GPS Forensics IV: Anti-Forense e Perspectivas

Como verificado, informações de GPS são cada vez mais comuns e claramente, podem significar muito em uma investigação de criminal ou de um incidente de qualquer natureza. O profissional de forensics deve se habituar a conhecer os sistemas de arquivos dos principais fabricantes, como TomTom, Garmin e Megallan, tendo também noção dos equipamentos "genéricos" existentes no mercado.

Para conhecer a estrutura de arquivos de outros fabricantes acesse: http://www.forensicswiki.org/wiki/Global_Positioning_System

A tendência é que tenhamos equipamentos com outras funções como conexão wireless, aplicações de escritório dentre outros, o que demandará do perito necessidade de estrutura para clonagens dos discos que já ultrapassam 20Gbytes em alguns modelos.

O perito deverá se habituar e certamente receberá no futuro casos onde poderá verificar que a origem de um e-mail partiu de um GPS ou mesmo a contrafação de conteúdo protegido por direito autoral (como e-books, músicas e vídeos) dentro dos dispositivos.

Será crescente o uso de máquinas digitais e celulares que contém GPS *receivers* embutidos, logo, tais máquinas registram latitude e longitude em metadados das imagens, denominados EXIFs, informações que podem ser extraídas pelo perito com ferramentas como jhead (http://www.forensicswiki.org/wiki/Jhead) .

Assim, o perito, sem desprezar as ferramentas que já possui para coleta e preservação de evidências, deverá se familiarizar com ferramentas específicas, como BlackThorn2

(http://www.blackthorn2.com/index.html) Igualmente, já pode buscar no exterior certificações específicas para GPS Forensics (http://www.berlacorp.com/training_advgps.html)

Será crescente a atividade pericial de rastreadores de veículos de empresas, em relações trabalhistas, eis que equipados com GPSs. Além de periciar o equipamento, o perito também terá a tarefa de analisar servidores dos dados recebidos e demais estações intermediárias.

Terá que lidar com técnicas anti-forense como *"GPS Jamming"*, dispositivos vendidos na Internet com capacidade de bloquear os sinais dos equipamentos, despistando um trajeto, impedindo o rastreamento. Interferência GNSS e falsificação de sinal serão outras técnicas que poderão iludir um policial indicando um caminho, quando na verdade o criminoso segue por outro. (http://www.gpsworld.com/defense/security-surveillance/expert-advice-gps-forensics-crime-and-jamming-8986)