AUTORIA

Amarelu e Martu Isla (Amartu)

AGRADECIMENTOS

Muito obrigade à companheires de Navegando Libres, Fembloc, Luchadoras e Maria d'Ajuda por seu tempo e por compartilharem tantas ideias. Esperamos que este material retribua e esteja à altura de seu extraordinário trabalho.

Muito obrigade à Rede Transfeminista de Cuidados Digitais, por compartilhar sua infraestrutura digital.

Muito obrigade também a Ariel, Lux, Foz, Tes, Inés e todes que dedicaram tempo para revisar o conteúdo e nos dar seu feedback.

Muito obrigade ao Center for Digital Resilience por confiar em nós para desenvolver este projeto.

VERSÃO WEB E DOWNLOADS

pt.celularhackeado.net (en Portugués)

es.celularhackeado.net (en Español)

CONTATO

amartu-zine@riseup.net

<SUE COMPANHEIRE NÃO É HACKER>

Parte 2: Desmistificando a análise de celulares

Licença

24 https://labekka.red/licencia-f2f/

vez você não saiba interpretar todas as informações, mas muitas outras sim!

Se você quiser aprender a fazer análises mais técnicas, recomendamos visitar a documentação do SocialTic sobre análise forense consentida em benefício da sociedade civil[21] e entrar em contato com linhas de atendimento feminista[22] e organizações de direitos digitais da sua região[23]. Elas certamente poderão recomendar mais recursos para aprender e esclarecer dúvidas sobre suas análises.

Esperamos que todas essas informações tenham sido úteis e que agora você se sinta com mais confiança e conhecimento para enfrentar qualquer suposto "hackeamento"!

21 https://forensics.socialtic.org/
22 https://feministhelplines.org/es/
23 https://securitylab.amnesty.org/digital-resources/

Conteúdos

Introdução

Ao colaborar com linhas de ajuda feministas de cuidados digitais, percebemos que muitos mitos cercam o tema da invasão de celulares, gerando concepções equivocadas que alimentam sentimentos de impotência, angústia e paranoia entre pessoas em situação de violência. Com base nessa experiência, desenvolvemos um conteúdo para desmistificar essas ideias e oferecer informações acessíveis sobre hackeamento e análise de celulares, buscando um equilíbrio entre a gravidade dos riscos e uma abordagem cuidadosa e realista. Esperamos que este material seja útil tanto para quem enfrenta violência digital quanto para suas redes de apoio e para as próprias linhas de ajuda, que constantemente enfrentam e desconstroem esses mitos.

Para produzir este conteúdo, realizamos entrevistas com 4 linhas de apoio feministas em cuidados digitais: **Navegando Libres**, do Equador; **Luchadoras**, do México; **Maria d'Ajuda**, do Brasil; e **Fembloc**, da Catalunha. Nesses encontros conversamos sobre os mitos que cada linha identificava, os motivos pelos quais os mitos existiam, que imaginários estão por trás dessas ideias e que

Não entre em pânico com cada aplicativo que você não reconheça, provavelmente é um app do sistema que seu celular precisa para funcionar. Pesquise na internet, existem milhares de fóruns com pessoas se perguntando a mesma coisa ;)

Antivírus como Malwarebytes[17] ou Koodous[18] também podem ser muito úteis para detectar configurações inseguras e software espião não sofisticado. No entanto, lembre-se de que eles **não vão detectar aplicativos ou funcionalidades que são consideradas legítimas**, como, por exemplo: Family Link (o controle parental do Google) ou o compartilhamento de localização por meio do app "Buscar" do iPhone.

Evite outros antivírus ou aplicativos que prometem escanear seu dispositivo em busca de software espião. Eles podem inclusive ser perigosos. Por exemplo, não recomendamos o uso do Incognito[19].

Também incentivamos você a revisar seu próprio Google Takeout[20], com paciência e considerando que tal-

17 https://www.malwarebytes.com/pt
18 https://koodous.com/product/koodous-mobile
19 https://play.google.com/store/apps/details?id=com.arcane.incognito
20 Veja a seção 4 (Como gerar um Google Takeout).

tas ou menos glamourosas que uma análise forense, são muito mais eficazes para proteger sua vida digital.

→ As **medidas mais técnicas**, como uma análise forense, **não resolvem situações complexas de violência ou vigilância**. Releia a seção 3 para ajustar suas expectativas antes de pedir uma análise.

*Certifique-se de realizar essas análises com **serviços confiáveis**, reconhecidos por **organizações feministas e que defendem os direitos digitais**. Tenha cuidado com golpes. Nenhuma linha de atendimento feminista ou para defensores de direitos humanos cobra por seus serviços.*

7. Algumas referências caso você queira fazer a análise por conta própria

Se depois de ler este fanzine você ficou com vontade de fazer sua própria análise **ficamos muito felizes! Temos certeza de que quem vai hackear pode ser você!**

Recomendamos revisar novamente a seção 2 e começar por uma análise manual do seu celular.

conteúdos poderiam ser úteis para ajudar a desconstruir esses mitos.

Finalmente, decidimos organizar o conteúdo em **dois volumes distintos**, **um dedicado a desmistificar o hackeamento de celulares**, e **outro dedicado a desmistificar a análise de celulares**, que é a análise feita para detectar sinais de hackeamento.

O volume que você tem em mãos é o volume 2, onde apontamos caminhos possíveis de serem seguidos caso seu celular tenha sido hackeado. Também trazemos informações sobre em que consiste uma análise de celular, quando ela deve ser realizada, o que você pode esperar de uma análise, como gerar relatórios para uma análise mais técnica, como documentar suspeitas e a quem você pode pedir suporte.

Este fanzine nasceu como o projeto final da Fellowship do Center for Digital Resilience do qual fizemos parte entre agosto de 2024 e julho de 2025. Foi um trabalho feito a quatro mãos, com quatro horas de diferença de fuso horário, de duas margens muito distantes do

Oceano Atlântico, entre o Rio de Janeiro e as Ilhas Canárias.

Neste material utilizamos linguagem neutra e o "e" para nos referirmos a qualquer pessoa que possa estar enfrentando uma situação de violência mediada pela tecnologia. Esta é uma abordagem feminista inclusiva para pessoas trans e não binárias. Esperamos que você se sinta confortável ao ler.

Também tentamos evitar o termo "análise forense" porque é um termo técnico pouco familiar. Preferimos dizer "análise de celulares" para nos referirmos a qualquer técnica ou procedimento que sirva para detectar um software ou configurações que possibilitem espionar ou rastrear uma pessoa.

Esperamos que você goste e seja útil ♥

Amarelu e Martu

→ **Capturas de tela, fotos ou vídeos:** Tente tirar print, foto ou fazer um vídeo do comportamento estranho. Guarde esses arquivos em um lugar seguro fora do celular suspeito.

6. A quem você pode pedir uma análise do seu celular

Existem várias coletivas que podem te apoiar nesse sentido. Você pode pedir ajuda a qualquer uma das linhas de atendimento mencionadas na seção 9 da Parte 1.No entanto, lembre-se de que:

→ Realizar uma análise forense do seu celular envolve tempo e trabalho de pessoas com conhecimento técnico especializado nesse tipo de análise. **Antes de solicitar, reflita se você realmente precisa disso e o que está esperando com a análise**.

→ Diante de um incidente de segurança digital, na maioria das vezes o que se precisa são **medidas básicas de proteção digital** (como as que recomendamos aqui), com as quais as linhas de atendimento podem te acompanhar. Embora essas medidas pareçam cha-

mesma história, **reduzindo a exposição emocional** e tornando o **processo mais rápido, objetivo e cuidadoso**.

Informações importantes de serem documentadas:

→ **Quando aconteceu:** Anotar quando cada situação aconteceu é essencial. Mesmo que você não lembre o horário exato, uma ideia aproximada já ajuda muito. Isso permite que, numa análise técnica, se busque nos registros do celular os eventos que aconteceram naquele período.

→ **O que aconteceu:** Descreva de forma concisa o que chamou atenção: comportamentos diferentes no celular, notificações inesperadas, etc. Não precisa usar linguagem técnica, o importante é registrar o que você viu ou achou esquisito.

→ **Onde aconteceu:** Descreva em que aplicativo ou conta você percebeu algo estranho.

→ **Com que frequência:** Saber se foi algo isolado ou se virou padrão ajuda a identificar o tipo de controle ou monitoramento. Anote se os sintomas voltaram, e em que frequência.

1. O que posso fazer se algo estiver realmente acontecendo?

Ainda que muitas vezes a gente acabe supervalorizando o poder e as habilidades tecnológicas das pessoas com quem nos relacionamos, enquanto subestimamos nossa própria capacidade de compreender e reagir, não podemos ignorar que **vivemos em uma estrutura social machista e patriarcal**. Essa estrutura normaliza o acesso não consentido à intimidade de mulheres cis e pessoas trans, atravessando relações afetivas, familiares e até institucionais. Ela marca profundamente muitas vivências, produzindo abusos, vigilância e formas sistemáticas de controle sobre nossos corpos e subjetividades. Ou seja, ainda que espionar alguém por meio do uso que faz de um dispositivo não seja algo tão simples ou imediato, essa é a realidade de muitas pessoas, seja através de softwares espiões voltados para contextos afetivos, ferramentas de controle parental usadas de forma abusiva, ou acessos indevidos a contas como Google e Apple.

Diante da suspeita de que "algo aconteceu" com o celular, é comum que surjam sentimentos de medo, insegurança, vergonha e confusão. Muitas pessoas se per-

guntam: “Será que estou exagerando?” ou “Como posso ter certeza?”. Nesse momento, é importante refletir cuidadosamente sobre os **sintomas[1] que você observa no celular** e verificar a **pirâmide de probabilidade do que pode ter acontecido[2]**. Se após isso você continua com a suspeita e com indícios, é necessário agir para preservar sua privacidade e segurança. No entanto, **não há uma única forma de lidar e um único caminho a seguir**, tudo vai depender dos seus objetivos, sua necessidade emocional, sua urgência, etc.

Caso sinta a necessidade de obter respostas mais objetivas e queira **tentar confirmar se de fato houve espionagem** (por exemplo, se alguém teve acesso remoto ao seu celular, instalou aplicativos de monitoramento ou teve acesso à sua conta), uma das possibilidades é buscar apoio para realizar uma **análise do celular** (análise forense), que envolve uma série de procedimentos voltados à identificação de sinais de invasão, rastros de atividades, vulnerabilidades de segurança e outros indícios. A realização dessa análise pode ajudar a reconstruir o que aconteceu e entender a extensão da exposição.

1 Veja a Parte 1 (6. Quais sintomas são preocupantes e quais não são)
2 Veja a Parte 1 (7. O que pode ter acontecido?)

- **Passo 4**. Depois de alguns minutos, você receberá um e-mail com o link para baixar o arquivo.

Em caso de necessidade de uma análise mais aprofundada do dispositivo, pode ser solicitado: uma extração de apps e SMS com Androidqf, acesso físico ao telefone para uma verificação mais detalhada, ou outros métodos de análise de rede que ultrapassam o escopo deste fanzine.

5. Cómo documentar

Documentar suspeitas e acontecimentos estranhos pode parecer um detalhe, mas é uma ferramenta fundamental tanto para quem está vivendo a situação, quanto para quem vai ajudar. Em momentos difíceis, nossa memória pode falhar, e anotar o que aconteceu, com data, hora e descrição, permite **registrar os detalhes enquanto ainda estão frescos**, organizar os fatos e construir uma linha do tempo. Isso não só **ajuda você a entender melhor o que está acontecendo**, como também oferece às equipes técnicas e de apoio o **contexto necessário para investigar** de forma mais precisa, sem precisar acessar tudo ou vasculhar dados desnecessários. Além disso, evita que você tenha que repetir muitas vezes a

*Os arquivos sysdiagnose y bug repor **não** contêm informações pessoais como fotos, vídeos, contatos, mensagens, etc., mas sim dados sobre os aplicativos instalados e outros detalhes técnicos do seu dispositivo. **Envie-os por um meio seguro**.*

Como gerar um Google Takeout

- **Passo 1**. Faça *login* na sua conta do Google e acesse takeout.google.com.
- **Passo 2**. Clique em "Desmarcar tudo" e marque apenas as opções que considerar necessárias. Geralmente são interessantes:
  - Alertas,
  - Atividade de registro de acesso,
  - Conta do Google,
  - Google Play,
  - Cronologia,
  - Minha atividade, e
  - Perfil.
- **Passo 3**. Clique em "Próxima etapa" e selecione:
  - Enviar link de download por e-mail.
  - Exportar uma vez.
  - Tipo de arquivo: .zip.

Se você sente que não precisa analisar tecnicamente o que aconteceu, seja por esgotamento emocional, medo de escalar a situação ou simplesmente porque **deseja apenas seguir em frente**, você pode pular a parte da análise e **focar em medidas de segurança**. Muitas vezes, o mais importante é restaurar sua segurança e autonomia, independentemente de conseguir uma prova mais concreta do que houve.

*Não há caminho melhor que o outro. E seja como for, recomendamos que busque ajuda de profissionais e ativistas com experiência na área e, de preferência, que trabalhem a partir de uma perspectiva feminista, com uma abordagem centrada no cuidado, na privacidade dos dados, e que tenha sensibilidade para lidar com contexto de violência de gênero. Ao buscar ajuda, tenha cuidado com supostos hackers e assistências técnicas genéricas[3]. Na seção 9 da Parte 1 e na seção 6 deste cuadernillo disponibilizamos informações sobre **como e onde pedir ajuda de forma confiável**.*

Caso queira tomar **medidas emergenciais e básicas de forma independente**, antes de buscar ajuda, segue algumas delas:

3 Veja a Parte 1 (8. Cuidado com supostos hackers e assistência técnica)

1. Altere suas senhas e revise os métodos de recuperação: Através de um dispositivo seguro, altere as senhas de suas contas mais importantes, como emails — principalmente o que utiliza no celular (Android) —, sua conta Apple, suas redes sociais e seus bancos. Utilize **senhas complexas e únicas** para cada serviço e utilize um gerenciador de senhas confiável, como KeepassXC[4] ou Bitwarden[5] para guardá-las. Não esqueça de revisar os métodos de recuperação de senhas (utilize emails e números de celular que você tenha acesso e que sejam seguros).

2. Configure a autenticação de dois fatores: Ative a autenticação em duas ou mais etapas em todas as plataformas que ofereçam essa funcionalidade, adicionando uma camada extra de segurança que dificulta o acesso não autorizado. Como forma de autenticação, **prefira utilizar aplicativos** (como o Aegis[6], por exemplo) em vez de SMS, quando for possível. SMS é uma opção mais vulnerável, pois pode ser interceptada ou ficar indisponível

4 https://keepassxc.org/
5 https://bitwarden.com/
6 https://getaegis.app/

quivo chamado **sysdiagnose-ano-mês-dia-hora-xxxx.tar.gz**.

Você também pode gerar o sysdiagnose usando a funcionalidade **"Toque"** ou **"AssistiveTouch"**:

- **Passo 1**. Configurações > Acessibilidade > Toque > AssistiveTouch > Ativar. Agora aparecerá um novo botão branco na tela com funções de acessibilidade.
- **Passo 2**. Em Personalizar menu flutuante > Adicionar ícone. Toque no novo ícone (com símbolo de "+") e selecione na lista "Análise" > OK.
- **Passo 3**. Agora, ao tocar no botão branco, verá a nova funcionalidade: "Análise" > toque nela e verá a notificação "Coletando análise". Aguarde alguns segundos até terminar.
- **Passo 4**. Se, depois de gerar o sysdiagnose, quiser remover o botão branco, volte para Configurações > Acessibilidade > Toque > AssistiveTouch > Desativar.

A documentação da Apple oferece uma guia visual[16] de como fazer isso.

16 https://it-training.apple.com/tutorials/support/sup075/

cinco vezes nos detalhes da CPU > Você verá uma notificação de que o relatório está sendo gerado (pode levar alguns segundos).

Ao terminar o processo, ***não se esqueça de desativar as "Opções para desenvolvedores"*** *em Configurações > Opções do desenvolvedor > Desativar.*

Como gerar um sysdiagnose (iPhone)

No caso do iPhone, o relatório de erros para análise se chama "sysdiagnose" e é gerado e extraído da seguinte forma:

- **Passo 1**. Pressione ao mesmo tempo os **botões de volume e de ligar/desligar** (os três juntos) por um ou dois segundos.
- **Passo 2**. Ao soltar os botões, **você sentirá uma vibração curta**, o que indica que o sysdiagnose começou a ser gerado.
- **Passo 3**. **Aguarde alguns segundos** até que o arquivo seja finalizado.

Para encontrar seu sysdiagnose vá até Configurações > Privacidade e Segurança > Análise e melhorias > Dados de análise > Buscar: sysdiagnose. Você deve ver um ar-

caso você não tenha acesso à rede de telefonia ou esteja em outro país.

3. Revise e revogue o acesso em contas: É importante verificar onde e em quais dispositivos suas contas estão conectadas, e cancelar o acesso de qualquer dispositivo suspeito, desconhecido ou desnecessário. Se alguém teve acesso indevido à sua conta, é possível que continue conectado em segundo plano mesmo que você troque a senha, por isso é essencial **revogar diretamente o acesso**.

4. Ative e utilize o Google Play Protect (Android): O Google Play Protect é um sistema de segurança nativo do Android, projetado para detectar aplicativos potencialmente maliciosos instalados a partir da Play Store ou de fontes externas. Acesse a **Play Store**, vá até "**Play Protect**" e execute uma verificação manual do dispositivo. Certifique-se de que a **opção de verificação de ameaças de segurança esteja ativada**, permitindo que o sistema monitore continuamente o comportamento dos aplicativos e alerte em caso de atividades suspeitas.

5. Analise detalhadamente os aplicativos instalados: Realize uma revisão minuciosa da lista de aplicativos presentes no dispositivo, identificando e removendo aqueles que sejam **desconhecidos ou desnecessários**. Além disso, examine cuidadosamente as **permissões concedidas** a cada aplicativo, especialmente permissões sensíveis como acessos à localização, câmera e microfone. **Revogue qualquer permissão** que não seja estritamente necessária para o funcionamento legítimo de cada aplicativo.

6. Atualize o sistema e os aplicativos: Garanta que o **sistema operacional** e **todos os aplicativos** estejam atualizados com as últimas **correções de segurança**. As atualizações corrigem **falhas de segurança** que podem ser utilizadas para vulnerabilizar o dispositivo.

7. Restaure o dispositivo para os padrões de fábrica: Ao restaurar o celular, todos os aplicativos e dados são apagados, e ele volta ao estado inicial, como quando saiu da fábrica. Isso significa que **qualquer aplicativo ou configuração usada para espionar será removido** do apa-

volvedor!" (o caminho para ver o "Número da versão" pode variar, dependendo do modelo do celular[15]).

- **Passo 2**. Volte para Configurações e agora verá uma nova opção chamada "Opções do desenvolvedor". Toque em **"Relatório de erros"** ou "*Bug report*".

- **Passo 3**. Selecione **"Relatório completo"** e toque em "Informar".

- **Passo 4**. **Após alguns segundos**, você será notificado(a) de que o relatório de erros está pronto. Para compartilhá-lo, **toque na notificação** ou procure-o no seu gerenciador de arquivos. Ele deve ter o nome "**bugreport-ano-mês-dia-hora.zip**".

Esse método funciona para **Google Pixel, Motorola, Samsung e alguns outros fabricantes**. Se não funcionar para o seu aparelho, procure na internet "*how to generate bug report* [modelo do seu celular]".

> ***Em aparelhos Xiaomi é diferente**, você deverá ir em Configurações > Sobre o telefone > Todas as especificações > tocar*

15 https://developer.android.com/studio/debug/dev-options?hl=es-419

4. Como gerar os arquivos necessários para uma análise

Para realizar análises (forenses) em celulares, são necessários, principalmente, os seguintes arquivos:

- **Bug report** (no caso de Android),
- **Sysdiagnose** (no caso de iPhone), ou
- **Google Takeout** (no caso de Android ou contas Google).

A seguir explicamos como gerar e extrair esses arquivos.

Como gerar um *bug report* (Android)

No Android, o relatório de erros para análise é chamado de "*bug report*" ou "relatório de erros". Existem várias formas de extraí-lo. Dependendo do fabricante, a forma mais comum é:

- **Passo 1. Ative as "Opções para desenvolvedores"**: Vá em Configurações > Sobre o telefone > Informações do software > toque sete vezes seguidas em "Número da versão" até ver "Você agora é um desenvolvedor". É uma forma "radical", mas muito eficaz de eliminar tudo.

- No Android: Configurações > Sistema > Opções de recuperação > Restaurar padrão de fábrica (pode variar conforme o fabricante)
- No iOS: Ajustes > Geral > Transferir ou redefinir o iPhone > Apagar conteúdos e ajustes

Mas **lembre-se**:

- **Todas as suas fotos, vídeos, conversas e outros dados** armazenados no celular serão apagados, então escolha o que deseja conservar e salve em um computador ou nuvem segura. Evite usar as opções de "backup", pois nelas pode estar presente o possível *malware* ou outras configurações;
- Qualquer prova pode ser perdida em caso de um processo judicial (se você não pretende seguir por esse caminho, desconsidere este aviso);
- Restaurar o celular **não bloqueia acessos não autorizados às suas contas do Google ou Apple**. Para isso, será necessário trocar a senha, ativar a verifi-

cação em duas etapas (2FA), configurar métodos seguros de recuperação e revogar sessões de login.

Preste atenção também as dicas rápidas que damos na seção 10 da Parte 1 para que a pessoa hacker seja você.

2. Em que consiste uma análise do celular

Aqui vamos te contar o que normalmente se faz para revisar um celular e tentar descobrir se há *software* espião ou outros aplicativos e configurações que podem ser usados para espionar.

Revisões manuais

Em **primeiro lugar**, costuma-se fazer uma **revisão manual dos aplicativos**. Ou seja, acessar a lista de aplicativos do celular e verificar um por um:

- É um aplicativo do fabricante do celular ou foi instalado pela pessoa usuária?
- Para que serve o aplicativo?
- Quais permissões ele tem? Faz sentido para a funcionalidade do app?

Quando a análise pode ajudar — e quando não é recomendada

Pode ser útil quando...	Pode não ser o melhor caminho
Você desconfia que instalaram um app espião no seu celular.	Você está em risco imediato.
Tem indícios sólidos de que alguém acessa suas contas (e-mail, Google, iCloud, redes sociais) sem autorização.	Você não se sente pronte emocionalmente para lidar com o processo e com o que pode aparecer.
Precisa recuperar registros que podem te ajudar a lembrar ou provar algo.	Você quer apenas seguir em frente sem precisar reviver detalhes da situação.
Quer entender melhor o que aconteceu para tomar decisões com mais clareza.	Espera que a análise traga "provas definitivas" (nem sempre isso é possível).
Está considerando fazer uma denúncia ou buscar apoio jurídico e quer se fortalecer com mais informações.	Já tomou medidas de segurança e já se sente segure com isso.

Importante lembrar: *Ainda que as linhas de ajuda feminista possam fazer análises e produzir relatórios, nem sempre é possível utilizar esses processos e produtos como prova em investigações, julgamentos ou tribunais. Isso vai depender do país, das leis e do contexto em que você estiver.*

sultados da análise forem inconclusivos ou difíceis de interpretar.

Por isso, é fundamental que a decisão de realizar ou não a análise seja tomada com cuidado, de maneira informada, levando o tempo necessário e respeitando as necessidades emocionais. **Nem sempre esse é o passo mais urgente ou necessário**, e é preciso sempre levar em conta a garantia do bem-estar e da autonomia. A análise do celular é apenas uma ferramenta dentro de um conjunto maior de estratégias para enfrentar a violência digital, e muitas vezes, fortalecer as medidas básicas de segurança digital e receber acolhimento já são passos fundamentais para retomar o controle da situação.

Em resumo, a análise técnica é mais apropriada quando as suspeitas são fortes, quando as tentativas básicas de proteção (trocar senhas, revisar permissões, atualizar o sistema) não resolveram o problema, quando há um objetivo claro de documentar o que está acontecendo ou quando se precisa obter evidências para processos judiciais. Fora desses casos, focar em fortalecer a segurança digital e emocional costuma ser mais importante e menos desgastante.

Quando há dúvidas, busca-se o nome do app na internet. Também é possível usar os sites *immuniweb.com* e *reports.exodus-privacy.eu.org* para obter mais informações.

No Android, também se verifica se o Google Play Protect[7] está ativado e se a instalação de apps desconhecidos está desativada para todos os aplicativos — especialmente para o navegador e o gerenciador de arquivos.

Além disso, costuma-se perguntar à pessoa se ela recebeu links suspeitos por SMS, WhatsApp ou outras plataformas — e então analisá-los. Para verificar esses links, normalmente se usa o *virustotal.com*.

Também são verificadas funcionalidades como controle parental (ex: Google Family Link) ou compartilhamento de localização, que não são identificadas como *software* espião ou vírus, mas que podem ser usadas para vigiar alguém.

Escaneamento com antivírus

Em **segundo lugar**, pode-se fazer um **escaneamento do celular com um antivírus recomendado**, como o

7 https://support.google.com/android/answer/2812853?hl=pt

Malwarebytes[8] ou o Koodous[9]. Esses antivírus são capazes de detectar facilmente software espião usados em relações afetiva e configurações inseguras, como a "instalação de apps de fontes desconhecidas" ativada.

Análise de relatórios de erro

Em **terceiro lugar**, se ainda houver suspeitas de uma possível intervenção no dispositivo, pode-se fazer uma **análise do relatório de erros do aparelho**. No Android, esse relatório é chamado de *bug report* e, no iPhone, é chamado de *sysdiagnose*.

Para fazer essa análise, a equipe de atendimento fornecerá as instruções para gerar o relatório de erros do seu dispositivo e enviá-lo. Esses relatórios contêm informações sobre os aplicativos instalados, as permissões concedidas, quando foram instalados, quando foram iniciados, os processos do sistema, o uso da bateria, erros ocorridos e detalhes técnicos sobre o dispositivo e suas configurações. Esses relatórios **não contêm fotos, vídeos, mensagens ou conversas**, nem configurações específicas de cada aplicativo.

8 https://www.malwarebytes.com/pt
9 https://koodous.com/product/koodous-mobile

- Se foram realizadas alterações ou configurações que possam indicar tentativas de vulnerabilizar o dispositivo, como funcionalidades de proteção desativadas, por exemplo.

- Se a conta vinculada ao telefone celular estiver sendo acessada de outro dispositivo, possibilitando o monitoramento de várias atividades, como o uso de aplicativos, pesquisas na Internet, localização etc. Nesse caso, não é o celular que seria analisado, mas os dados que a conta pode oferecer. Para as contas do Google, será muito útil analisar o conteúdo do "Google Takeout".

Apesar desses potenciais benefícios, é importante lembrar que a análise técnica do celular **não garante respostas definitivas em todos os casos**. Tecnologias de vigilância podem ser sofisticadas e deixar poucos rastros, e **o fato de nada ser encontrado não garante que nada esteja acontecendo**, o que pode gerar frustração, ser motivo de paranóia, ou mesmo gerar uma falsa noção de segurança. O processo também pode ser **emocionalmente desafiador**, e intensificar sentimentos de ansiedade, insegurança e até medo, especialmente se os re-

***Aqui queremos apenas oferecer uma visão geral sobre a análise de celulares e tornar o tema mais compreensível**. Naturalmente, isso **não é um guia de como fazer análise forense de celulares**, nem pretende definir procedimentos obrigatórios. Cada caso é único e cada equipe de atendimento terá sua abordagem na hora de realizar uma análise.*

3. O que uma análise do celular pode (ou não) fazer por mim

A análise do celular pode ser um recurso valioso para **identificar sinais de violência digital**, e quando feita com cuidado, por pessoas ou coletivos que atuam com responsabilidade e uma abordagem feminista, ela pode oferecer mais do que provas: pode trazer alívio, confirmar suspeitas ou simplesmente ajudar a nomear uma sensação de insegurança que, até então, parecia vaga demais para ser explicada. Tecnicamente, a análise pode revelar uma série de coisas, como, por exemplo:

- Se algum aplicativo com capacidades de espionagem foi instalado, e quando e como isso aconteceu. Em alguns casos, sendo possível até compreender quem é a pessoa responsável pelo monitoramento.

A análise desses relatórios **não é mágica e seus resultados também não são mágicos**. A ferramenta mais usada para analisar esses relatórios é o MVT[10] (Mobile Verification Toolkit), desenvolvida pela Anistia Internacional e voltada para a detecção de software espião em celulares de pessoas defensoras de direitos humanos. Essas análises podem detectar software espiões usados em relações afetivas (menos sofisticado) — por meio de uma verificação automatizada de aplicativos — e também alguns programas espiões mais sofisticados, mas com certas limitações.

O MVT funciona com "Indicadores de Comprometimento" (*Indicators of Compromise*, ou IOC em inglês), que basicamente são elementos considerados suspeitos e associados a possíveis softwares maliciosos (como URLs, nomes de processos, erros, etc.). A Anistia Internacional e outras organizações se dedicam a identificar esses IOCs a partir do estudo de softwares espiões descobertos em investigações ou reportados pela comunidade. No entanto, o ecossistema de software espião — especialmente o mais sofisticado — é bastante obscuro. Por isso, IOCs

10 https://docs.mvt.re/en/latest/

que serviam para detectar um *Pegasus* há alguns meses talvez não funcionem mais hoje.

Em alguns casos, após a análise do relatório de erros do dispositivo, pode ser considerado necessário um exame mais aprofundado que envolva **acesso físico ao aparelho** ou o uso de ferramentas de extração de aplicativos como o Androidqf[11].

Análise do Google Takeout

Em **quarto lugar**, em casos de dispositivos Android e/ou suspeita de acesso à conta Google, pode ser muito útil a **análise de dados do Google Takeout**[12]. Essa análise consiste em solicitar ao Google os dados da conta que se deseja investigar, por meio do formulário disponível em *takeout.google.com*.

O Google envia um arquivo `.zip` com todas as informações solicitadas sobre a conta, como: mudanças de senha ou recuperação de conta; aplicativos instalados e assinaturas vinculadas à conta Google Play; dispositivos onde a conta foi configurada; dispositivos que fizeram

11 https://github.com/mvt-project/androidqf/
12 https://es.wikipedia.org/wiki/Google_Takeout

login (incluindo IP e região); histórico de navegação no Chrome (buscas e URLs acessadas); pesquisas e downloads no Google Drive e muito mais.

Essa análise pode ser bastante extensa, por isso é muito importante **definir intervalos de tempo**, dias ou horários específicos para revisar.

Análise de tráfego

Por fim, queremos te contar que, em casos de suspeita de software espião sofisticado, também podem ser feitos **análises de tráfego de rede do dispositivo**. Isso basicamente consiste em capturar o tráfego de rede do celular e analisá-lo para verificar se está enviando dados para servidores considerados suspeitos.

Para isso, pode ser solicitado que você se conecte a uma rede ou VPN específica (que capturará o tráfego para análise), ou que você mesmo(a) capture o tráfego com ferramentas como o PCAPdroid[13] e depois envie para análise. A ferramenta PiRogue[14] também pode ser usada para esse tipo de análise.

13 https://play.google.com/store/apps/details?id=com.emanuelef.remote_capture&hl=es_VE
14 https://pts-project.org/docs/pirogue/overview/