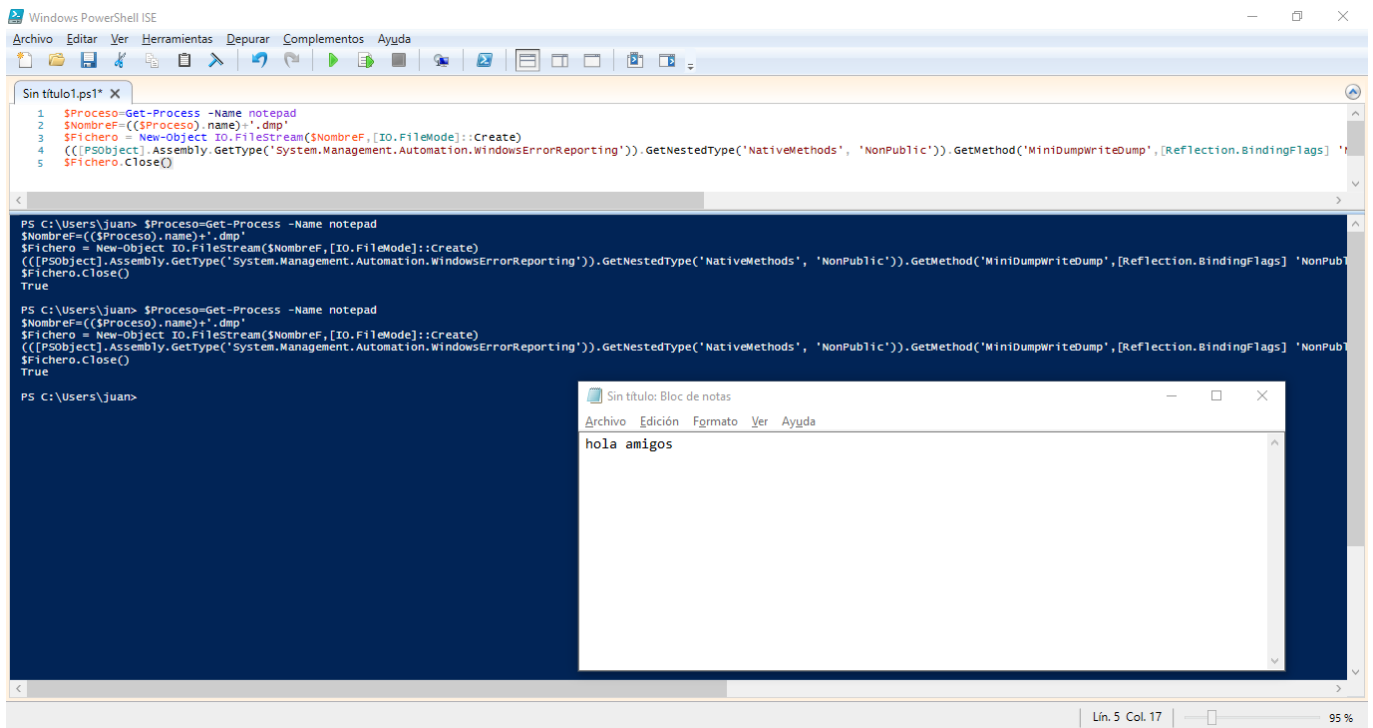


Crear un fichero de volcado de memoria de un proceso y buscar una cadena

[crayon-6a9d4fa29ff70929759623/]



Buscar cadena en el fichero de volcado

HxD - [C:\Users\juan\notepad.dmp]

ArchivoEdiciónBuscarVerAnálisisExtrasVentanas?

24ANSIhex

notepad.dmp

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17					
001391A0	99	2E	FD	7F	00	00	84	91	30	31	FD	7F	00	00	00	00	00	00	00	00	00	00	00	00	00	"..ý.....'01ý.....			
001391B8	00	00	00	00	00	00	79	B6	E7	E6	4D	02	00	00	00	00	00	00	00	00	00	00	B0	EF	00	yçæM.....*i			
001391D0	E7	E6	4D	02	00	00	00	90	E7	E6	4D	02	00	00	00	00	DD	2D	FD	7F	00	00	DC	FF	00	çæM.....çæM.....ÿ-ý...Dy			
001391E8	6D	CA	C5	28	D3	01	30	00	68	F6	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	mÊÀ(Ô.0.hð.....			
00139200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	5B	34	D9	39	A7	17	00	0F	43	6F	[4Ü9\$...Co		
00139218	6D	6D	6F	6E	50	72	6F	67	72	61	6D	57	36	34	33	32	3D	43	3A	5C	50	72	6F	67	67	67	mmonProgramW6432=C:\Prog		
00139230	72	61	6D	20	46	69	6C	65	73	5C	43	6F	6D	6D	6F	6E	20	46	69	6C	65	73	00	00	00	00	ram Files\Common Files...		
00139248	00	00	00	00	00	00	5D	34	D9	3F	B0	17	00	0D	43	4F	4D	50	55	54	45	52	4E	41	41	41	]4Ü?°...COMPUTERNA		
00139260	4D	45	3D	4C	41	4D	35	34	00	00	00	00	00	00	00	00	5A	34	D9	38	B6	17	00	0C	43	00	ME=LAM54.....Z4Ü8\$...C.		
00139278	3A	00	5C	00	57	00	49	00	4E	00	44	00	4F	00	57	00	53	00	5C	00	53	00	79	00	00	00	:\.W.I.N.D.O.W.S.\S.y.		
00139290	73	00	74	00	65	00	6D	00	33	00	32	00	5C	00	67	00	64	00	69	00	33	00	32	00	00	00	s.t.e.m.3.2.\g.d.i.3.2.		
001392A8	66	00	75	00	6C	00	6C	00	2E	00	64	00	6C	00	6C	00	00	00	00	00	00	00	00	56	34	34	f.u.l.l...d.l.l.....V4		
001392C0	D9	34	B1	17	00	08	10	F6	E9	E6	4D	02	00	00	80	B2	E8	E6	4D	02	00	00	3E	62	62	62	Ü4±...oæM...E*æM...>b		
001392D8	70	CA	C5	28	D3	01	40	F3	E8	E6	4D	02	00	00	00	B0	E8	E6	4D	02	00	00	3E	62	62	62	pÊÀ(Ô.ðæM...°æM...>b		
001392F0	70	CA	C5	28	D3	01	80	F1	E8	E6	4D	02	00	00	40	AE	E8	E6	4D	02	00	00	3E	62	62	62	pÊÀ(Ô.êæM...@æM...>b		
00139308	70	CA	C5	28	D3	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	pÊÀ(Ô.....		
00139320	00	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	YYYYYYYYYYYY.....		
00139338	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	D0	07	00	02	00	00	00	59	34	34	B.....Y4		
00139350	FB	19	BD	17	00	20	68	00	6F	00	6C	00	61	00	20	00	61	00	6D	00	69	00	67	00	00	00	00	Ü.4...h.o.l.a...a.m.i.g.	
00139368	6F	00	73	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	o.s.....	
00139380	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00139398	00	00	00	00	00	00	00	08	00	07	EA	4D	02	00	00	00	00	00	00	00	00	00	00	5B	34	34	èM.....[4		
001393B0	D9	39	B2	17	00	0F	46	50	53	5F	42	52	4F	57	53	45	52	5F	41	50	50	5F	50	52	52	52	52	Ü9*...FPS BROWSER APP PR	
001393C8	4F	46	49	4C	45	5F	53	54	52	49	4E	47	3D	49	6E	74	65	72	6E	65	74	20	45	78	78	78	78	OFILE_STRING=Internet Ex	
001393E0	70	6C	6F	72	65	72	00	00	00	00	00	00	00	00	5D	34	D9	3F	B0	17	00	13	48	4F	4F	4F	4F	plorex.....]4Ü?°...HO	
001393F8	4D	45	44	52	49	56	45	3D	43	3A	00	00	00	00	00	00	00	00	00	00	00	00	56	34	34	34	MEDRIVE=C:.....V4		
00139410	D9	34	B6	17	00	0A	00	00	00	00	00	00	00	00	93	D5	EC	E4	20	00	6E	00	E0	11	11	11	Ü4g....."Öia .n.A.		
00139428	E8	E6	4D	02	00	57	00	69	00	6E	00	64	00	6F	00	77	00	73	00	2E	00	53	00	00	00	00	00	æM...W.i.n.d.o.w.s...S.	
00139440	65	00	63	00	75	00	72	00	69	00	74	00	79	00	2E	00	45	00	6E	00	74	00	65	00	00	00	00	e.c.u.r.i.t.y...E.n.t.e.	
00139458	72	00	70	00	72	00	69	00	73	00	65	00	44	00	61	00	74	00	61	00	2E	00	50	00	00	00	00	00	r.p.r.i.s.e.D.a.t.a...P.
00139470	72	00	6F	00	74	00	65	00	63	00	74	00	69	00	6F	00	6E	00	50	00	6F	00	6C	00	00	00	00	00	r.o.t.e.c.t.i.o.n.P.o.l.
00139488	69	00	63	00	79	00	4D	00	61	00	6E	00	61	00	67	00	65	00	72	00	00	00	5C	34	34	34	34	i.c.y.M.a.n.a.g.e.r...\4	
001394A0	FB	1C	BD	17	00	20	10	30	EC	E6	4D	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Ü.4...0iaM.....	
001394B8	00	00	00	00	00	00	78	00	07	EA	4D	02	00	00	00	00	00	00	00	00	00	00	4C	34	34	34	34	x...æM.....L4	
001394D0	D9	2E	B7	17	00	10	F0	5A	E7	E6	4D	02	00	00	10	53	E7	E6	4D	02	00	00	5B	34	34	34	34	Ü....8ZçæM...SçæM...[	
001394E8	E7	E6	4D	02	00	00	20	53	E7	E6	4D	02	00	00	30	53	E7	E6	4D	02	00	00	10	5B	34	34	34	34	çæM... SçæM...0SçæM...[

Posición: 139356

Bloque: 139356-13935D

Longitud: 8

Sobreescribir

Sin título: Bloc de notas

ArchivoEdiciónFormatoVerAyuda

hola amigos