

2.025

2º Año

TUP - UTN

# LEGISLACIÓN

Profesora:  
Dra. Lonati,  
Marcela Paola

UTN \* TUC

Perito  
Informático e  
Información de  
la Pericia en  
Sistemas

## Perito Informático

Tanto el Código Procesal Civil y Comercial como el Procesal Penal reglamentan acerca de la idoneidad para ser Peritos en las causa judiciales. Ambos indican que de estar reglamentada la profesión los Peritos deberán tener título habilitante en la ciencia, arte, industria o actividad técnica especializada a la cual pertenezcan las cuestiones a expedirse; y sólo en el caso en que no lo estuviera o no hubiere Peritos diplomados o inscriptos deberá designarse a una persona de conocimiento o de práctica reconocidas.

La gran mayoría de las provincias del país regulan el ejercicio profesional informático. Cada una poseen normativas específicas que legislan en todo el ámbito provincial.

El Colegio de Graduados en Ciencia y Tecnología Informática de Tucumán (C.G.C.T.I.T) reglamenta el ejercicio profesional del Informático a través de la Ley 7490.

Los colegios o consejos profesionales son asociaciones integradas por quienes ejercen una profesión liberal y que suelen estar amparados por el Estado. Sus miembros asociados son conocidos como **colegiados**. La finalidad de los colegios profesionales es la de velar por el cumplimiento de una buena labor profesional, donde la práctica ética del trabajo se constituye como uno de los principios comunes que ayudan a definir los estatutos de cada corporación.

## Pericia y Análisis Forense de Memoria

**Un volcado de memoria es un registro no estructurado del contenido de la memoria en un momento concreto, generalmente utilizado para depurar un programa que ha finalizado su ejecución incorrectamente o para realizar copias del contenido de la misma.**

El Análisis Forense de Memoria consiste en la adquisición de datos provenientes de la memoria principal de un sistema de computación (*memoria RAM*) con el fin de obtener información relevante sobre el mismo.

En el ámbito Forense se trabaja con **volcados de memoria** porque así se realiza una intrusión mínima sobre el sistema, además se garantiza la posibilidad de reproducir el análisis y obtener los mismos resultados.

Es fundamental conocer las herramientas seleccionadas para realizar el volcado de memoria, ya que afectará al mismo: si se trata de un hardware tendrá algunas condiciones en las cuales funciona y un puerto al que debe conectarse (*que la computadora, objeto de análisis, debe tener disponible*), y si se trata de un software, el mismo se cargará en memoria.

Una vez obtenida la información para el análisis, es necesario conocer la estructura que almacenan la información de interés: procesos, threads, módulos, conexiones, sockets, drivers, entrada de registro, entre otras, son estructuras propias de cada Sistema Operativo y que, además, varían de acuerdo a las versiones y arquitecturas del procesador. El conocimiento de estas estructuras es fundamental para obtener la información que se almacena en ella y que posiblemente sólo esté disponible en memoria.



- El reconocimiento de estructuras consiste en identificar los distintos artefactos que pueden encontrarse dentro de la memoria explorando el volcado de memoria.
- El paso siguiente relaciona entre sí los distintos artefactos identificados.
- El análisis automático se realiza a partir de los datos identificados previamente en base a reglas y condiciones predefinidas.
- En base a la información que los motores de análisis pueden recuperar de manera automatizada queda en el analista forense realizar un análisis más profundo y dar significado a la misma en el contexto del caso investigado.

El análisis de la memoria principal puede ayudar a inferir el uso que se le ha dado al equipo o detectar indicios que soporten una hipótesis particular, también puede permitir la eventual detección de un malware que haya tomado control del equipo y sea responsables de las actividades que se han llevado a adelante desde esa computadora en particular (*este caso es de suma importancia porque se podría estar investigando a una persona inocente y el verdadero culpable esconderse detrás de ella. Para estas situaciones es vital el análisis de memoria ya que los indicios de malwares son difíciles de identificar y pueden hacer perder la evidencia digital*).

De la memoria también pueden extraerse contraseñas y claves de cifrados que estuvieran alojados en ella lo que puede permitir el acceso a cuentas de usuarios o información encriptada en otras imágenes forenses del caso.

Conociendo las particularidades y generalidades del análisis forense en memoria principal es posible descubrir muchos datos que pueden llevarnos a relacionar el mismo con actividades de interés para la investigación:

- Búsqueda del contexto de seguridad de cada proceso: puede identificarse el contexto de seguridad obtenido, es decir, el nivel de privilegios con el cual se ejecuta el proceso (*en Windows, la estructura \_TOKEN*), su proceso padre y otros elementos mencionados que permitan realizar un análisis y establecer previamente conclusiones sobre la eventual presencia de malware.
- Búsqueda de información que no se encuentra en el disco y que se sospecha se quiso ocultar: búsqueda de contenido cifrado, búsqueda de contenido “*legible*” (*se pueden encontrar fragmentos de texto de un archivo, documento o un correo electrónico que ha sido leído o escrito*), búsqueda de archivos.
- Búsqueda de información de conexiones y sockets: dentro de los datos de conexiones ya sean TCP, UDP o sockets, es posible vincular las mismas con los Process ID y así llegar hasta el proceso en sí mismo, pudiendo verificar si este resulta sospechoso. Esto permite relacionar procesos que resulten sospechosos con direcciones IP remotas y eventualmente extender la investigación.
- Búsqueda de información que indique la utilización de algún dispositivo periférico en el equipo, como podrían ser drivers cargados en memoria.
- Búsqueda de software específico: procesos, entrada de registros, módulos.

El análisis de la memoria no se circumscribe a estas estructuras y las relaciones entre ellas. También es importante incorporar el análisis a la búsqueda de datos que pueden ser relevantes y no forman parte de ninguna estructura en particular. En la figura se puede observar parte del contenido de una página web que fue abierta en el equipo desde donde se extrajo un volcado de memoria.

49091600	14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	43 2E 30 42 10 3C 00 00 00 00 00 00 00 00 00 00	zoveador).</p>
24847680	09 00 09 09 09 09 09 09 09 3C 70 20 20 69 64 3D 22	64 65 6E 20 63 6F 6E 74	<p id="
24847690	4C 43 31 30 35 22 3E 41	64 76 65 72 74 65 6E 63	LC105">Advertenc
248476A0	69 61 3A 20 6C 61 73 20	70 C3 A1 67 69 6E 61 73	ia: las páginas
248476B0	20 77 65 62 20 70 75 65	64 65 6E 20 63 6F 6E 74	web pueden cont
248476C0	65 6E 65 72 20 65 6C 65	6D 65 6E 74 6F 73 20 6D	ener elementos m
248476D0	61 6C 69 63 69 6F 73 6F	73 20 70 61 72 61 20 65	aliciosos para e
248476E0	6C 20 65 71 73 69 70 6F	2E 20 45 73 20 69 6D 70	l equipo. Es imp
248476F0	6F 72 74 61 6E 74 65 20	65 73 74 61 72 20 73 65	ortante estar se
24847700	67 75 72 6F 20 64 65 20	71 75 65 20 65 6C 20 63	guro de que el c
24847710	6F 6E 74 65 6E 69 64 6F	20 70 72 6F 76 69 65 6E	ontenido provin
24847720	65 20 64 65 20 75 6E 61	20 66 75 65 6E 74 65 20	e de una fuente
24847730	63 6F 6E 66 69 61 62 6C	65 20 61 6E 74 65 73 20	confiable antes
24847740	64 65 20 63 6F 6E 74 69	6E 75 61 72 2E 3C 2F 70	de continuar.</p>
24847750	3E 0D 0A 09 09 09 09 09	09 09 09 3C 70 20 20 69	<p i

Figura 9.2: Contenido del volcado de memoria en una ubicación en particular visto con un editor hexadecimal.

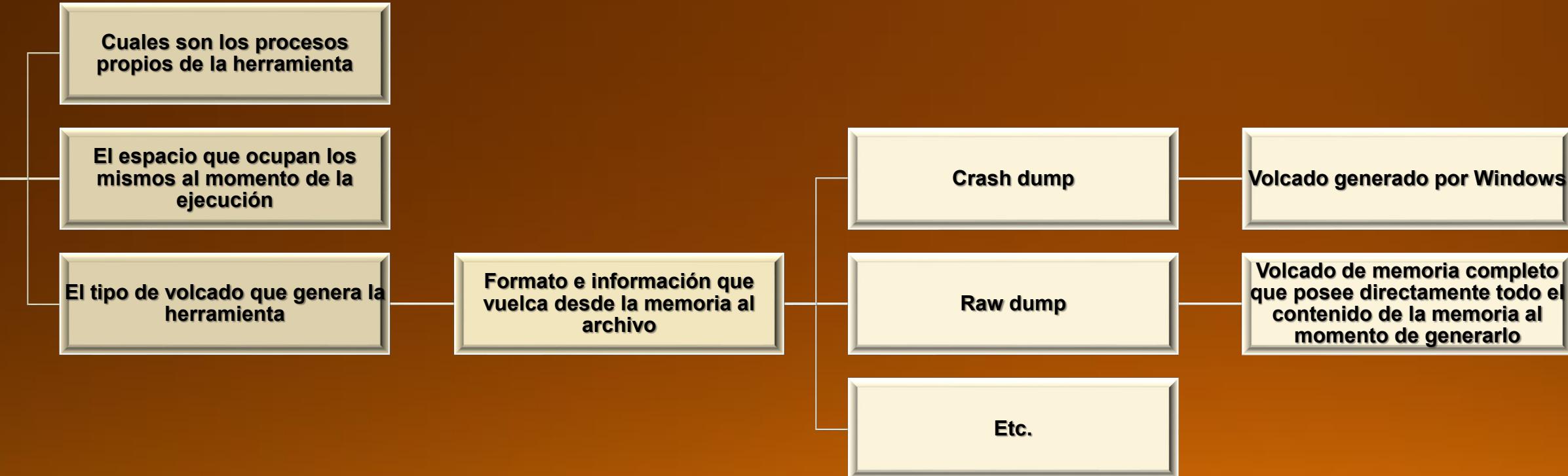
Cualquiera sea la pericia a realizar, los datos contenidos en un volcado de memoria se almacenan de diferente manera y pueden formar parte o no de distintas estructuras. Por esto es necesario saber como interpretarlos y que herramientas utilizar como soporte de análisis.

DAS95A00	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 00 00 00 00 00	Pool-tag:Proä
DAS95A01	00 00 00 00 01 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
DAS95A02	AF 00 00 00 03 00 00 00	03 00 26 00 00 00 00 00 00 00 00 00 00 00 00 00	
DAS95A03	00 9A 77 83 1B 50 80 8D	03 00 26 00 00 00 00 00 00 00 00 00 00 00 00 00	
DAS95A04	F0 DA E3 85 F0 DA E3 85	F8 DA E3 85 F8 DA E3 85	
DAS95B00	00 50 18 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
DAS95B10	00 00 00 00 FO D9 E3 85	40 27 1B 86 00 00 00 00 00 00 00 00 00 00 00 00	
DAS95B20	01 00 01 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
DAS95B30	2C DB E3 85 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Create Time
DAS95B40	0C 00 00 00 08 00 00 00	FF 07 5A A2 01 00 00 00 00 00 00 00 00 00 00 00	
DAS95B50	00 00 00 00 00 00 00 00	FF 07 5A A2 01 00 00 00 00 00 00 00 00 00 00 00	
DAS95B60	00 00 00 00 00 00 00 00	FF 07 5A A2 01 00 00 00 00 00 00 00 00 00 00 00	
DAS95B70	A0 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
DAS95B80	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
DAS95B90	94 C2 CF 3F FB ED CF 01	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
DAS95BA0	F8 AD 02 87 A8 5B 78 83	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
DAS95BB0	00 00 00 00 00 00 00 00	0F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Identificador del Proceso
DAS95BC0	00 00 00 00 00 00 00 00	09 A7 77 83	
Direcciones virtuales de estructura _LIST_ENTRY.			
Se encuentran almacenados en LittleEndian y representan direcciones virtuales:			
FLINK: 8702ADF8			
BLINK: 837858A8			
Nombre del Proceso			System

Figura 9.3: Contenido del volcado de memoria en la ubicación donde se encuentra el proceso *System*, visto con un editor hexadecimal.

La adquisición del volcado de memoria es una tarea prioritaria en las actividades a realizar *in situ*, debido a la volatilidad de los datos y porque otras actividades a realizar en la escena (tareas de adquisición o triage) pueden afectar a la información presente en memoria.

## Volcado de memoria si se utiliza un software



El análisis forense informático debe tener en cuenta el nivel de volatilidad de los datos que se pueden convertir en información relevante a partir de la evidencia digital. La adquisición del volcado de memoria para llevar adelante un análisis forense del mismo, debe realizarse en los primeros instantes en los que se tiene contacto con el equipo, dado que el contenido de la memoria RAM cambia constantemente. La elección de la herramienta a utilizar para la adquisición del volcado de memoria es factor de éxito del posterior análisis.

## Bibliografía:

- ✓ **El Rastro Digital (Aspectos Técnicos, Legales y Estratégicos de la Informática Forense) – Autores Varios – Editorial Fasta 2017 – Cap. 4, 9.**
- ✓ **Wikipedia – Volcado de memoria.**