# GPS Forensics III: Apreensão, transporte e análise

Ainda não pensamos em “rootkits” para GPS, logo, até o momento tão logo tenha contato com a evidência, a desligue utilizando os comandos apropriados. Tenha em mente que o dispositivo está trocando informações com o Satélite, o que poderá sobrescrever dados na memória. Congele o estado do dispositivo, mas antes de desligar, cheque a versão para analisar se nenhuma senha será solicitada no *bootloader.*

Policiais também devem considerar que antes de removerem veículos para delegacias ou pátios, devem observar se não existe dispositivo GPS, pois caso exista, devem manter o veículo no local até a chegada da perícia ou profissional com habilidades para desligamento forense ou até mesmo primeiras coletas.

Lembrando que os GPSs podem ter até 2gb de memória (TomTom) e buscam informações nos satélites U.S. NAVSTAR Global

Positioning System (GPS), como aliás ocorre com a grande maioria dos modelos no mercado.

O examinador também deve ter uma estação forense própria para análise e ter a certeza que não está periciando o GPS em um PC que existam drivers do dispositivo. Com os drivers, ao detectar a conexão de um dispositivo, a aplicação irá rodar atualizações de mapas e outras informações, o que poderá destruir a evidência necessárias.

Se o GPS indicar como último ponto de partida o endereço da delegacia de polícia… Concluam como desejarem!

Já no equipamento (TomTom), alguns arquivos são relevantes, os quais podemos citar:

- **MAPSETTINGS.CFG** – Contém informações sobre mapas, itinerários e endereços nos favoritos;
- **CURRENTLOCATION.DAT** – Contém a última posição do dispositivo quando foi desligado;
- **SETTINGS.DAT** – Pode conter informações sobre provedor wireless, conexões e dispositivos móveis conectados;
- **Arquivos .ITI** – Em alguns modelos também armazenam itinerários.

Para a análise dos arquivos em padrão DAT, recomendamos a ferramenta PoiEdit, capaz de exibir todos os registros armazenados em tais arquivos. (http://www.poiedit.com/screenshots.htm).

# CNASI: Painel sobre mobilidade, segurança e privacidade

No dia 19/10/2010 participamos um painel no CNASI – Congresso Latinoamericano de Auditoria de TI, Segurança da Informação e Governança.

Nosso Painel foi sobre "Painel Mobilidade
Mobilidade: privacidade, questões Legais de Segurança". Tive a honra de reencontrar amigos e profissionais como Denny Roger – CEO -EPSEC e Jaime Orts Y Lugo – Presidente ISSA – Information Systems Security Association. O debate abordou questões como uso de internet desprotegida para atos ilícitos, responsabilidade civil e do empregador por atos de seus executivos.

Estimativas revelam que 4 entre 5 executivos do mundo utilizam os dispositivos móveis para negócios. A questão que não cala é: Eles sabem dos riscos? Os equipamentos contram com segurança e criptografia?

Agradeço o IDETI pelo convite à palestrar no evento! O debate foi filmado e em breve disponibilizaremos os links para o download!