Relatório sobre destruição e recuperação de dados em dispositivos Android

Henrique da Silva
henrique.pedro@ufpe.br

5 de setembro de 2023

Sumário

1 Introdução

Neste relatório, exploramos técnicas de destruição e recuperação de dados em dispositivos Android. Para isso, investigamos o uso de ferramentas especializadas na destruição de dados, como *shred*, bem como a utilização de ferramentas de recuperação de dados, como *adb* e *jmptfs* e *dd*.

Além disso, abordamos a restauração do funcionamento do dispositivo após a destruição de dados e alertamos sobre as práticas inadequadas de destruição de dados que podem permitir restaurações com fins maliciosos.

Todos arquivos utilizados para criar este relatório, e o relatório em si estão em: `https://github.com/Shapis/ufpe_ee/tree/main/6thsemester/SegurancadaInformacao/RelatorioAndroid/`

2 Partições em dispositivos android

Para compreendermos como destruir dados em dispositivos Android, é crucial entendermos como os dados são armazenados. Nesse contexto, empreenderemos uma análise do particionamento de um dispositivo Android.

É importante ressaltar que o particionamento de um dispositivo Android pode variar de acordo com o fabricante e o modelo do aparelho.

2.1 Bootloader

O bootloader é um software de baixo nível que é executado antes do sistema operacional e é responsável por inicializar o hardware do dispositivo e carregar o kernel do sistema operacional na memória. Ele também fornece uma interface para o usuário ou desenvolvedor selecionar diferen-

tes modos de inicialização, como inicialização normal, modo de recuperação ou modo de bootloader (fastboot).

Abaixo, encontra-se uma lista das suas funções:

- Inicialização de Hardware: Quando você liga o seu dispositivo Android, o bootloader é o primeiro software que é executado. Ele inicializa e verifica os componentes de hardware, como a CPU, a memória e os periféricos, garantindo que eles estejam em um estado adequado para o funcionamento do dispositivo.

- Seleção do Modo de Inicialização: O bootloader fornece uma interface para o usuário ou desenvolvedor selecionar diferentes modos de inicialização, como inicialização normal, modo de recuperação ou modo de bootloader (fastboot). Essa flexibilidade permite que os usuários recuperem seus dispositivos, instalem firmware personalizado ou realizem diagnósticos.

- Verificação e Autenticação: O bootloader verifica as assinaturas digitais do kernel e de outras imagens de inicialização críticas antes de carregá-las na memória. Esse processo de verificação garante que o software sendo carregado seja autêntico e não tenha sido adulterado, aumentando a segurança do dispositivo.

- Carregamento do Kernel: Após verificar a integridade do kernel, o bootloader o carrega na memória e transfere o controle para o kernel. O kernel é o núcleo do sistema operacional Android e é responsável por gerenciar os recursos de hardware e executar aplicativos de usuário.

- Modo de Recuperação: Em casos de problemas de software ou atualizações, o bootloader também pode facilitar a instalação de imagens de recuperação oficiais ou personalizadas. O modo de recuperação permite que os usuários realizem várias tarefas, como aplicar atualizações de software, apagar dados ou restaurar o dispositivo para as configurações de fábrica.

- Desbloqueio do Bootloader: Alguns dispositivos Android permitem que os usuários desbloqueiem o bootloader, o que lhes concede a capacidade de instalar ROMs personalizadas, obter acesso mais profundo ao sistema e modificar o software do dispositivo. O desbloqueio do bootloader geralmente anula a garantia do dispositivo e pode apresentar riscos de segurança.

2.2 Imagem de recuperação (Recovery)

A recuperação em um dispositivo Android é um ambiente independente e minimalista que é separado do sistema operacional Android principal. Normalmente, é acessado por meio de uma combinação de botões de hardware durante o processo de inicialização do dispositivo.

As funcoes disponibilizadas pela imagem de recuperação variam mas em geral incluem:

- Recuperação do Sistema: O papel principal da recuperação em um telefone Android é auxiliar na recuperação do sistema. Ela fornece ferramentas e opções para corrigir diversos problemas que podem surgir durante a operação normal do dispositivo, como falhas de software, travamentos ou problemas de inicialização.

- Atualizações de Software: A recuperação é usada para aplicar atualizações e patches de sistema oficiais. Quando uma nova atualização de software está disponível, o dispositivo pode inicializar na recuperação para instalar a atualização. Isso garante que a atualização seja aplicada corretamente e pode reverter para a versão anterior em caso de problemas.

- Restauração de Fábrica: A recuperação permite que os usuários realizem uma restauração de fábrica, que apaga todos os dados e configurações do usuário, retornando o dispositivo ao seu estado original. Isso pode ser útil para solucionar problemas persistentes ou preparar o dispositivo para a revenda.

- Backup e Restauração: Algumas recuperações personalizadas oferecem opções para criar e restaurar backups do dispositivo. Isso é especialmente útil para usuários que desejam fazer backup de seus dados antes de realizar alterações significativas no software do dispositivo.

- Instalação de ROMs Personalizadas: Usuários avançados frequentemente usam recuperações personalizadas para instalar ROMs personalizadas, que são versões modificadas do sistema

operacional Android. Isso permite personalização além do que está disponível no software original.

Além disso, como veremos na discussão sobre a recuperação de dispositivos, existem dois tipos de recuperação disponíveis para a maioria dos dispositivos Android, e estas são:

- Recuperação de Fábrica: Este é o ambiente de recuperação que vem pré-instalado na maioria dos dispositivos Android. Ele fornece funções básicas para atualizações do sistema, restaurações de fábrica e limpeza de partições de cache.
- Recuperação Personalizada: Muitos usuários instalam ambientes de recuperação personalizados, como TWRP (Team Win Recovery Project) ou CWM (ClockworkMod Recovery). Essas recuperações personalizadas oferecem recursos adicionais e flexibilidade, como a instalação de ROMs personalizadas, criação de backups e opções avançadas de solução de problemas.

2.3 Kernel

Dispositivos a android utilizam o *Linux Kernel*, que eh um *kernel* de codigo aberto e livre, que eh conhecido pela sua estabilidade e confiabilidade, este permite que fabricantes facam alteracoes a ele para adicionar funcionalidades especificas ao seu dispositivo.

O kernel tem como funcoes:

- Abstração de Hardware: O kernel Linux atua como uma ponte entre o sistema operacional Android e o hardware do dispositivo. Ele fornece uma interface padronizada para interagir com vários componentes de hardware, como a CPU, memória, tela, dispositivos de entrada e muito mais. Essa abstração permite que o Android seja executado em uma ampla variedade de plataformas de hardware.
- Gerenciamento de Processos: O kernel é responsável por gerenciar processos e threads no sistema Android. Ele aloca recursos do sistema, agenda tarefas e garante que várias aplicações possam ser executadas simultaneamente sem interferir umas nas outras.
- Drivers de Dispositivos: O Linux possui uma vasta coleção de drivers de dispositivos, que são essenciais para habilitar a comunicação entre o sistema operacional e periféricos de hardware, como câmeras, sensores, Wi-Fi, Bluetooth e muito mais. Esses drivers são frequentemente integrados ao kernel Android.
- Segurança: O kernel Linux aplica mecanismos de segurança, como permissões de usuário e grupo, para proteger a integridade e a confidencialidade de dados e processos no dispositivo. Ele desempenha um papel crucial no modelo de segurança do Android.
- Gerenciamento de Energia: O gerenciamento eficiente de energia é vital para dispositivos móveis. O kernel auxilia na regulamentação da frequência da CPU, controla os despertares do dispositivo e gerencia recursos de economia de energia para otimizar a vida útil da bateria.
- Suporte a Sistemas de Arquivos: O kernel Linux suporta vários sistemas de arquivos, incluindo ext4, F2FS e outros, que são usados para armazenar e gerenciar dados em dispositivos Android.
- Rede: Ele gerencia conexões de rede e protocolos de comunicação, possibilitando a conectividade com a Internet e funcionalidades relacionadas a redes no Android.

2.4 Partição de sistema

O sistema operacional Android é acomodado nesta partição. Essa partição é montada como somente leitura *(read-only)*, com o propósito fundamental de salvaguardar a integridade do sistema operacional. Nela residem os pilares do Android, servindo como a base sólida que sustenta todo o funcionamento do dispositivo. Essa abordagem somente leitura impede modificações acidentais ou não autorizadas, assegurando que o sistema principal permaneça estável e confiável ao longo do tempo.

2.5 Vendor Partition

A "Vendor Partition"abriga arquivos e drivers proprietários, fornecidos pelo fabricante do dispositivo, que desempenham o papel de garantir o funcionamento adequado e eficiente do hardware do dispositivo. Esses componentes exclusivos, desenvolvidos pela fabricante, são vitais para permitir que o dispositivo opere com desempenho máximo e compatibilidade otimizada.

2.6 Partição de Dados

A Partição de Dados é o espaço onde sao armazenados os dados do usuário e informações relacionadas aos aplicativos, bem como vídeos e preferências pessoais. Comumente, esta partição é a de maior dimensão no dispositivo.

De forma geral, quando o objetivo é a destruição ou recuperação de dados, esta é a partição na qual direcionaremos nossos esforços.

2.7 Partição de Cache

Dados temporários do sistema e de aplicativos encontram moradia neste local específico com a finalidade de aprimorar o desempenho geral do sistema. Esta partição serve como uma espécie de depósito para informações transitórias, como caches, arquivos temporários e outros dados efêmeros, que são usados para acelerar o funcionamento do dispositivo Android.

A capacidade de armazenar temporariamente esses dados na partição proporciona um ganho de eficiência notável, pois permite que o sistema acesse informações frequentemente utilizadas de maneira mais rápida e sem a necessidade de processamento repetitivo. No entanto, ao longo do tempo, esses dados temporários podem se acumular, ocupando espaço precioso no dispositivo e, em alguns casos, até mesmo causar problemas de desempenho.

Para solucionar essas questões e liberar espaço, os dados temporários podem ser apagados dessa partição. É uma medida que pode ser tomada para resolver problemas específicos, otimizar o espaço de armazenamento e, em alguns casos, melhorar o desempenho geral do dispositivo Android. Portanto, essa partição desempenha um papel importante na manutenção e no gerenciamento eficiente do sistema Android.

2.8 Partições Diversas

Em alguns dispositivos, é possível encontrar partições adicionais, cada uma com propósitos variados e específicos. Essas partições podem incluir, por exemplo, o firmware do modem, o firmware de rádio e outras que desempenham funções especializadas. A existência e a finalidade dessas partições costumam estar intimamente relacionadas com o hardware e o fabricante do dispositivo em questão.

3 Destruição de dados

Conforme observado em 2.2, existem opções padrão para a exclusão de dados do usuário 1. No entanto, é importante notar que essas opções padrão não realizam a sobreposição dos dados na memória do dispositivo, o que permite que ferramentas de recuperação de dados possam recuperar essas informações.

É relevante destacar, no entanto, que a partir da versão *10* do Android, todos os arquivos são criptografados por padrão, o que torna o processo de recuperação de dados consideravelmente mais desafiador.

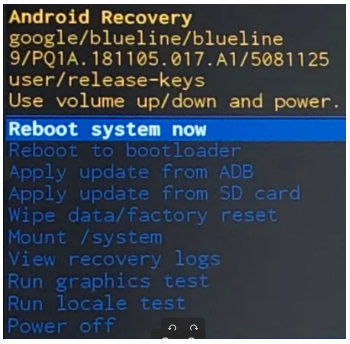

Figura 1: Foto da tela de recuperação de dados de um dispositivo Android.

3.1 Sobrescrita de dados

Utilizaremos uma distribuição Linux para todo o processo abaixo.

Para realizar a destruição de dados, primeiro precisamos explorar as partições do nosso dispositivo para identificar onde os dados que desejamos explorar estão armazenados. Para isso, temos algumas opções.

Primeiro, precisamos habilitar o "USB debugging"no dispositivo. Isso é feito em "Developer Options". Para habilitar as "Developer Options", precisamos clicar 7 vezes em "Build Number"em "About Phone".

Com o dispositivo conectado ao computador, podemos tentar acessar as partições diretamente com o comando "fdisk -l". Se o dispositivo permitir, para sobrescrever os dados, basta identificar a maior partição do dispositivo e utilizar uma ferramenta como o "shred"para sobrescrever todos os dados dela.

Possivelmente, o dispositivo não permitirá o acesso direto às partições. Nesse caso, podemos utilizar o "adb"para acessar o dispositivo. Para isso, precisamos instalar o "adb"no computador e,

com o "adb"instalado, podemos acessar o dispositivo usando o comando "adb shell".

Através do "adb", podemos navegar pelas partições do dispositivo e identificar onde os dados que desejamos sobrescrever estão armazenados.

O "adb"também permite que utilizemos ferramentas do nosso sistema no dispositivo Android. Para isso, basta executar, por exemplo, o comando "adb shell "su -c 'dd if=/dev/block/mmcblk0'".

Com acesso às partições, podemos utilizar a ferramenta de nossa preferência para realizar a sobrescrita dos dados.

Outra alternativa é a ferramenta "jmptfs"; alguns dispositivos serão reconhecidos como um dispositivo "MTP"ao invés de um dispositivo de armazenamento externo. Nesse caso, podemos utilizar o comando "jmptfs /pasta_de_destino"para montar o dispositivo e acessar as partições.

4 Recuperação de dados

Muito do processo é similar ao que foi abordado na destruição de dados. Nesta etapa, nosso objetivo é recuperar informações cruciais, e para isso, precisamos identificar as partições presentes no dispositivo e empregar ferramentas de recuperação de dados especializadas, como o renomado "foremost"e o versátil "photorec".

O primeiro passo consiste em realizar a cópia do conteúdo das partições para o nosso computador. Essa tarefa pode ser executada utilizando a ferramenta "dd"para transferir as partições relevantes para o sistema local.

Com as partições agora disponíveis em nosso computador, podemos utilizar as capacidades do "foremost"e do "photorec"para realizar uma busca minuciosa por dados perdidos ou excluídos. Essas ferramentas possuem algoritmos avançados de recuperação que podem varrer as partições copiadas em busca de arquivos e informações.

Entretanto, é importante notar que dispositivos mais recentes geralmente possuem criptografia de dados robusta, o que torna a recuperação de informações um desafio considerável. Nesses cenários, é possível explorar a opção de utilizar o "adb"para tentar acessar o dispositivo Android e, assim, tentar recuperar os dados protegidos pela criptografia. Vale ressaltar que essa abordagem pode ser mais complexa.

5 Recuperação do dispositivo

Após da destruição de dados, é importante destacar que é possível restaurar o funcionamento do dispositivo. Para realizar essa restauração, basta utilizar a ferramenta "adb"para instalar uma nova imagem do sistema no dispositivo. Geralmente, essa imagem está disponível para download no site oficial do fabricante do dispositivo.

No entanto, é importante notar que alguns fabricantes não disponibilizam essas imagens de sistema, o que pode tornar o processo de restauração do dispositivo mais complexo. Em tais situações, é viável recorrer a ferramentas alternativas, como o "fastboot", que permite a instalação de uma nova imagem do sistema diretamente no dispositivo.

Há também fabricantes, como a Samsung, que oferecem ferramentas específicas, como o "Odin", para facilitar o processo de restauração. O "Odin"possibilita ao usuário a instalação de uma nova imagem do sistema, incluindo a imagem de

recuperação do sistema e o bootloader, tornando a restauração completa e abrangente.

Portanto, a restauração do dispositivo após a destruição de dados pode variar de acordo com o fabricante e a disponibilidade de ferramentas específicas, mas em geral, é um procedimento factível com as ferramentas adequadas.

6 Conclusões

Percebe-se que, embora o sistema de particionamento não seja uniforme em todos os dispositivos, existem partições recorrentes. Constatamos que o processo de destruição de dados pode ser realizado de maneira relativamente simples. No entanto, a recuperação de dados pode se revelar uma tarefa mais complexa, uma vez que sua eficácia depende das especificidades do dispositivo e da versão do sistema Android.

Essa diversidade no sistema de particionamento, aliada à crescente complexidade das versões do Android, demonstra a necessidade de abordagens flexíveis e adaptáveis tanto na destruição quanto na recuperação de dados. Enquanto a destruição pode ser conduzida com relativa simplicidade, a recuperação requer um conhecimento aprofundado das particularidades do dispositivo em questão, assim como da versão do Android que o equipa.

Dessa forma, torna-se fundamental considerar esses fatores ao planejar procedimentos de segurança de dados e ao lidar com situações que envolvem a eliminação ou a restauração de informações em dispositivos Android. Cada caso exigirá uma estratégia sob medida para garantir a proteção ou a recuperação eficiente dos dados, levando em consideração a complexidade do cenário em questão.