

# Automatización de Procesos de Análisis Forense Informático

Marcelo Rodríguez

Grupo de Seguridad  
Instituto de Computación  
Facultad de Ingeniería - UdelaR  
[marcelor@fing.edu.uy](mailto:marcelor@fing.edu.uy)

Jueves 24 de Junio, 2010



# Contenido

- 1 **Introducción**
  - Contexto
  - Definiciones
  - Proceso forense
  - Estado actual
- 2 **Trabajo realizado**
  - Objetivos y Metodología
  - Lenguaje utilizado
  - Herramienta desarrollada
- 3 **Conclusiones y Trabajo futuro**
  - Conclusiones
  - Trabajo futuro
- 4 **Referencias**

# Contexto

- A mediados de 2006 el GSI comienza a investigar sobre análisis forense (herramientas de recuperación de datos, kits anti-forenses, etc).
- En el 2007 se identifican objetivos y se busca relacionar con otras áreas de seguridad.
- En el 2009 se plantea un proyecto de grado (M.Barrere) con objetivos específicos y acotados.



# Definiciones

## Definición de ciencia forense digital

- Uso de principios y métodos científicos, aplicados sobre evidencia obtenida de fuentes digitales, con el fin de facilitar la reconstrucción de eventos dentro de un proceso legal (Digital Forensic Research Workshop DFRWS).



# Definiciones

## Definición de ciencia forense digital

- Uso de principios y métodos científicos, aplicados sobre evidencia obtenida de fuentes digitales, con el fin de facilitar la reconstrucción de eventos dentro de un proceso legal (Digital Forensic Research Workshop DFRWS).

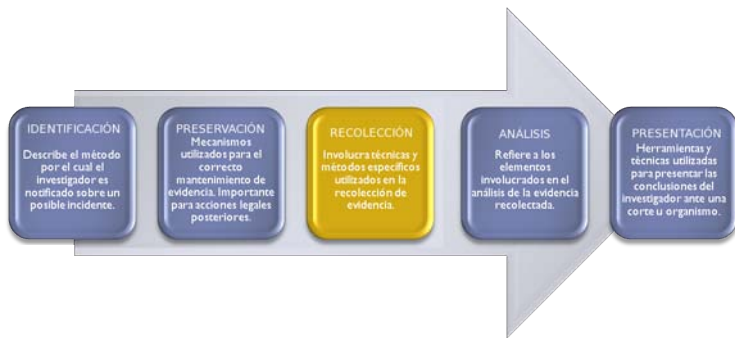
## Objetivos

- Confirmar el incidente ocurrido.
- ¿Quién? ¿Cómo? ¿Cuándo? ¿Desde dónde?
- Entender, corregir y protegerse de futuros compromisos.



# Proceso forense

- Etapas del proceso de una investigación forense



- Tratar de obtener la mayor información posible con el mínimo impacto.



# Estado actual

- Fortalezas.
  - Existencia de esfuerzos conjuntos por generar un marco de referencia consensuado dentro del ámbito forense.
  - Variedad de herramientas para recolección de evidencia volátil y no volátil.



# Estado actual

- Fortalezas.
  - Existencia de esfuerzos conjuntos por generar un marco de referencia consensuado dentro del ámbito forense.
  - Variedad de herramientas para recolección de evidencia volátil y no volátil.
- Debilidades.
  - Carencia de estándares rigurosos que definan las pautas generales de la actividad.
  - Herramientas desarrolladas con objetivos específicos y difíciles de extrapolar a otros entornos.



# Objetivos

- Investigar metodologías que describan los lineamientos de la actividad forense. (A Formalization of Digital Forensics)
- Contar con una infraestructura adecuada para plasmar los conceptos definidos en los procedimientos utilizados. (Lenguaje OVAL - Mitre Corporation)
- Contar con una herramienta que incorpore la metodología utilizando la infraestructura definida.



# Metodología

- Un ataque puede ser visto como un proceso que afecta a un conjunto de componentes sobre un sistema.
- Un procedimiento forense puede verse como un conjunto de primitivas forenses (métodos probados) que inspeccionan cada uno de los componentes afectados.

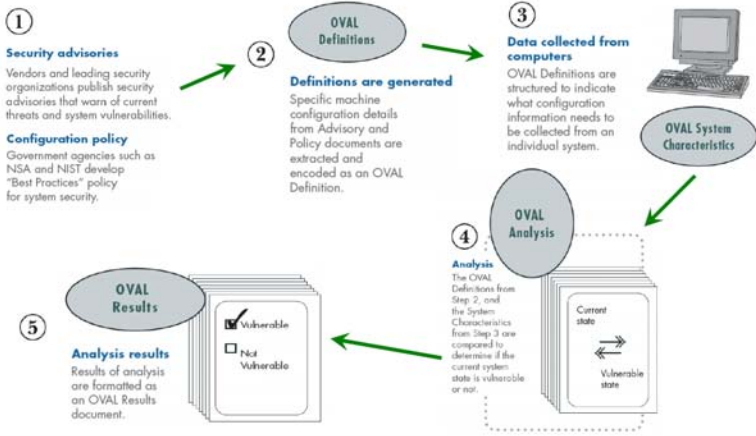


# Lenguaje OVAL

- OVAL (Open Vulnerability and Assessment Language) es un lenguaje orientado a la evaluación de sistemas en busca de vulnerabilidades o configuraciones específicas.
- Especificado mediante una colección de esquemas XML que permiten representar información de sistemas; expresar estados de máquinas específicos y reportar resultados de evaluación.



# Lenguaje OVAL II



# ¿Por qué OVAL?

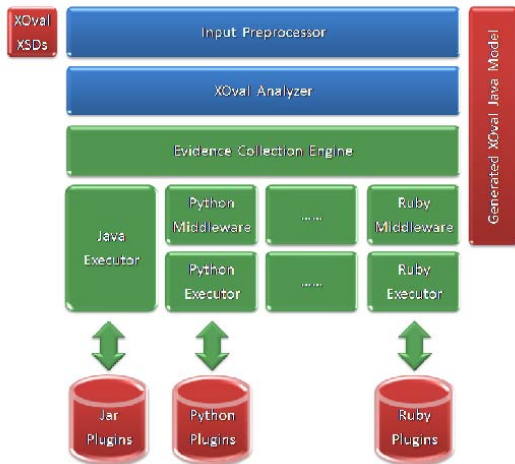
- Lenguaje desarrollado sobre un marco formal, altamente expresivo y poderoso.
- Fuerte tendencia a establecerse como estándar en la divulgación de contenido vinculado a la seguridad informática.
- Sus características estructurales lo hacen apropiado para dar soporte a los conceptos metodológicos establecidos.



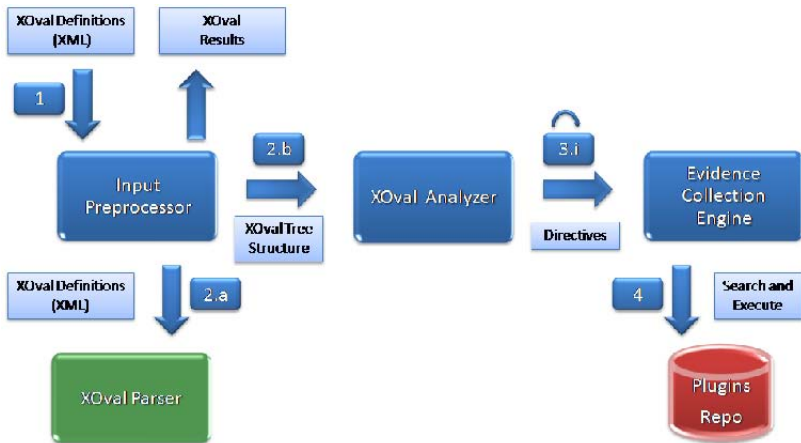
# Características

- Se extiende el lenguaje OVAL para soportar la metodología planteada. XOvaldi (eXtended Ovaldi)
- Herramienta desarrollada en Java. Permite su ejecución en múltiples plataformas.
- Recolección de evidencia digital basada en plugins diseñados para las diferentes plataformas de interés.
- Extensibilidad sin afectar el núcleo de la herramienta.
- Ejecución desde medios extraíbles como unidades flash USB o CDs.

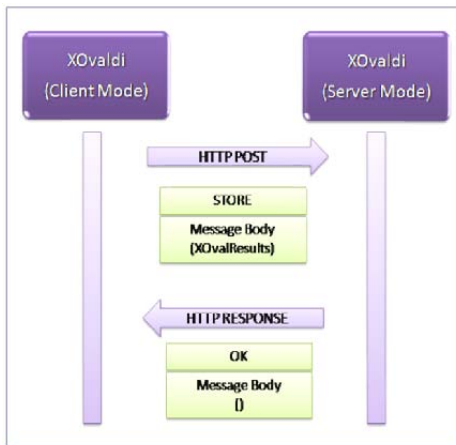
# Arquitectura de la herramienta



# Funcionamiento de la herramienta



# Modalidades de uso



# Conclusiones

- Se ha propuesto un modelo de trabajo para la etapa de recolección de evidencia digital.
- La capacidad de especificar procedimientos forenses y su evaluación automatizada permiten que:
  - Analistas especializados especifiquen qué es lo que se debe hacer, e incluso cómo, desarrollando los plugins apropiados.
  - Quien hace la recolección no necesariamente debe ser un experto en la materia.
  - Se reduzca el espacio de errores basándose en los mecanismos automáticos de recolección.



# Trabajo a futuro

- Repositorio de Elementos Dinámicos Online.
  - Útil sobre todo en ambientes distribuidos con gestión centralizada de recolección de evidencia.
- Editor de Procedimientos Forenses.
  - Especificaciones extensas, propensa a errores.
- Aspectos legales.
  - Analizar mecanismos de almacenamiento, integridad de la evidencia, trazabilidad, cadena de custodia, etc.
- Investigar sobre la automatización de otras etapas del proceso forense de una manera correlativa.



# Referencias

-  MITRE Corporation.  
*OVAL - Open Vulnerability and Assessment Language .*  
<http://oval.mitre.org/>.
-  Gary Palmer, The MITRE Corporation.  
*A Road Map for Digital Forensic Research.*  
TECHNICAL REPORT.
-  Ryan Leigland and Axel W. Krings.  
*A formalization of digital forensics.*  
Article - International Journal of Digital Evidence.
-  M. Barrere.  
*Análisis Forense Informático.*  
Tesis de grado 2009.

