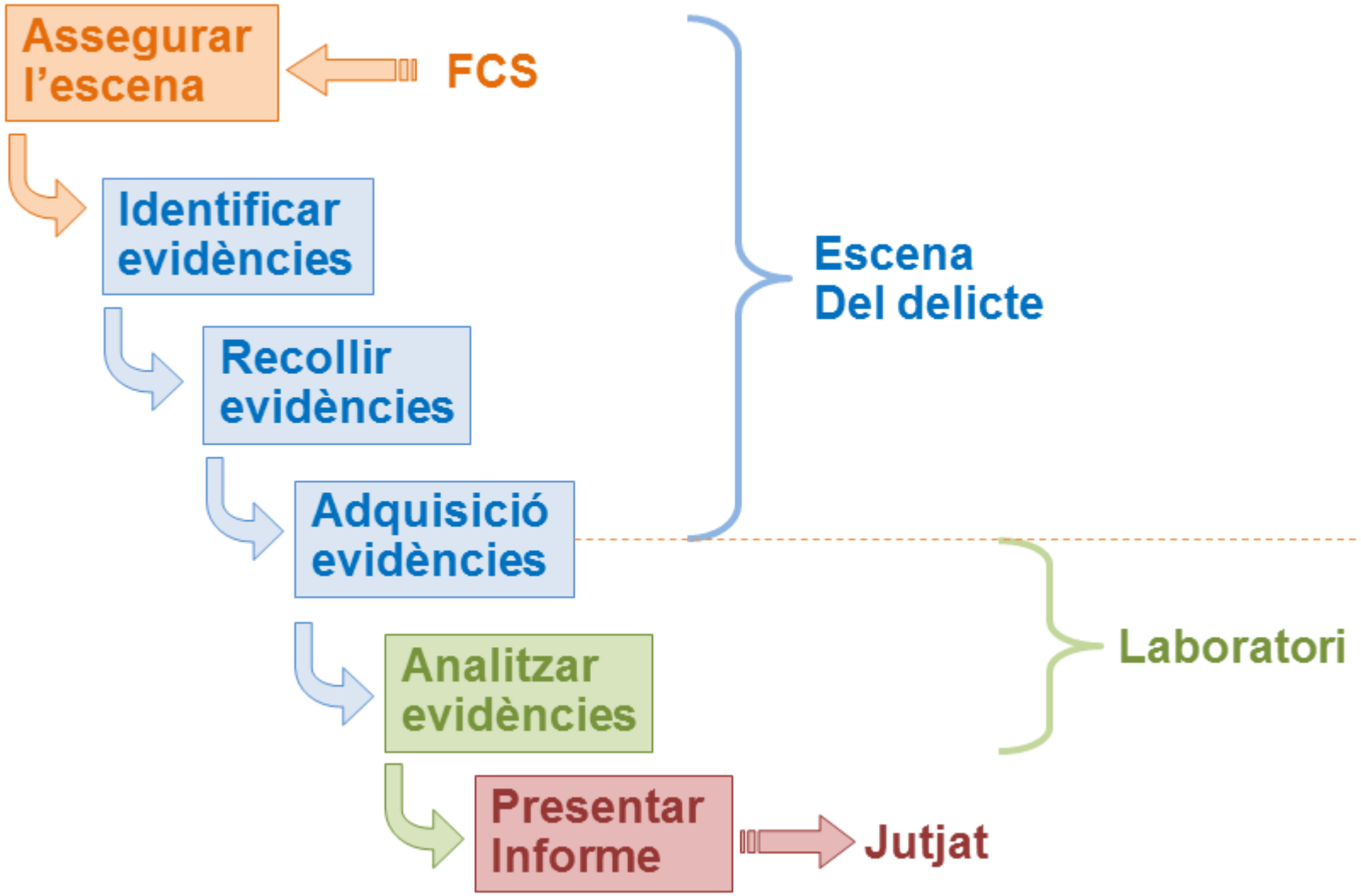
ANÀLISI FORENSE INFORMÀTIC

Xavier Baubés Parramon

Què és l’anàlisi forense informàtic?

- És una disciplina que combina el dret i la informàtica per recopilar i analitzar dades de sistemes informàtics i xarxes d'una manera admissible com a prova en un tribunal.
- Les tècniques són reactives, s'accedeix al sistema un cop aquest ha sigut danyat: Reconstrucció de l'actiu informàtic, obtenció de dades residuals, autenticació de dades, etc

Etapes de l'anàlisi forense (I)



Etapes de l’anàlisi forense (II)

- Assegurar l'escena: Per part de les Forces i Cossos de Seguretat de l'Estat (FCS).
- Identificar evidències: Recerca, reconeixement i documentació de l'evidència digital en l'escena de l'incident.
- Recollir evidències: Aquí els dispositius que potencialment poden contenir evidències digitals, són recollits i transportats a un laboratori.

Etapes de l’anàlisi forense (III)

- Adquisició d'evidències: La creació d'una còpia bit a bit de l'evidència continguda en els dispositius digitals, així com la documentació dels mètodes emprats i dels passos realitzats.
- Analitzar evidències: S’estudien les evidències digitals i s’elaboren les hipòtesis.
- Presentar informe: S'elaborarà un informe pericial. L'informe s'adreça sovint a persones no tècniques en la matèria, cal que contingui descripcions i indicacions clares.

Principis davant les evidències

- Captura una imatge del sistema.
- Fer notes detallades.
- Minimitzar els canvis en la informació que s'està recopilant i eliminar els agents externs.
- Recopilar la informació abans d’analitzar-la.
- Recopilar informació per ordre de volatilitat.
- La recopilació d'informació es realitza de forma diferent segons els dispositiu.

Ordre de volatilitat

- Es refereix al període de temps en què determinada informació és accessible. Primer s'ha de recopilar la informació que estarà disponible durant el període de temps més curt, és a dir, aquella que tingui una volatilitat més gran.
- La memòria RAM, la caché i la informació temporal del sistema que podem trobar en un ordinador obertes tenen màxima prioritat.

Cadena de custòdia

- Consisteix en un informe detallat que documenta la manipulació i l'accés a les proves objecte d'investigació. La informació continguda en el document s'ha de conservar adequadament i mostrar les dades específiques, en particular tots els accessos amb data i hora.
- Cal conèixer tots els detalls sobre com es va gestionar l'evidència a cada pas del camí. Documentar per cada prova el "qui, quin, quan, on, per què i com".