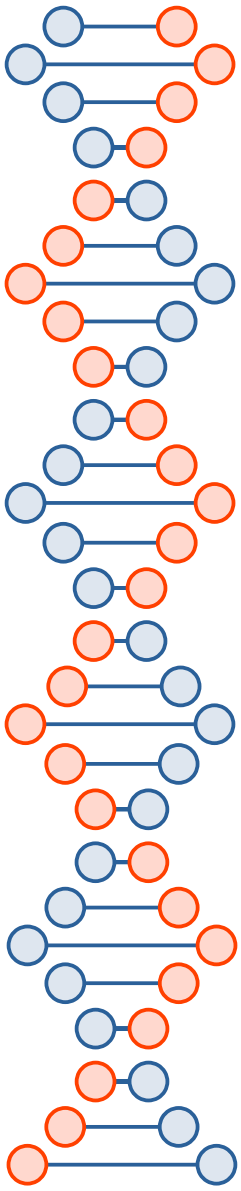
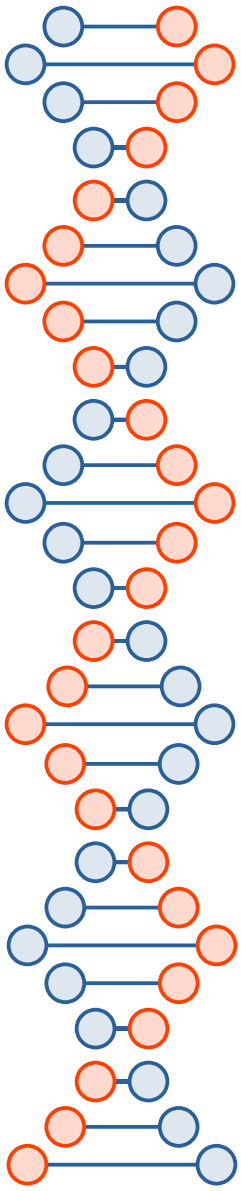


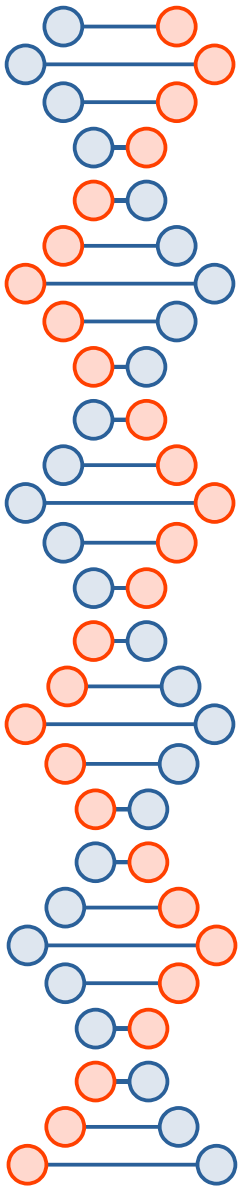
UD1 – Adopción de Pautas de Seguridade Informática

Introdución ao Análise Forense



Introdución

- O análise forense consiste na *aplicación de técnicas científicas e analíticas especializadas que permiten identificar, preservar, analizar e presentar datos válidos que expliquen determinados sucesos*.
- Un informe pericial está realizado por un perito informático para a súa presentación nun proceso legal
- A informática forense permite solucionar conflitos tecnolóxicos relacionados coa seguridade e a protección de datos. É importante na persecución de delitos contra a privacidade, competencia desleal, fraude, roubo de información e espionaxe industrial cometidos mediante o uso de tecnoloxías da información
- A **evidencia dixital** é o conxunto de información de valor para unha investigación que se almacena, recibe ou transmite por un dispositivo electrónico. Esta evidencia se obten cando os dispositivos se aseguran para o seu exame
- Un dos obxectivos é recrear o ocorrido nun dispositivo dixital durante un incidente de seguridade de xeito que o análise da incidencia permita impedir que se repita no futuro.



A evidencia dixital

A evidencia dixital:

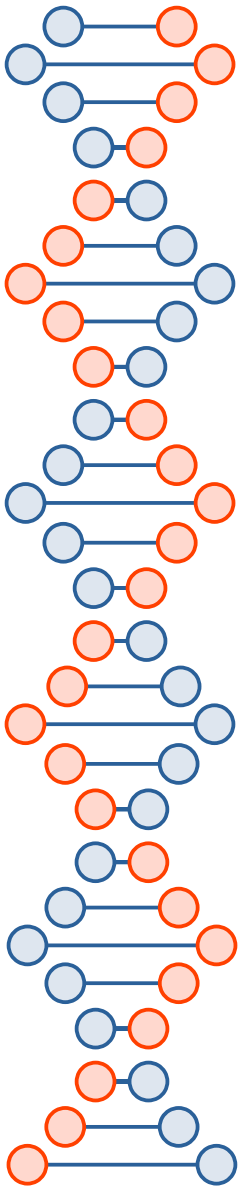
- Está oculta, e necesario sacala a luz mediante o exame forense
- Pode ser danada, alterada ou destruída facilmente
- Pode ser sensible ao tempo
- Pode cruzar rápida e facilmente fronteiras xuridiscionais

A fonte da evidencia dixital pode ser numerosa:

- Ordenadores
- Dispositivos independentes baseados en internet (routers, proxys, ...)
- Dispositivos móbiles

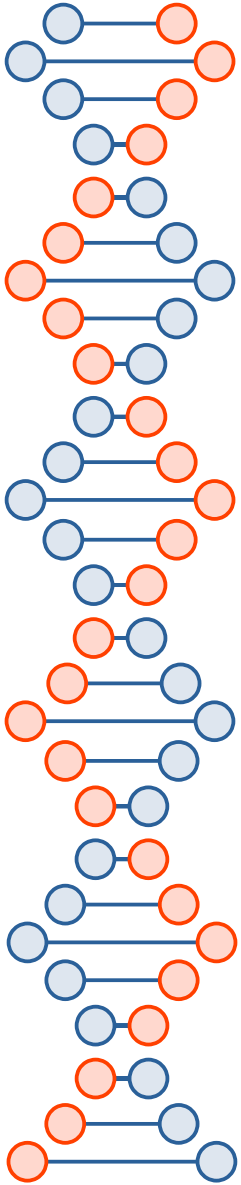
Un análise cumpre os seus obxectivos cando:

- Se coñece a causa do incidente e as súas circunstancias
- Se coñece a identidade e obxectivos dos atacantes
- Se coñece o momento en que se produciu o suceso e se teñen as evidencias que o demostran



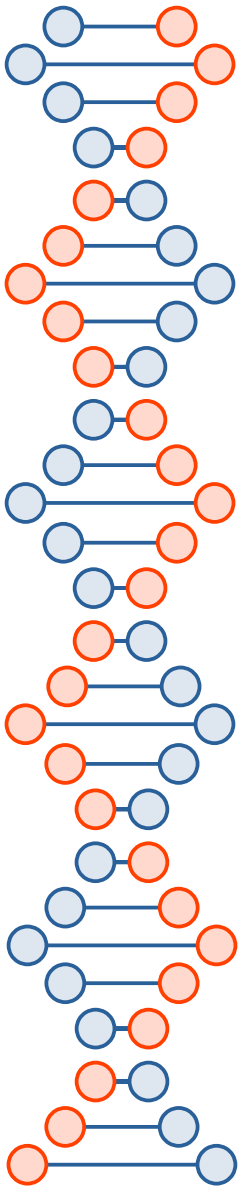
Fases do Análise Forense

- **Adquisición de datos**: Se deben identificar as fontes das evidencias e preservalas para evitar calquera modificación accidental. A adquisición se pode realizar na escena do incidente ou no laboratorio informático.
- **Análise de datos**: Consiste en indexar e recopilar a información pertinente de entre todos os datos adquiridos.
- **Informe de conclusións**: Se detallan todas as actividades do proceso de investigación e as conclusións obtidas respecto a información dispoñible e os obxectivos perseguidos.



Metodoloxía e Boas Prácticas

- Se debe establecer un Plan de Adquisición, que indique un método de recolección de evidencias sistemático e documentado.
- Se debe establecer unha cadea de custodia con etapas ben descritas e documentadas:
  - Identificación, extracción e rexistro da evidencia
  - Preservación e almacenamento da evidencia
  - Traslados das evidencias
- Se deben indicar a tecnoloxía e recursos empregados no análise, describir o contorno de traballo e anotar os procedementos seguidos.

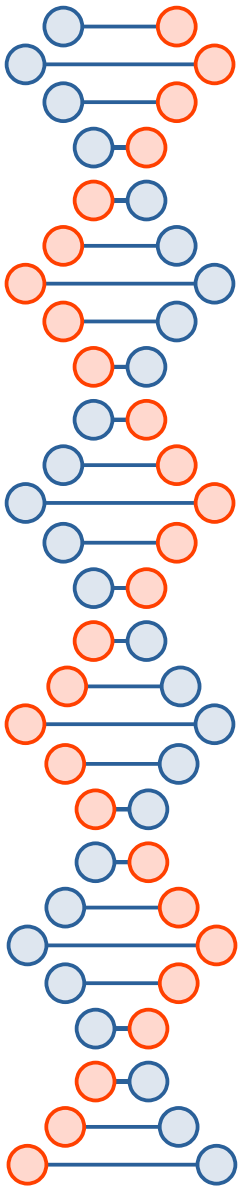


Orixes de información forense

- Contido dos Discos (Ficheiros, e-mails, etc)
- Recuperación de ficheiros borrados
- Historial de conexión a redes e a internet
- cachés do navegador
- tablas de enrutamento e caché arp
- arquivos temporais
- Contactos, axendas e mensaxería
- Programas instalados
- Ficheiros descargados e Compartidos
- Rexistros do sistema (logs)
- etc.

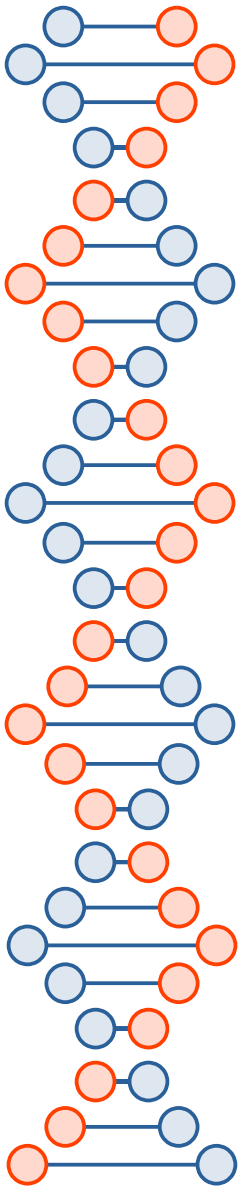
Requisitos da evidencia dixital

- Debe ser obtida lícitamente (articulo 11 da LOPJ)
  - Dereito do afectado a intimidade na obtención da proba dixital.
  - Segredo nas comunicacións e protección de datos persoais
  - Inviolabilidade do domicilio
- Debe garantizarse a autoría do aportado como proba
- Debe garantizarse a integridade das probas, sendo fundamental a cadea de custodia.
- Debe ser pertinente aos feitos do litixio
- Debe ser útil para aclarar a disputa
- Debe ser clara, de xeito que todos os intervinientes podan comprendela.



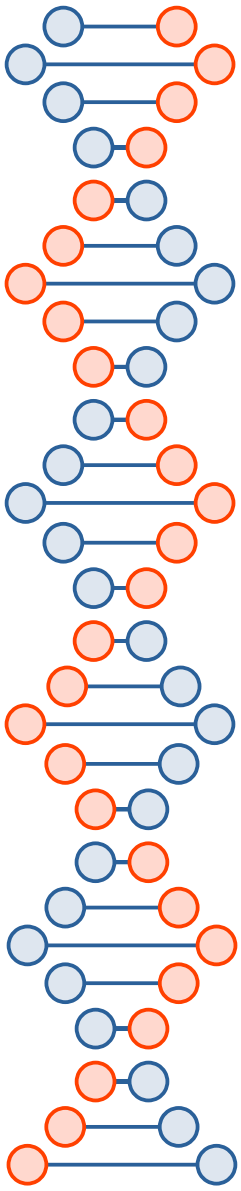
Preparación para a investigación

- Os procesos de análise son de gran consumo e requiren hardware potente
- Debe ser posible analizar multiples sistemas, a compatibilidade é básica a nivel de conexións de dispositivos, sistemas operativos ou lectura de datos.
- Debe dispoñerse de abundante espazo de almacenamento para almacenar as evidencias e se deben realizar copias de seguridade.
- Se debe valorar o uso de bolsas antiestáticas, caixas apropiadas (acolchadas, etc), xaulas de faraday, cámaras de fotos ... etc.
- Se debe dispoñer de software de adquisición e análise de datos. Podemos distinguir entre “suites” e ferramentas especializadas. As “suites” proporcionan un conxunto de ferramentas para todo tipo de investigación forense (Autopsy/Sleuthkit, Digital Forensics Framework, Encase...). Ferramentas especializadas típicas son dd, editores hexadecimais... etc.



Adquisición de Datos I

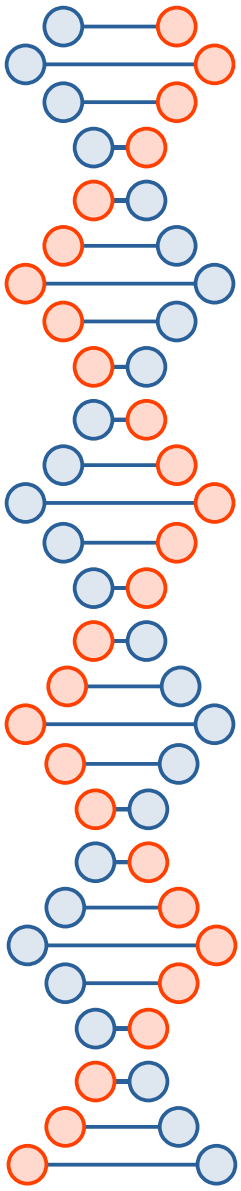
- A adquisición dos datos depende do tipo de incidente que esteamos a analizar. E importante identificar o incidente, notificar aos afectados si a regulación o require (LOPD) e garantir a conservación das evidencias.
- Os datos non se adquiren sobre o os dispositivos orixinais que deben preservarse no posible no seu estado orixinal.
- As accións deben axustarse a un plan meditado e previsto.
- As actuacións son moi diferentes si os equipos están encendidos ou apagados.
  - A actuación sobre equipos apagados se chama **análise post-mortem**. Nestes casos é máis fácil preservar as evidencias, pero se perde a información volátil.
  - A actuación sobre equipos encendidos se chama **análise en vivo**. Nestes casos é posible moitas veces acceder a dispositivos cifrados ou ao contido da memoria RAM e os arquivos temporais, pero é moito máis complexa a preservación de evidencias polo que non sempre é posible.
- A adquisición de datos máis común é a adquisición estática mediante extracción de información de discos fixos, tarxetas SD, memorias USB... xerando unha imaxe que se analizará posteriormente.
- Se debe garantizar que os datos orixinais non son modificados para o que se debe acceder a eles en modo so de lectura, incluso utilizando dispositivos hardware protectores contra escritura.
- No caso de captura de datos en vivo e importante que tanto o software instalado como o dispositivo destino da captura sexa externo (USB)



Adquisición de Datos II

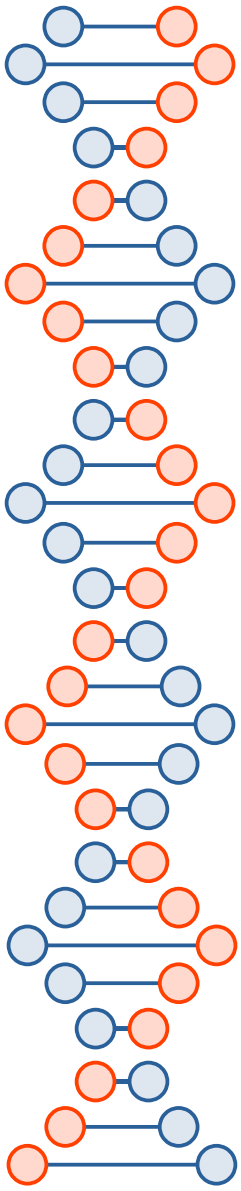
Típicamente se recopilan:

- Data e hora do sistema
- Instantánea dos dispositivos de almacenamento e busca de arquivos borrados.
- Portos TCP/UDP activos e aplicacións conectadas ou en espera de conexión.
- Usuarios activos no sistema
- Procesos en funcionamento no sistema
- Configuración de rede (ip, rutas e caché ARP)
- Logs do sistema
- Análise do tráfico de rede



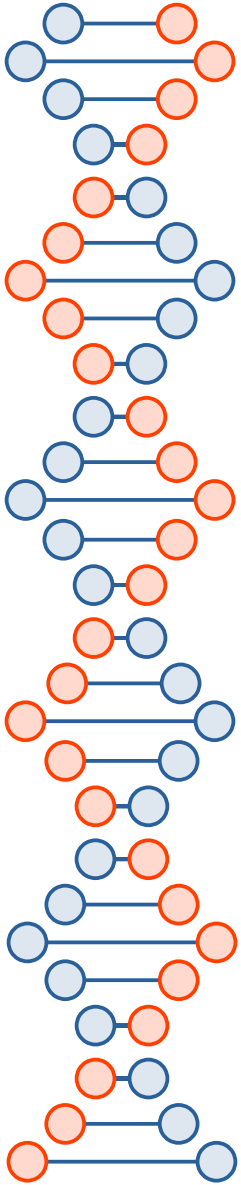
Adquisición de datos III

- Copias de memoria: /dev/mem, LIME (lime-forensics-dkms), FTK Imager
- Imaxes de disco. ***dd***, FTK Imager, Caine Linux GuyManager
- Uso de hardware forense: Clonadores de disco, bloqueadores de escritura, estacións forenses. (https://ondatashop.com/equipo-forense-velociraptor-7)
- Se debe evitar a escritura no disco orixinal, para o que e imprescindible montalo en so lectura utilizando si é necesario bloqueadores de escritura hardware / Clonadoras de disco
- Unha firma hash MD5 ou SHA-1 pode garantizar a integridade das imaxes.



Análise de Evidencias

- Identificación de evidencias
  - As ferramentas de análise de imaxes de disco nos proporcionan acceso ao contido aínda que fora borrado.
  - Se deben definir os criterios de busca segundo a investigación a realizar
  - Mediante “carving” é posible extraer información eliminada (photorec/testdisk, scalpel, foremost,WinUndelete ...)
- Aseguramento das evidencias
  - Deben almacenarse en lugares de acceso restrinxido e con control ambiental
  - Se debe traballar con protección contra picos de corrente ou cortes de luz, nun ambiente limpo e estable.
  - No caso de dispositivos móbiles deben usarse jaulas de Faraday e usar packs de baterías para evita que se descarguen. O dispositivo rexistrará ese feito que se debe documentar.
- Documentación das evidencias
- Establecemento da cadea de custodia



Normativa

- ISO/IEC 2037: Directrices para identificación, recopilación, adquisición e preservación de evidencias dixitais.
- ISO/IEC 27042: Normas para análise e interpretación de evidencias dixitais.