Mobile Forensics: Extraindo informações em Celulares

Em um de nossos treinamentos em perícia em dispositivos móveis fomos indagados sobre a real popularidade de tais ferramentas junto à Polícia Investigativa. Embora no Brasil ainda a procura seja modesta na área policial, lá fora a situação é diferente. A Polícia de São Francisco na Califórnia, por exemplo, segundo o site http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/09/08/BUPA12OC2V.DTL já utiliza a tecnologia. Dispositivos de investigação móvel como Cellebrite (o meu preferido), Data Pilot e o Oxygen Software tem se difundido na área da perícia computacional.
E porque alguém se preocuparia com celular ? Segundo um entrevistado Sfgate:

"The reason why the cell phone is important is that you are carrying around a personal diary of who you talk to and often what you talked about," Morgester said in reference not to conversations but rather to texting, adding: "Youth today communicate through MySpace and texting." Disse o Procurador Robert Morgester ao Sfgate.com.

Até mesmo toques e ringtones podem ser úties. Em um inquérito na Califórnica, uma testemunha recordou uma sinfonia durante o cometimento de um crime. Não é prova, mas um indício.Embora

popular, a briga nos Estados Unidos está em torno da constitucionalidade ou não destes dispositivos, briga acirrada envolvendo inlusive o Jurídico da EFF (Eletronic Frontier Foundation)
E lá, o mandado de busca e vistoria é necessário? Parece que os Tribunais não vêm exigindo o Mandado para que a polícia saia recuperando SMS apagados e imagens de celulares de meros investigados:
"So far, most court decisions involving this new technology have allowed police officers to use forensic devices to extract information without a warrant. But civil libertarians favor one ruling by a federal judge in San Francisco that pushed the sliding scales toward requiring a warrant to search cell phones in most cases."
Na matéria feita pelo SFGate, o Perito afirma que a necessidade de mandado é uma "zona cinzenta" e que em determinados casos urgentes como homicídios e sequestros em São Francisco, o papel pode ser substituido por uma "delcaração do Oficial". (A validade disso no direito brasileiro é zero, isso só cola lá em cima mesmo)
Deve-se destacar também que tais dispositivos de recuperação de dados em celulares possuem criptografia Md5, que mantém intacta a integridade do material coletado… Em partes…Pois segundo Nate Lawson, da Oakland Consulting, a criptogragia do Cellebrite pode ser quebrar possibilitando ao manipulador "plantar provas" sem ser detectado. Argumenta que o ideal seria a criptografia SHA-256. Já a equipe Cellebrite alega que somente os melhores hackers do mundo podem realizar tal façanha:
"Cellebrite's Ofrat said that despite the theoretical possibility of hacks to MD5, the likelihood is low. "You'd have to have the best hacker in the world," he said. But his firm is studying SHA-256 and will move to that if it becomes an industry standard, he said."