

COFFORENSE

CONFERÊNCIA DE
CAFÉ COM FORENSE

WWW.MARCOSMONTEIRO.COM.BR

Análise Forense em Android

Pedro Verissimo

pedro@verissimo.net.br



APRESENTAÇÃO

Pedro Verissimo



SysAdmin na Agência de
Defesa Agropecuária

Curriculo

8 (oito) anos no segmento de TI
6 (cinco) anos dedicados ao Linux
Certificações LPI 101 e 102

Qualificações

Consultor em Redes e Segurança,
Perito Ad-Hoc Computacional e
Admirador do .

Estatísticas

01. Origem

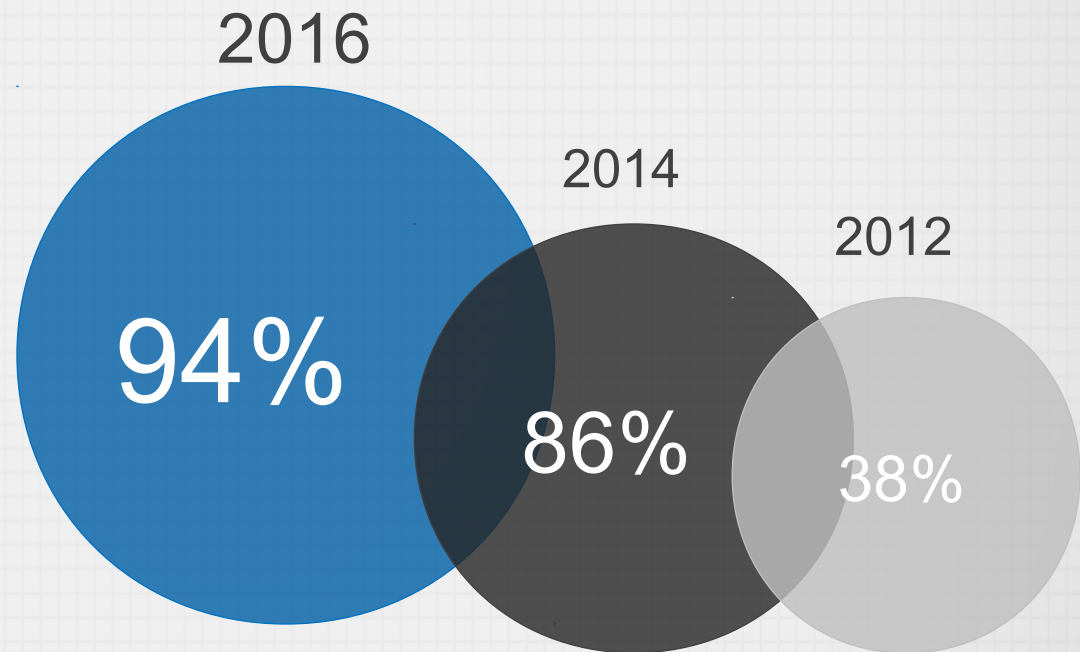
Criado em 2003, na cidade de Palo Alto na California por Andy Rubin, Rich Miner, Nick Sears e Chris White. Foi vendido ao Google em 2005.

02. Lançamento

Foi lançado oficialmente em 22/10/2008 pela HTC, e pouco tempo depois pela Samsung, Sony, Nextel e T-Mobile.

03. Força no Brasil

É um dos países onde o mercado de Android é o mais dominante, com 94,4% em Out/2016.



Como é feita a **Análise**?

Logs

Tráfego

FileSystem

Memória

Extração Manual

A extração é realizada de forma manual, acessando o sistema de arquivos via gerenciador de pastas e copiar arquivos ou pastas individualmente.

Extração Lógica

A extração lógica é realizada utilizando alguma ferramenta para realizar um backup completo do sistema Android, realizando em modo root.

Extração do Cartão SD

A extração do cartão de memória se dá exclusivamente plugando o cartão em algum PC ou notebook e realizando um backup físico ou lógico dele.

Extração Física

A extração física é realizada utilizando geralmente linhas de comando para realizar um clone físico da(s) partição(ões) do Android.

Plataforma Android

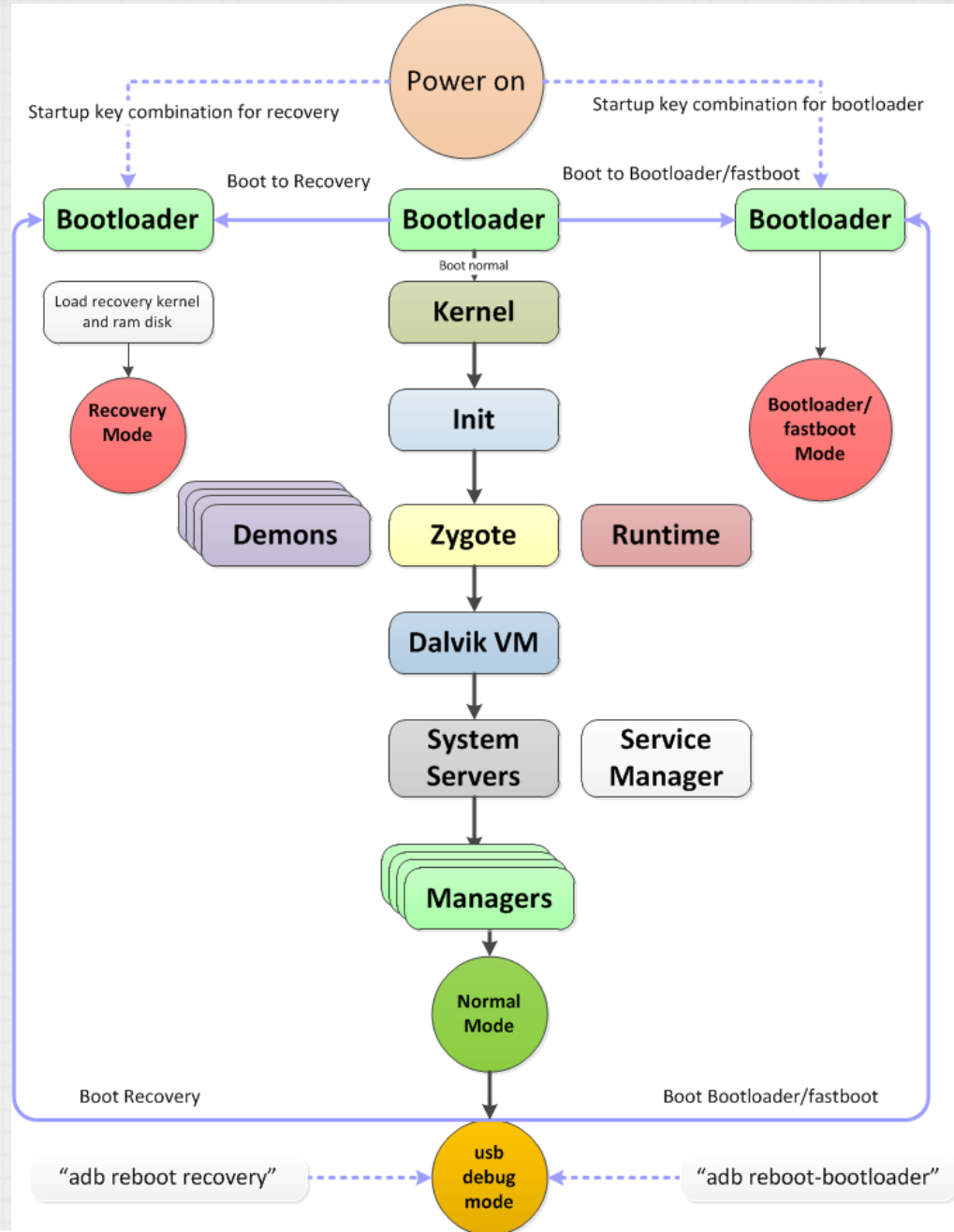
O Sandbox3 atribui uma espécie de ID permitindo que os aplicativos sejam executados isoladamente.

O sistema possui SQLite como banco de dados, seu código é de domínio publico, portanto pode ser usado para qualquer finalidade comercial ou privada.

O sistema de arquivos utilizado é o EXT4, presente de forma estável no kernel do Linux.

O sistema Android possui o ADB (Android Debug Bridge) uma versátil ferramenta de linha de comando que lhe permite comunicar com uma instância do emulador ou dispositivo com Android conectado ao desktop.





ADB

Android Debug Bridge é uma ferramenta versátil em linha de comando que permite comunicar com um dispositivo Android conectado.

Para ativar no Android você terá que habilitar o modo desenvolvedor e permitir a Depuração USB nas configurações de desenvolvedor.

Alguns Comandos ADB

adb devices

- lista os dispositivos conectados ao PC com depuração USB habilitada.

adb shell

- Se conecta no dispositivo conectado via USB.

adb pull

- Realiza o download de um arquivo do seu dispositivo Android para o PC.

adb push

- Realiza o envio de um arquivo do seu PC para o seu dispositivo Android.

adb logcat

- Mostra os logs de baixo nível do Android.

adb install

- Realiza a instalação de um pacote no dispositivo Android.

adb uninstall

- Realiza a desinstalação de algum pacote instalado no Android.

FastBoot

Ferramenta utilizada para modificar o sistema de arquivo no seu aparelho Android.

Alguns comandos fastboot

fastboot devices

- Lista os dispositivos conectados via USB.

fastboot erase

- Limpa toda a partição selecionada.

fastboot reboot

- Reinicia o dispositivo.

fastboot flash

- Sobrescreve a partição usando uma imagem de origem.

Root

O acesso ao root é feito por um script, instalado no modo download ou recovery do Android que, em seguida, executa-se automaticamente.

Este script usa, normalmente, uma vulnerabilidade no kernel do sistema operacional e executa a chamada Privilege Escalation.

Esses novos direitos fazem de você um superusuário, com os privilégios mencionados acima.

O aplicativo instalado, SuperSU ou KingRoot, permite que você mantenha o controle sobre qual momento um aplicativo pode usar os privilégios de root.

Recovery Mode

O Recovery é um ambiente de execução independente do sistema operacional Android, situado numa outra partição da memória interna. Esta separação permite que ele seja acessado mesmo que o sistema principal esteja danificado (brick), oferecendo ao usuário um conjunto de instrumentos para reparar o dispositivo. Por esse motivo, uma versão “base” desse modo está presente em qualquer dispositivo Android.

O Bootloader irá determinar quando executar o Android ou o Recovery, mas nós podemos interferir e forçar a inicialização do modo Recovery sempre que o bootloader não esteja bloqueado.

Custom Recovery

Se as funções-base do Recovery são um tanto limitadas, o mesmo não pode ser dito dos recovery personalizados pela comunidade open-source do Android. Além das funções oferecidas pelo Recovery stock, encontraremos muitas outras opções. Entre elas estão:

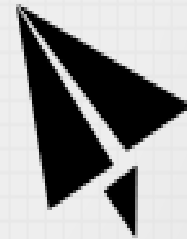
- **Backup and Restore:** Permite efetuar backups completos, chamados NANDroid. De uma só vez, você poderá salvar aplicativos, dados, configurações e todas as suas personalizações, criando assim uma cópia exata do seu dispositivo.
- **Install zip:** É uma evolução de “apply...” que permite instalar qualquer ROM customizada, além de firmwares oficiais, diretamente do celular.
- **Advanced:** Opção que abrirá um segundo menu, cheio de outras funções. Entre as mais utilizadas está “wipe dalvik cache”, o terceiro dos wipes aconselhados (diria obrigatórios) para instalar ROMs diferentes.

COFFORENSE

CONFERÊNCIA DE
CAFÉ COM FORENSE

WWW.MARCOSMONTEIRO.COM.BR

Dúvidas?



COFFORENSE

CONFERÊNCIA DE
CAFÉ COM FORENSE

WWW.MARCOSMONTEIRO.COM.BR

Obrigado pelo seu
Tempo

E-Mail: pedro@verissimo.net.br

Telegram: (85) 98768-7880

