De case

Deze ochtend is een melding binnen gekomen van een inbraak bij kermis PvIB. Naast inbraakschade zijn ook de electronische tags (e-tags) gestolen van medewerkers van de ticket balie. Het is onbekend waarom juist deze e-tags gestolen zijn. De kermis is niet in staat om nieuwe e-tags te maken voor het einde van de dag.

Er zijn drie verdachte personen gezien ten tijde van de inbraak. De drie verdachten zijn opgepakt, maar moeten nog verhoord worden.

De opdracht

Om de zaak op te kunnen lossen is de recherche ingezet. Daarnaast is de hulp van een digitaal forensisch onderzoeker ingeroepen om te achterhalen of de dader(s) sporen hebben achtergelaten op de PC waar de e-tags digitaal opgeslagen zijn.

Recherche

De opdracht van de recherche is bewijslast verzamelen zoals vingerafdrukken, schoenafdrukken, DNA of ander bewijsmaterial dat mogelijk aan één van de drie verdachten gekoppeld kan worden. Daarnaast moeten de drie verdachten verhoord worden. Het gaat om:

- E. K.
- J. J.
- P. v/d H.

Digitaal forensisch onderzoeker

De opdracht van de digitaal forensisch onderzoeker is in kaart brengen hoe het mogelijk is gebleken om de e-tags te stelen en bewijslast te verzamelen dat mogelijk aan één van de drie verdachten gekoppeld kan worden.

Wat al bekend is

Er is bekend dat maar één persoon toegang mag hebben tot de computer. In het verleden hebben ze nog een medewerker gehad dat toegang heeft gehad, maar de kermis is niet zeker of de rechten van deze persoon ingetrokken zijn.

De dader(s) moet bekend zijn geweest met de locatie van de omputer aangezien andere waardevolle spullen niet meegenomen zijn.

Er is een extern bedrijf ingehuurd voor het ontwikkelen van de e-tag manager. Dit bedrijf claimt geen toegang te hebben tot de betreffende computer en dat de applicatie jaarlijks onderworpen is aan een penetratietest. De applicatie heeft echter geen audit trail, waardoor niet te zien is wie ingelogd heeft en welke acties uitgevoerd zijn.

Hoe om te gaan met bewijslast

Indien een notitie gemaakt moet worden met betrekking tot het onderzoek, dan moet de vlag genoteerd worden. De vlag ziet er als onderstaand uit, maar het kan zijn dat de data tussen de brackets omgedraaid moeten zijn:

Flag {.....}

Het OM zit er op te wachten, dus de deadline is vandaag!