Análise Forense em iPhone/iPod Touch

Ivo de Carvalho Peixinho
Perito Criminal Federal
peixinho.icp@dpf.gov.br

São Paulo (SP), Novembro de 2008

Agenda

- Introdução
- Arquitetura
- Diferenças iPhone/iPod Touch
- Acessando o iPhone
- Copiando o *filesystem*
- Análise forense da imagem
- Conclusões

Introdução

- iPhone
  - Telefone celular
  - 8Gb e 16Gb
  - Bluetooth (fone de ouvido)
  - Wi-Fi
  - GPRS/EDGE/3G/AGPS
  - Mp3 e vídeo
- iPod Touch
  - Tocador mp3 e vídeo
  - Wi-Fi
  - 8Gb, 16Gb e 32Gb

Introdução

- Celular comum
  - Agenda
  - SMS
  - Ligações
  - Fotos
- iPhone
  - Email
  - Páginas HTML
  - Arquivos pdf, word, ppt, excel
  - Vídeos
  - Programas (v2.x)

A análise é a mesma?

Arquitetura

- Primeira geração
  - CPU: Samsung/ARM S5L8900B01 512Mbit SRAM
  - EDGE: Infineon PMB8876 S-Gold 2 EDGE Baseband Processor
  - GSM: Infineon M1817A11 GSM RF Transceiver
  - Disk: Samsung 65-nm 8/16GB MLC NAND Flash
  - Amplifier: Skyworks SKY77340-13 Signal Amplifier
  - Wireless: Marvell 90-nm 88W8686
  - I/O Controller: Broadcom BCM5973A
  - Flash Memory: Intel PF38F1030W0YTQ2 (32M NOR + 16M SRAM)
  - Audio: Wolfson WM8758
  - Bluetooth: CSR BlueCore 4
  - Touchscreen: Philips LPC2221/02992

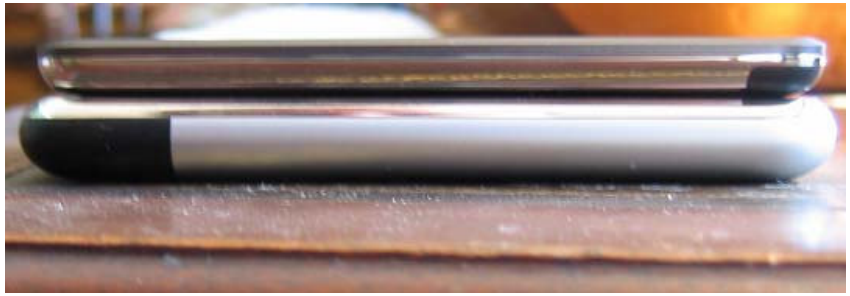
Arquitetura

- Sistema operacional
  - Versão *mobile* do Mac OS X 10.5 (Leopard)
  - Diversas similaridades com a versão *desktop*
    - File system do disco: HFS/X (Apple)
- Mac OS iPhone vs Mac OS PC
  - Arquitetura ARM (Advanced RISC Machine)
  - Hardware especial
    - Acelerômetro, sensor de proximidade, tela multi-touch, GSM, Wi-Fi, Bluetooth, etc.
  - Interface customizada
    - Frameworks (controles *finger friendly*)
  - Kernel assinado pela Apple
    - *Jailbreak*

Diferenças iPhone / iPod Touch

- Ausências
  - GSM/EDGE
  - Bluetooth
  - Alto falante
  - Microfone
  - Câmera

O iPod Touch é um iPhone sem Celular e Bluetooth: Mesmas técnicas de análise



Acessando o iPhone

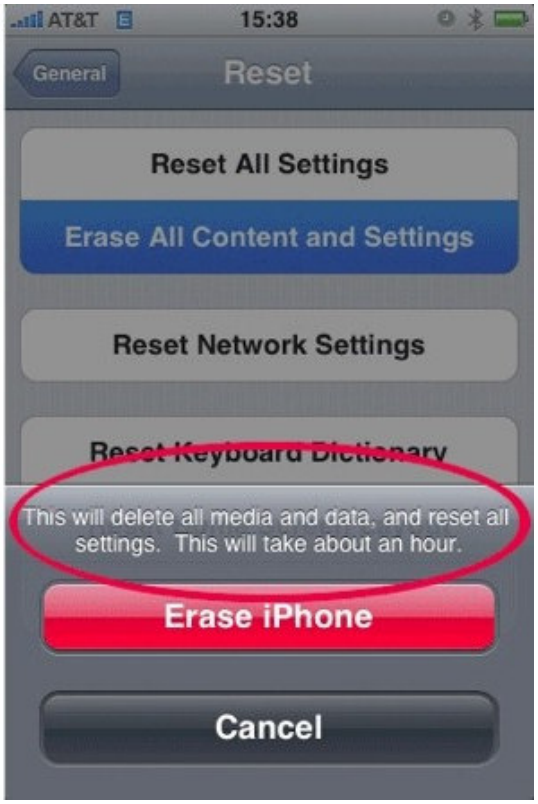
- iTunes
  - Ferramenta Apple para acessar o iPhone
  - Sincronizar música, vídeos, contatos, configurações, fotos, *podcasts,* contas de email, *bookmarks* e aplicações
  - Atualizações e recuperação do *firmware*
    - Restaurar um iPhone ao estado de fábrica
  - iTunes Store

Acessando o iPhone

- Restaurar um iPhone ao estado de fábrica?
  - **Refurbished iPhones are an excellent source of previous users' data**
    - Engadget: http://www.engadget.com/2008/05/20/refurbished-iphones-are-an-excellent-source-of-previous-users-d/
  - Função restore do iTunes e “erase all settings” do aparelho não apagam totalmente os dados do iPhone.
    - Análise forense pode recuperar os dados

Acessando o iPhone

- Versão 2.0 do software aparentemente apaga os dados de forma segura
- Possível técnica anti-forense
- Ainda não testei ☺



Acessando o iPhone

- Best anti-forensics for iPhone EVER!!

Acessando o iPhone

- Onde vou achar um liquidificador tão legal????
  - Na casa do pão de queijo!!!
  - Aeroporto de Brasília

Acessando o iPhone

- Acesso físico ao disco do iPhone
  - Possibilidade de recuperação de informações escondidas ou apagadas do iPhone (resto do iceberg)
  - Possibilidade de cálculo de *hash* que comprove a integridade da mídia
  - Possibilidade de uma cópia física (bit-a-bit) do disco do iPhone
    - Preservação da evidência original

Acessando o iPhone

- Exemplos de informações armazenadas no disco
  - *Caches* do teclado contendo usuários, senhas, termos de busca, etc.
  - ***Screenshots* do último estado de aplicações**
  - Imagens apagadas da biblioteca de fotos, fotos da câmera e navegação Internet
  - Entradas apagadas do catálogo de endereços, contatos, calendários e outros dados pessoais
  - Histórico de até 100 chamadas
  - Imagens do google maps e coordenadas das últimas buscas
  - Cache do *browser* e objetos apagados
  - Mensagens de email e SMS apagadas
  - Gravações apagadas da caixa postal

Acessando o iPhone

- Acesso físico ao disco
  - Comunicação via USB utiliza o protocolo AFC (Apple File Connection)
  - Não permite acesso completo ao iPhone, somente a um ambiente "enjaulado"
    - /private/var/mobile/Media (ou /private/var/root/Media em versões antigas)
  - Permite o envio de alguns comandos de baixo nível
    - Modo de recuperação (DFU mode)
  - Não permite acesso baixo nível (*raw*) ao dispositivo
    - Necessidade de instalar algo no aparelho para esta tarefa
    - Protocolo proprietário (documentação?)
    - Função não documentada pela apple?

Acessando o iPhone

- Configuração de discos
  - Duas partições em uma NAND flash
    - Funciona como um disco comum
  - Partição 1 – 300MB (root)
    - Sistema operacional
    - Aplicações padrão
    - Normalmente montada como *read-only*
    - Projetada para não ser alterada pelo funcionamento do iPhone
  - Partição 2 – (user)
    - Dados do usuário
    - Restante do disco
    - Montado em /private/var

Acessando o iPhone

- Configuração de discos
  - Block Devices:

brw-r----- 1 root operator 14, 0 Apr 7 07:46 /dev/disko Disk
brw-r----- 1 root operator 14, 1 Apr 7 07:46 /dev/diskos1 System
brw-r----- 1 root operator 14, 2 Apr 7 07:46 /dev/diskos2 Media

  - Raw Devices:

crw-r----- 1 root operator 14, 0 Apr 7 07:46 /dev/rdisko Disk
crw-r----- 1 root operator 14, 1 Apr 7 07:46 /dev/rdiskos1 System
crw-r----- 1 root operator 14, 2 Apr 7 07:46 /dev/rdiskos2 Media

Acessando o iPhone

- Objetivo: Criar uma cópia física da partição de usuário (rdisk0s2)
- Processo
  1. Instalar um conjunto de ferramentas na partição de sistema
  2. Calcular um *hash* da partição de usuário para comparar depois
  3. Realizar uma cópia física do disco através da rede *wireless* (criptografia opcional)
  4. Conferir o *hash*
  5. Analisar a cópia física do disco na estação forense

Copiando o *filesystem*

- Ferramentas necessárias
  - Md5 – Cálculo do *hash* da partição de usuário
  - Dd – Cópia física da partição
  - Netcat – Transferência dos bits da imagem pela rede
  - OpenSSH – Acesso remoto ao iPhone
    - Cópia de arquivos (ferramentas - WinSCP)
    - Facilita a digitação de comandos
    - Criptografar os dados enviados (túnel SSH)

Como instalar ferramentas se a partição de sistema é *read only?*

Copiando o *filesystem*

- iPhone já desbloqueado (*jailbreak*)
  - Versão anterior ao 3G
  - iPhones comprados no exterior e desbloqueados para usar qualquer SIM
  - Partição de sistema *read/write*
  - Alguns já com OpenSSH instalado
  - Installer/Cydia disponível
- iPhone não desbloqueado
  - iPhone 3G
  - Necessita montar a partição de sistema *read/write* (i.e. *jailbreak)* para instalação das ferramentas

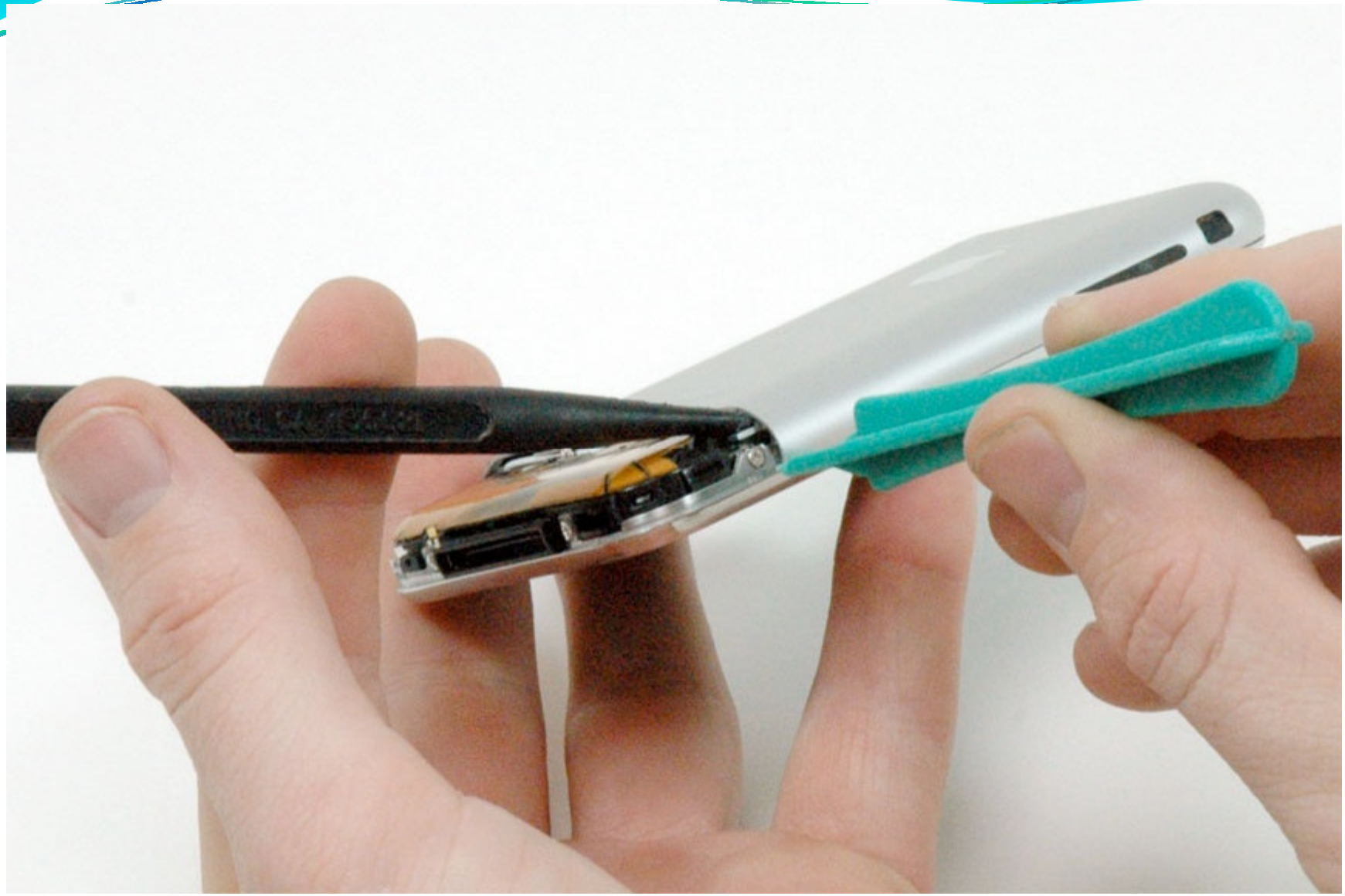
Copiando o *filesystem*

- Modificação na primeira partição
  - Compromete a prova? (documentar mudanças)
  - Dados de usuário na segunda partição
    - Possibilidade de haver dados na primeira em caso de *jailbreak* já existente
  - Necessita um "convencimento" da questão
  - Único meio conhecido atualmente de fazer uma cópia do disco
    - Paraben Device Seizure?

*__iPhone Support:__ The amount of data acquired from the iPhone plug-in can vary depending on the version of the operating system and whether the phone has been unlocked using Jailbreaking software.

Copiando o *filesystem*

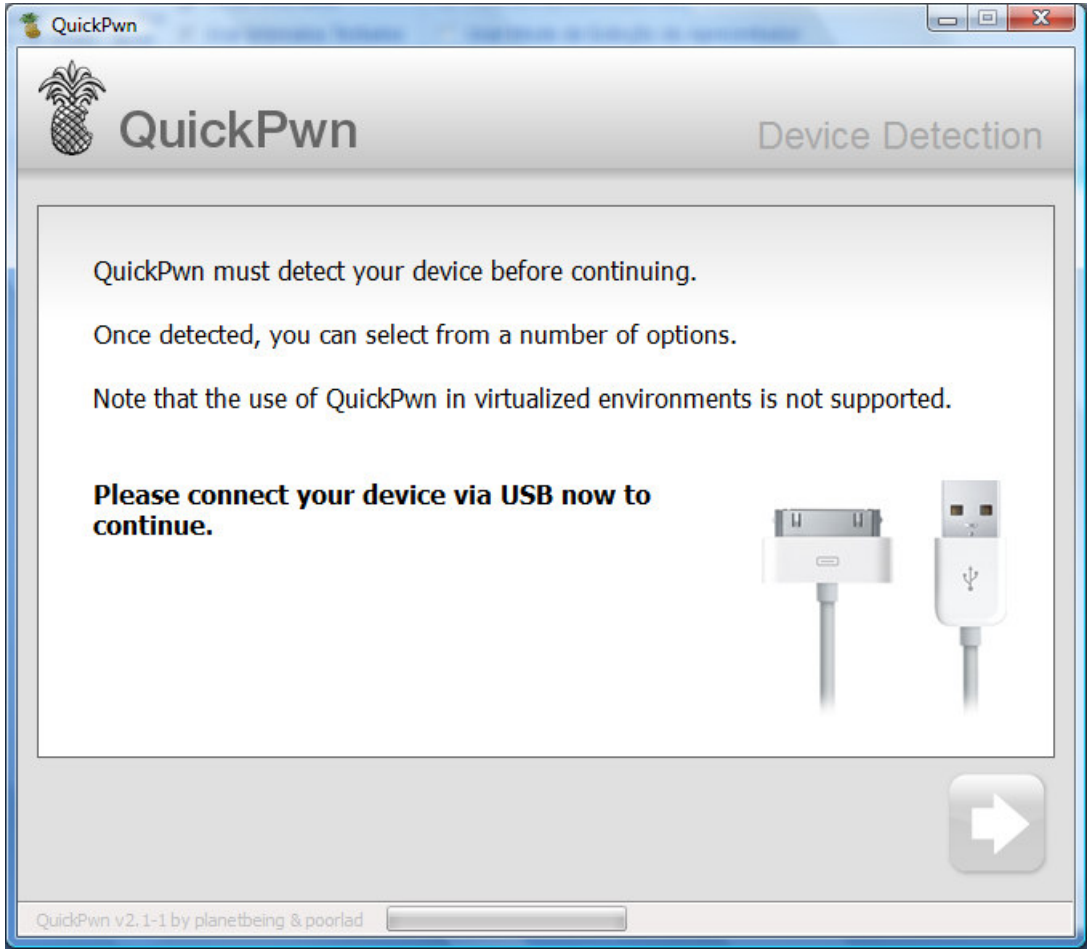
- Considerações sobre acesso físico ao iPhone
  - Necessita de ferramentas específicas
    - E habilidade/conhecimento do processo
  - Possibilidade de dano ao aparelho
    - Remontagem
    - Arranhões
  - Memória *flash* soldada na placa
    - Aparentemente nenhuma interface de leitura



Copiando o *filesystem*

- Realizando o *jailbreak*
- Ferramentas
  - iLiberty+ (Firmware 1.0.2 a 1.1.4)
    - Possibilidade de customizar o *payload* (ferramentas instaladas)
  - Ziphone (Firmware 1.0.2 a 1.1.4)
  - Pwnage tool / Quickpwn / Winpwn (Firmware 2.x)
- Cuidados com a contaminação da evidência
  - Usar uma conta para cada caso
  - Desabilitar o sincronismo automático do iTunes

Copiando o *filesystem*



Copiando o *filesystem*

- Configuração de rede
  - Acesso via *wireless*
    - Único acesso IP ao iPhone
    - Rede ad-hoc entre a estação forense e o iPhone
      - Considerar uso de criptografia
      - Mais seguro (sem intermediários)
    - Access point entre a estação forense e o iPhone
      - Considerar uso de criptografia (WPA, WPA2)
  - Acesso SSH ao iPhone
    - OpenSSH instalado (Cydia, Installer, etc.)
    - Senha de root padrão: **alpine**
  - Instalação de ferramentas
    - Cópia com SCP (menos “intrusivo”)
      - Cuidado com a sobreescrita de bibliotecas!!!
    - Instalação com Cydia/Installer

Copiando o *filesystem*

- Calculando *hash (via ssh)*
  - *cd /*
  - *umount –f /private/var*
  - *mount –o ro /private/var*
  - *md5 /dev/rdisk0s2*
- Não usar o iPhone durante o processo
  - Montagem *read-only* deixa o aparelho instável
- Conectar o aparelho em uma fonte de energia
- Ao final (um pouquinho de paciência)...
  - md5 e4fc1b35381cb43cc9a87363b00c02bf /dev/rdisk0s2

Copiando o *filesystem*

- Na estação forense
  - nc –L –p 7000 | dd of=./imagem.dmg bs=4096
- No iPhone
  - dd if=/dev/rdisk0s2 bs=4096 | nc x.x.x.x 7000
  - x.x.x.x = IP da estação forense
  - Conectar o iPhone em uma fonte de energia
- Processo MUITO demorado (>5h – 16Gb)
- Possibilidade de uso de SSH para criar túnel criptografado
  - Exercício para o leitor ☺
  - Pode ser desnecessário se a rede wireless fizer criptografia
- Conferindo MD5
  - md5sum imagem.dmg
  - e4fc1b35381cb43cc9a87363b00c02bf *touch.dmg

Copiando o *filesystem*

- Exemplo de cópia de disco – iPhone 16Gb

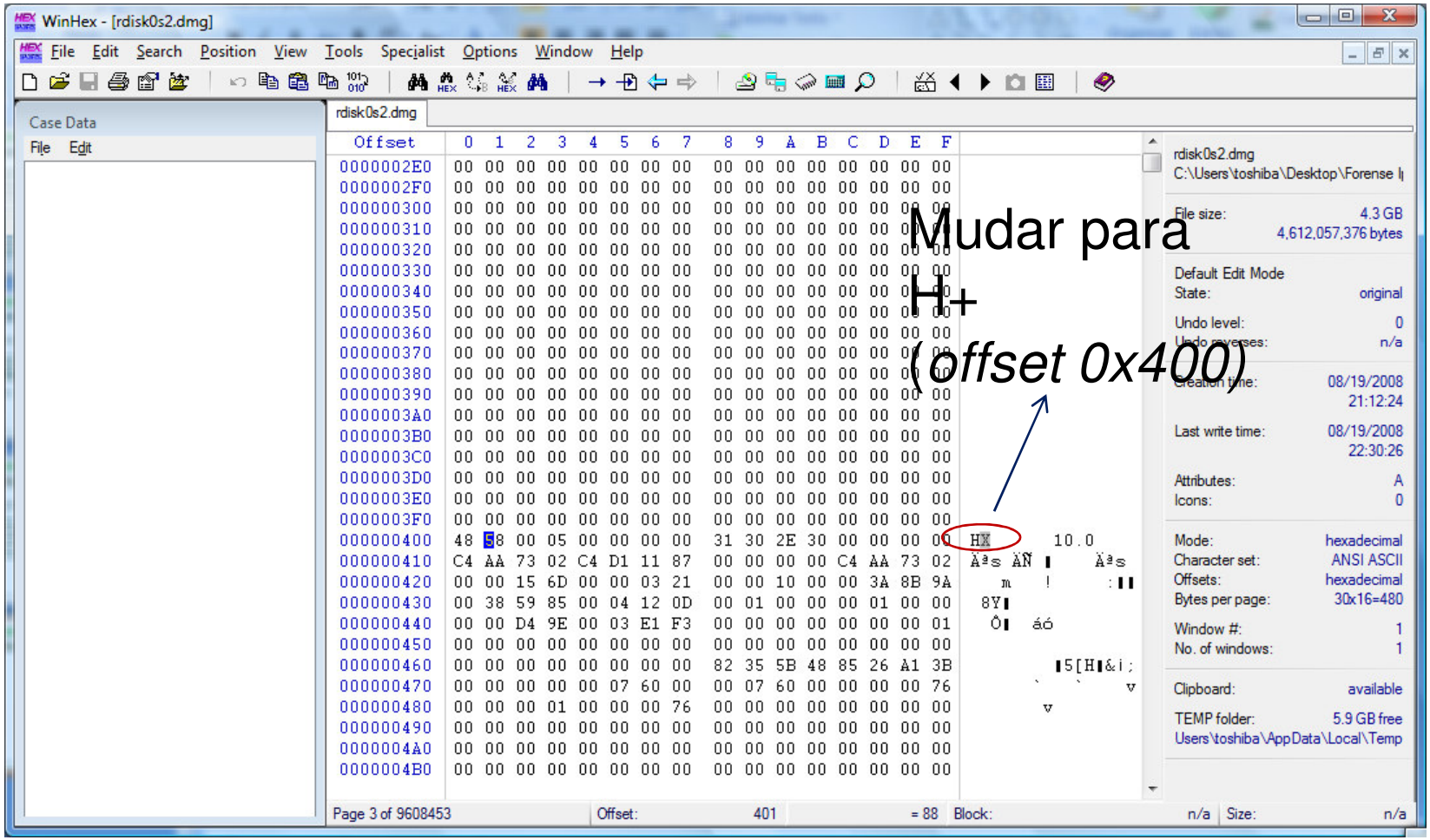
root# dd if=/dev/rdisk0s2 bs=4096 | netcat 192.168.0.1 7000
3836826+0 records in
3836826+0 records out
15715639296 bytes (16 GB) copied, 20465.5 s, 768 kB/s

- 20.465.5s = 341min = 5,7 horas!

Análise forense da imagem

- Análise com ferramentas convencionais
  - Encase
- Ferramentas antigas não suportam partições HFS/X
- *Workaround*
  - Alteração com editor hexadecimal
    - Trocar identificador de HFS/X pra HFS/+
    - Documentar as mudanças

Análise forense da imagem



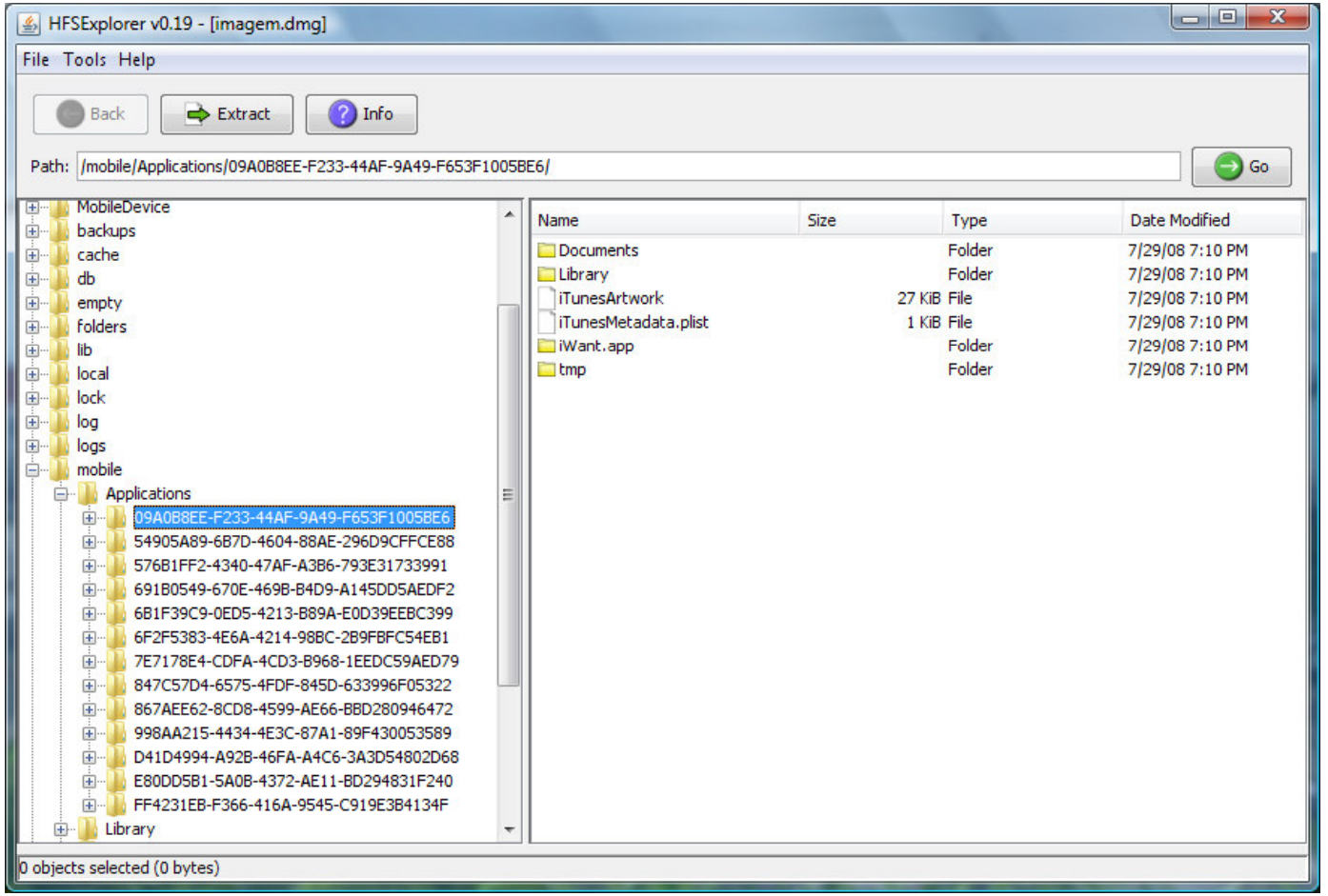
Análise forense da imagem

- Análise com ferramentas gratuitas
  - Montagem do disco com HFSExplorer
  - Busca de arquivos apagados/fragmentos com Scalpel / Foremost
    - Carving específico do iPhone
    - Imagens apagadas e *screenshots* de aplicações
  - Dump de *strings*
  - Buscas nas bases de dados SQLite com Sqlite Browser ou Sqlite3Explorer

Análise forense da imagem

dat y 16384 DynamicDictionary
amr y 65535 #!AMR
plist y 4096 <plist </plist
sqlitedb y 5000000 SQLite\x20format
email y 40960 From:
htm n 50000 <html </html>
pdf y 5000000 %PDF- %EOF
doc y 12500000 \xd0\xcf\x11\xe0\xa1\xb1
txt y 100000 -----BEGIN
png y 40960 \x89PNG
jpg y 5000000 \xff\xd8\xff\xe1 \x7f\xff\xd9

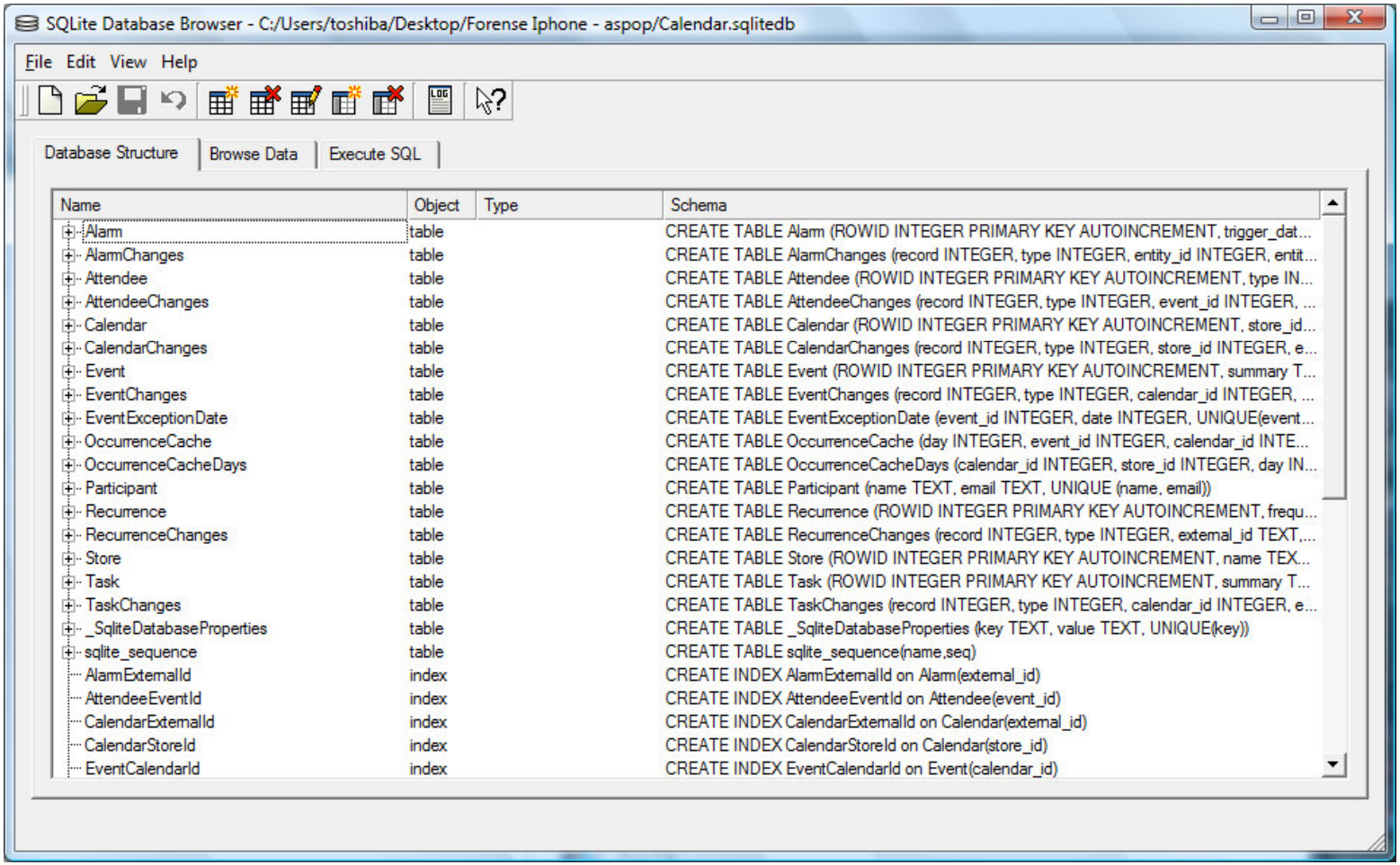
Análise forense da imagem



Análise forense da imagem

- Lugares interessantes de busca
  - Calendar:/mobile/Library/Calendar/Calendar.sqlitedb
  - Call History: /mobile/Library/CallHistory/call_history.db
  - Notes: /mobile/Library/Notes/notes.db
  - SMS: /mobile/Library/SMS/sms.db
  - Address Book: /mobile/Library/AddressBook/AddressBook.sqlitedb
  - ABook2: /mobile/Library/AddressBook/AddressBookImages.sqlitedb
  - Voicemail: /var/root/Library/Voicemail/voicemail.db (arquivos .amr – QuickTime)
  - Photos: /mobile/Media/DCIM/100Apple
  - Photos2: /mobile/Media/Photos
- Atenção à versão do *firmware* (diretórios diferentes)!!

Análise forense da imagem



Análise forense da imagem

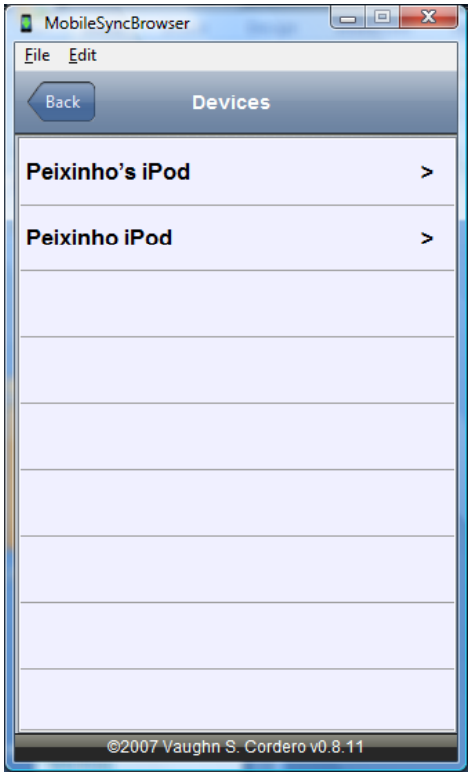
- Mais coisas interessantes...
  - Safari: /mobile/Library/Safari
  - Email: /mobile/Library/Mail/
  - Cookies: /mobile/Library/Cookies/Cookies.plist
  - Google maps: /mobile/Library/Caches/MapTiles/MapTiles.sqlitedb
  - Cache do teclado: /mobile/Library/Keyboard/dynamic-text.dat

Conclusões

- Celulares estão se tornando computadores
- Técnicas convencionais de análise em celulares insuficientes
  - Uso de técnicas de análise em mídias
- Análise de iPhone usando ferramentas disponíveis na Internet é possível
  - Necessita boa documentação
- Análise física do disco revela informações importantes
  - “resto do iceberg”

Próximos passos...

- Verificar outras informações presentes no iPhone
  - Configurações de VPN
  - Endereços IP obtidos via DHCP
- Evidências na máquina usada para sincronizar o iPhone (MobileSyncBrowser)
- Montagem dos *tiles* do google maps
- Automatização do processo
  - Extração das informações nos arquivos DB
  - Relatório com as informações relevantes
- Processo de duplicação via cabo
  - Possível "feature" não documentada da apple
  - DFU mode



Referências

- Iphone Forensics: Rough Cuts
  - Jonathan A. Zdziarski
  - http://oreilly.com/catalog/9780596153892/
- Macintosh and iPhone Forensics
  - BlackBag Technologies, Inc.
  - TechnoSecurity June 2008
  - http://www.techsec.com/2008PDF/Sunday/Track%201%20iPhone.pdf
- Will It Blend?
  - http://www.willitblend.com/

Referências

- Ferramentas
  - DD, HFSExplorer, NetCat, iLiberty, XPwn, Pwnage
    - http://www.zdziarski.com/iphone-forensics/
  - Ziphone
    - http://www.ziphone.org
  - SQLite Browser
    - http://sqlitebrowser.sourceforge.net
  - Sqlite3Explorer
    - http://www.singular.gr/sqlite/
  - Winhex
    - http://www.x-ways.net/winhex/
  - Scalpel
    - http://www.digitalforensicssolutions.com/Scalpel/
  - MobileSyncBrowser
    - http://homepage.mac.com/vaughn/msync/

Obrigado pela paciência!

Perguntas?

peixinho.icp@dpf.gov.br