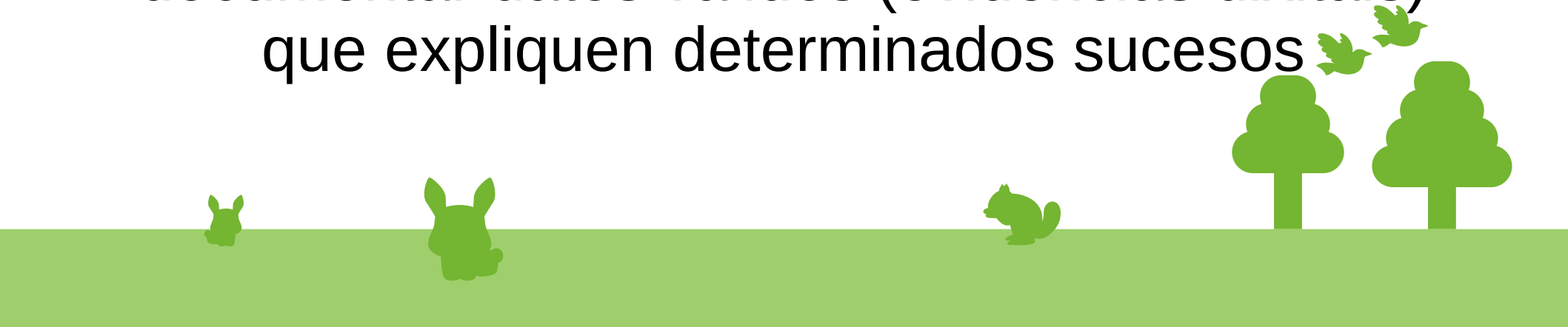
Introdución ao Análise Forense

Proceso de Investigación mediante técnicas científicas e analíticas especializadas que permiten identificar, preservar, extraer, analizar e documentar datos válidos (evidencias dixitais) que expliquen determinados sucesos



Introdución ao Análise Forense

- Normalmente o análise forense debe facerse seguindo os procedementos necesarios que permitan que a información obtida sexa utilizable en procedementos legais.
- Analiza os sistemas informáticos, dispositivos de almacenamento, redes...
- O Obxectivo é reconstruír accións e identificar infraccións ou delitos dixitais

Conceptos Básicos

- Informe Pericial
  - Documento elaborado polo perito informático detallando o proceso de investigación e as evidencias atopadas presentando as súas conclusión.
- Informática Forense
  - Rama da informática adicada a investigación de incidentes relacionados coa ciberseguridade (ataques, roubo de datos, accesos non autorizados, recuperación de información...)
- Evidencia Dixital
  - Calquera información ou dato almacenado ou transmitido que poda ser utilizado como proba nunha investigación

Metodoloxía

- Plan de Adquisición
  - Debe detallar os dispositivos e datos que se van a adquirir e as ferramentas e técnicas a empregar
- Cadea de Custodia
  - A evidencia debe ser rastrexada dende o momento da adquisición ata a súa presentación
- Rexistro de Métodos, Procedementos e Tecnoloxías
  - Todos os pasos e procedementos deben ser documentados no informe final.

A Evidencia Dixital

- Obtida Lícitamente
- Orixe Garantido
- Integridade Garantida
- Pertinente, Útil e Clara

Fases do Analise

- Adquisición de Datos
  - Pode ser en frío ou en quente
  - Imaxes de Discos: logs, recuperación de información
  - Clonación da RAM
- Análise de Datos
  - Busca de patróns anormales
- Informe de Conclusións

Adquisición de Datos

- Multiples Ferramentas:
  - EnCase, FTK, WireShark, PartClone, Recuva, TestDisk
  - Máquinas de clonación de discos
- Multiples Obxectivos:
  - Arquivos borrados
  - Logs
  - Memorias Caché
  - Configuración da Rede
  - Arquivos temporais do sistema
  - Contido do Swap y si é posible da RAM
  - Aplicacións Instaladas
  - Ficheiros Descargados.
  - Análise de Metadatos

Análise de Evidencias

- Identificación das Evidencias
- Aseguramento das Evidencias
- Documentación das Evidencias
- Establecemento da Cadea de Custodia