Desired Access. H		
12.30	Colorer EXE	2000 Performance	UNCLE Colorana Chasses		2000622	Query Name		
12.30	Evolver EVE	2500 Page walker	WC10 Software Classes		CLICCESS CLICCESS	Query Hande Tag		
12.36	Evolution EVE	2988 Register	HKC10 Software (Classes) and		SUCCESS	Designed Access: R		
12.36	European EXE	2922 Real and an	HKT11 Software Microsoft We	where Version Evolution	SUCCESS	Query HandaTan		
12:36	Evolow EXE	2988 BegOpenKey	HIC'LI'Software/Moreadt/We	dows\CurrentVersion\Explore	SUCCESS	Desired Access: B		
12:36	Epolowr EXE	2988 RecQuer/Key	HKCLI/Software/Mcrosoft/W/r	down\CurrentVersion\Explore	SUCCESS	Query Hande Tao		
12:36	Explorer EXE	2988 RegOpenKey	HKCU/Software/Microsoft/W/r	dows\CurrentVersion\Explore	SUCCESS	Desired Access: R		
12:36	Explorer EXE	2988 RecQuer/Key	HKCU/Software/Mcrosoft/We	ndows\CurrentVersion\Explore	SUCCESS	Query Hande Tag		
12:36	Epolorer EXE	2988 ReoOpenKey	HKCU/Software/Mcrosoft/Wir	ndows \Current Version \Explore	SUCCESS	Desired Access: Q		
12:36	Epplorer EXE	2988 RegQueryValue	HKCU\Software\Mcrosoft\We	dows\CurrentVersion\Explore	SUCCESS	Type: REG_SZ, Le		
12:36	Explorer EXE	2988 RegCoseKey	HKCU\Software\Mcrosoft\W/r	ndows\CurrentVersion\Explore	SUCCESS			
12:36	Epplorer EXE	2988 RegCloseKey	HKCU\Software\Mcrosoft\Win	ndows\CurrentVersion\Explore	SUCCESS			
12:36	Explorer EXE	2988 RegOoseKey	HKCU\Software\Mcrosoft\Win	ndows/Current/Version/Explore	SUCCESS			
12:36	Eplorer.EXE	2988 RegQueryKey	HKCU/.Software/Classes		SUCCESS	Query: Name		
12:36	Epplorer.EXE	2988 RegQueryKey	HKCU/Software/Classes		SUCCESS	Query: Handle Tag		

عيمجت متي ەنأ نمو Procmon يف ةلصلا تاذ ةيفصتلا لماوع ةفاك رايتخإ نم دكأت .5 تانايبلا.

6. ةادألا مادختساب لطعملا Windows ضرف كنكمي ،لطعلا راركت ىلع ارداق نكت مل اذا قدعاسملا مادغتساب لمايي ما ميل مايي ما مي من المي مي مي المعالي NotMyFault64.exe أو الممل

انه ةدوجوملا ليغشت ةيفيك لوح تاميلعتلا: <u>https://docs.microsoft.com/en-us/windows/client-</u> management/generate-kernel-or-complete-crash-dump

Printer Printer Col	And the set of the	of Automort with react first		
THE CARE DATE THE	TONS OPPORT PAR			
	7 A Q X A			
Ins. Poper tare	PD Genter	Fat	Fault Deal	
23. Eduar	100 Bulletin	C Proper NerCenn 487/3314 Lawing	9.00000 (Mar 2004.5	F
23. 14.00	W Carolina	<ol> <li>C. Prepari RenCash (MP) 111 (Low No.</li> </ol>	\$UCCESS VilureDealer	
State State	The Dary Street	<ul> <li>C Proper Ner Carrielle (11.6) and by 10.10 Advances (11.6) and (11.6) and (11.6)</li> </ul>	BUTCHICK CARDINE IN THE	
Contraction of the local division of the loc	The Part Institute	18 M Schwart Rougel Western 17 Constitution To	and out that they have been	
238 8140.000	170 Charlester	HEAL Selecter Hunself Western 17 Current lensers for	NAME AND POST OFFICE ADDRESS ADDRE	
23. EV.m	170 Danibardar	<ol> <li>Prepar Rendam AR11114Lawing</li> </ol>	\$10020 Annator Day 3	
23. 19.00	The Date Service	<ol> <li>Vegen Rendern der 11 Tell der bg.</li> </ol>	PLOTED Accessible	
20 D C C	The second second	<ul> <li>Compare Neuroland (1971) 11 (1971) 401</li> </ul>	ALCON VANADA	
23. 814.00	1707 Bellan Winton	<ul> <li>C Proper Rendard AP (1114) and Ig</li> </ul>	survey (serve). (searches )	
23. Exten	111 Charlowine	18.M Schware Human Western Mr.C. prestranger Tor	NAME AND POST OFFICE ADDRESS.	
23. EVE+*	The Section Pro-	TRUM Subvery Human Western 1711 prestinences for	NAME AND POST OFFICE ADDRESS OF TAXABLE ADDRESS OF	
5	The second second	<ul> <li>A provide the set of the set of</li></ul>	Automatic descention	
C.H. Kirkan	The Balancharder	6. C Proper Rendard AP (111-4) and 10	9.01205 Anosector	
CH. EVEN	THE BUNKING	C Proper Nerr (acr 44P 111 Arrents	\$10,000 (Ref (\$100.)	
2.0. 8.0.00	The basedone	<ol> <li>Proper Nerrisch 48*11114: en hg</li> </ol>	\$10,805 Valueballer	
	The Party State	The Advancement of the second second	and out they have been	
City Kingson	1 IN CASE AND	The M Schwarz (Renault Westwork) Constrainers for	want out think instal Array	
CH. EVEN	110 Charlowthe	mit of Schwarz (Actual) Mexicos (C) premience: To	NAME AND POST OFFICE ADDRESS ADDRESS.	C
23. EXt. 44	170 Million Charles	<ol> <li>Prepar Services AR* 111 Acres 19</li> </ol>	Access Accession	
10- 10- mar	The second second	Company New York and Company of the log	And and a second	
Contraction of the local division of the loc	I'm Burnty	Company Parcel and All Property de	ALCEN Dates ha	
Cit. Extran	THE BLOCK	Companition Capital Protocols	\$10080 Deturne Asse	Description Differences Report Provider The Section Section 2014
Cit. Extras	100 Burnshieler	pa C Proper Ner Central Protocols	9.00895 (Mar 1.05)/4	IN ATOM POST AT
2.0. EXtern	The second se	<ul> <li>Proper Ner Cech JAP Trace drawing</li> </ul>	NAME AND POSTO DAMAGE ACTION	
20.000	The second second	Property and the second second	states and shares have	
Coll. Barran	110 Bellen having	d. C. Propert Revision and Property de	SALES Acception	Example of the second s
CH. Kirken	100 Aureorfedry	pa ( Proper NorCech AP Interacts	9,0088 Ohe 1,0524	A Same device the second of second second
2.0. 10.00	110 Australia	<ol> <li>Chapter RenCapital P111 Acres by</li> </ol>	9.00805 Viuralization	View and Contract of States and S
50- 50 m	No. Concerning	<ul> <li>I Proper Ner Carrielle (11) 41 de 19</li> <li>I Marcelle (11) 41 de 19</li> </ul>	state of the local lines in	
10.000	110 Parlantes	with the former internet inferiors of Complement In-	want out think land hours	NAME AND ADDRESS OF ADDRESS ADDRES
C.M. Kirken	110 Anglering	HUM Schware (Renault Westow 10" Caractilasses The	NAME OF TAXABLE ACCOUNTS	REACHER CONTRACTOR AND A DESCRIPTION
Cit. Electron	110 Bilancharder	6. C Proper RenCess (MPC) Educes by	9.0000 Accelerities	21 (20-2010) 15 (21-20) (20-20
20. DAM	IN BLANKARD	<ol> <li>C. Propert RenCarol all P. 711 Mathematics</li> </ol>	ACCESS Received as	Tribert
10.000	The second	<ul> <li>Comparison Residence and Providence Report Frances</li> </ul>	ACTES Viscolation	3 D(p/s) - 27,875,046,031 Spree free
U.M. Birtham	110 Alban/Writer	<ul> <li>C Proper RenCentation 718 at reachs</li> </ul>	auronoutry, Date Ins 1	Endowerswije/hit/trave/beitrag/ed-typijanome.http://
CO. Elfonse	110 Chalteria	HUM Orbert Hensell Western HT Carentiesters In-	NAME AND POSTO DARREST ACCOUNT.	the base web with a set of the base of the
20.00	10 Partnerfe	HLM Ofwari Menadi Medras III Curantiasari Te	NAME HOT POINT DIAMAGE Across	
10- 10- E	The second second	A. S. Stranger, Rev. Const. (1997) 21 (1997) 201	A CORE ADDRESS AND ADDRESS	Endower with Public way disclosed and in a public for the public of the
210. E.M.m.	100 Million/Aprile	6. C Proper RevCard 4987-757 at use he	9.0000 Broate-las 2	
U.S. Kirken	100 Bulletin	C Propert Ren Carol all P (21) 8 all and by	9.0088 Ofer 20864	
10. Distant	100 Cardineral	<ol> <li>C Prepare RenCennister (118 all sea by</li> </ol>	9.0000 WareCepter	1
10.00	110 Charlestin	and M. Schwarz Street Street and V. Completence To-	land out that for any long	
U.S. Watan	100 Charles Ter	HEAP School (Renault Writing W Constitution) To	NAME OF TAXABLE ADDRESS	1
U.M. Kirken	100 Charles No.	HEM Scheme Monadi Western W Commission Ter	AMERCEPTION CAME Arrest	
Contraction of the local division of the loc	100 Million Renter	<ol> <li>C. Prepare RenCerci (MRV 711 R all rate leg.</li> </ol>	S.C.BUI Recater Day 2	1
10.00	100 Addates	Company Residence and Provide Lands	BACCERS (Mar 1998)	1
238 B 40 mm	100 Millionational	<ul> <li>C Proper RenCard (007-018 all on her</li> </ul>	9.0000 WareCester	· · · · · · · · · · · · · · · · · · ·
236. Woltow	100 Casher/Writer	<ul> <li>E Vegen Re/Celot/ddP/2018-blanche</li> </ul>	BUTCHIONEYL, Destrolling 1	
23. Edited	100 Challentin	HEM Selecter Human Western HT Constitution Se	AND REPORT FOR CARNER ACTION	· · · · · · · · · · · · · · · · · · ·
1	The Part Service	the officer thread the bird of the second se	And the first state of the	1
12. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	100 Million Partie	<ol> <li>C. Avgues Res Card (MP) 211 di una but</li> </ol>	BACTER Manageria	1
238 B Man	100 Million Aprile	<ol> <li>C. Propert Ren Calor (MR* 251) et une les</li> </ol>	success mountained as	
CH. Kidow	100 Advanta	C Proper RenCennet#1018 #Lawing	9.0000 (Ref 2000)	L.
and the second second second	5.5 Case a	C. Property March 1996 (1996) Total State (1996)	NAME AND POSTOCIONAL ACCOUNTS	
C 10 Company	THE PROPERTY.	NUMBER OF STREET, STRE	BACTER CARDON COMPANY	
CH. Compression	200 Children Aug	HEALDSTRUCT AND ADDISONDED	BUCCETT Grey NA Sal	n de la constante de
CH. Elementer	200 Challen Per	<ol> <li>HEM SOFTWARE Assess VEDVCMORE</li> </ol>	BUMEN TOO EN.	
C.S. Compression	210 Chattan	<ul> <li>NUMBER OF ADDRESS AND ADDRESS</li></ul>	NO.001 Tax PELLS	a
and the second sec	THE PART NUMBER	THE REPORT OF CALLSRIDE AND ADDRESS OF CALLSRIDE	Barrier Anna	
C.M. B. Managerine and	THE PARTINE TO	HEAVIER HAVE AN ADDIVING NO.	PLOTED Daniel Access	
23. 8	200 Challenter	HEAD STRATE ASSAULT ADDITION	9.0000 Gary NA Sal	
CH. Elementer	CO Challenger	LINE ADDRESS A ADDRESS ADDRESS ADDR	8,010 N 100 DK	
A Real Property lies	THE RECEIPTION	and the second s	No. of the PELAC	F
			100.000	
NAMES OF A DESCRIPTION	E AND CALL	point in Construction on the party interesting	a way part	

#### .ةلآلا لطع

دجوي ،ايودي MEMORY.dmpو Procmon.pmb عيمجتو "نمآلا عضولا" يف زاهجلا ليمحتب مق .8 دلجملا يف نيفلملا الك c:\Windows. عم تكراش نوكي نأ دربم اذه C:\Windows. دلجملا يف نيفلمل

🗼 Windows					_	8
😋 🕞 🗸 🗸 Compute	r 🔻 Local Disk (C:) 👻 Win	dows 👻	÷ 🙀	Search Windows		
Organize 👻 📄 Open 🔹	New folder				8= • 🖬	
🚖 Favorites	Name +		Date modified 11/21/2010 4:24 AM	Type Application	Size 2,805 KB	
Computer	<ul> <li>fveupdate.exe</li> <li>HelpPane.exe</li> <li>hh.exe</li> <li>IE11_main.log</li> <li>MEMORY.DMP</li> <li>mib.bin</li> <li>msdfmap.ini</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 1/6/2020 12:41 PM 7/14/2009 1:06 AM 6/10/2009 10:36 PM	Application Application Application Text Document DMP File BIN File Configuration sett	15 KB 717 KB 17 KB 14 KB 331,914 KB 43 KB 2 KB	
Local Disk (C:) Local Disk (C:) CD Drive (D:) Shared Folders (\\vn	notepad.exe ntbtlog.bt PFRO.log		7/9/2015 7:57 PM 1/6/2020 12:41 PM 1/6/2020 12:30 PM	Application Text Document Text Document	189 KB 83 KB 576 KB	
📭 Network	Procmon.pmb ProfessionalN.xml	Type: XML Document Size: 52.3 KB Date modified: 6/10/20	1/6/2020 12:41 PM 6/10/2009 10:30 PM :39 AM :30 PM :30 PM 7/14/2009 0:56 AM 11/21/2010 4:24 AM 6/10/2009 10:31 PM	PMB File XML Document Application Text Document Text Document Application XML Document	320,740 KB 53 KB 417 KB 29 KB 0 KB 66 KB 48 KB	
Procmon.pmb PMB File	Date modified: 1/6/2020 1 Size: 313 MB	12:41 PM Date crea	sted: 1/6/2020 12:41 PN	4		

ءاشنإ مت اذإ "يداعلا عضولا" يف ليغشتلا ديەمت ىلع ارداق تنك اذإ ،يرايتخإ لكشب .7 ىرتسف ،ىرخأ ةرم ProcMon ليغشتب تمق اذإ ذئدنع ،Windows دلجملا يف PMB تافلم .ظفح رزلا قوف رقنلاب ثادحألا ظفح ةداعإ كنكمي ،اذه نم .ةيلاتلا تالجسلا

2 Process Monitor - Sysintemails: www.spsintemails.com			
File Edit Event Filter Tools Options Help			
Time - Pourse Name PID Densities Falls	Read	Detel	

Presenta Mondae	Ξ
2 Sing of laser time activity was control by a persistal inducer of Process Vientins. So you with in solve the collected data new?	
Tm. He	

_
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	INCH Gyster Correct Control State Control SESSION MANA.	CUCCESS	Index O Name A
A1 Brance and	202 PasEn militar	LVI M Custon Custon Custon Caston Control COCCOM MANA	CINCESS	Index 5 Name M
41	292 RecEnceValue	HALM CYREM LUTERLOTED SELLOTED SELLOTED SESSION MANA	SUCCESS	Index 3 Name M
A1 Brends and	292 PasEn militar	LVI M Crater Crater Control Set Control SESSION 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	
41	292 ResOurceMay	HIGH System Control of Doctor Sci Control CERCINA MANA.	CUCCESS	Daried Access M
supercise	eve meguperney	INTER OVER COLORDON FORD SE22YON WARK.	3000633	VEHEV /VVEH. P

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما