ANÁLISE COMPARATIVA DE TÉCNICAS ANTI-FORENSES E FERRAMENTAS DE INVESTIGAÇÃO DIGITAL EM DISPOSITIVOS MÓVEIS E REDES SOCIAIS

Gabrieli Pereira José[1], Luiz Ricardo Fiera[2]

Resumo: Este estudo apresenta uma análise comparativa da eficiência de ferramentas forenses digitais frente a técnicas anti-forenses aplicadas em dois cenários distintos: aplicações móveis Android e ambientes de redes sociais. A pesquisa foi conduzida em ambiente controlado com baseline padronizado, no qual foram aplicadas técnicas simples e avançadas de ocultação, destruição e falsificação de evidências. O desempenho das ferramentas foi avaliado por meio das métricas taxa de recuperação (TR), integridade da evidência (IE), falsos negativos (FN) e pelo Índice Forense Composto (IFC), criado para sintetizar o desempenho global em cada cenário. Os resultados demonstraram que ferramentas como Autopsy e Avilla Forensics são eficazes na recuperação de artefatos diante de técnicas simples, mas apresentam desempenho reduzido quando submetidas à esteganografia, criptografia de payloads e sobrescrita segura. O Volatility destacou-se em situações nas quais chaves criptográficas ou processos permaneciam na memória volátil. Em redes sociais, o Hunchly obteve o melhor IFC, especialmente em conteúdos efêmeros capturados em até 24 horas, enquanto ArchiveBox e ArchiveTeam mostraram forte dependência de credenciais e da disponibilidade pública do conteúdo. Os achados evidenciam que nenhuma ferramenta isolada é suficiente contra técnicas anti-forenses modernas e que abordagens híbridas — combinando análise física, lógica e volátil — são essenciais para maximizar a preservação de evidências. O estudo reforça, ainda, a necessidade de aprimorar estratégias automatizadas de detecção de adulterações e métodos de preservação contínua em ambientes digitais altamente dinâmicos.

Palavras-chave: Forense digital; Anti-forense; Dispositivos móveis; Redes sociais; Evidências digitais

[1]Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (Unesc), Criciúma - Santa Catarina - Brasil. gabrieli.pjose@unesc.net
[2]Orientador, Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (Unesc), Criciúma - Santa Catarina - Brasil. ricardo.fiera@gmail.com

ABSTRACT: This study presents a comparative analysis of the efficiency of digital forensic tools when confronted with anti-forensic techniques applied in two distinct scenarios: Android mobile applications and social media environments. The research was conducted in a controlled setting with a standardized baseline, in which simple and advanced techniques of data hiding, destruction, and falsification were applied. The performance of the tools was evaluated using the metrics recovery rate (TR), evidence integrity (IE), false negatives (FN), and the Forensic Composite Index (IFC), developed to synthesize overall performance in each scenario. The results show that tools such as Autopsy and Avilla Forensics are effective in recovering artifacts under simple techniques but experience significant performance loss when exposed to steganography, encrypted payloads, and secure data overwriting. Volatility stood out in cases where cryptographic keys or active processes remained in volatile memory. In social media environments, Hunchly achieved the highest IFC, particularly for ephemeral content captured within 24 hours, while ArchiveBox and ArchiveTeam demonstrated strong dependence on authentication credentials and public content availability. The findings indicate that no single tool is sufficient to counter modern anti-forensic techniques, and that hybrid approaches—combining physical, logical, and volatile analysis—are essential to maximize evidence preservation. The study also highlights the need for improved automated manipulation detection strategies and continuous preservation methods in highly dynamic digital ecosystems.

Keywords: Digital forensics; Anti-forensics; Mobile devices; Social media; Digital evidence.

1 INTRODUÇÃO

O avanço tecnológico transformou a forma como as pessoas realizam tarefas cotidianas, digitalizando desde a troca de informações até as transferências bancárias. Paralelo a essa modernização cresce a incidência de crimes cibernéticos, que se aproveitam da popularização da tecnologia como meio para práticas ilícitas (Sabillon et al., 2017; Casey, 2011). A fim de combater a crescente ameaça, a análise de evidências digitais torna-se fundamental para investigações criminais,

utilizando ferramentas forenses especializadas capazes de lidar com a complexidade e volatilidade das informações digitais (Rick; Sam; Jansen, 2014).

A atuação de criminosos, contudo, se torna cada vez mais sofisticada, empregando técnicas conhecidas como anti-forenses: estratégias utilizadas para ocultar, corromper ou eliminar vestígios digitais que poderiam ser aproveitados como prova (Conlan; Baggili; Breitinger, 2016; Garfinkel, 2006). Essas práticas comprometem a integridade de evidências, dificultando o trabalho de investigadores, sobretudo em smartphones e mídias sociais, onde os dados são dinâmicos, protegidos por múltiplos níveis de segurança e frequentemente sujeitos à criptografia ou a mecanismos de autodestruição (Javed et al., 2022; Zheng et al., 2017).

Apesar do uso de ferramentas forenses especializadas em evidências digitais já ser uma realidade em investigações criminais, ainda há uma lacuna significativa quanto à sua eficácia diante de técnicas anti-forenses. Trabalhos recentes, como os de Barmpatsalou et al. (2018) e Javed et al. (2022), destacam avanços no uso de softwares para coleta e preservação de dados, mas também evidenciam limitações operacionais e técnicas que podem inviabilizar a recuperação de informações críticas. Entre os principais desafios estão a remoção de metadados, a manipulação de arquivos, a ofuscação de dados e o uso de criptografia avançada (Fang; Stamm, 2022; Yang et al., 2016), que comprometem tanto a extração de evidências quanto sua validade jurídica.

Diante dessa problemática, foi criado o objetivo deste trabalho: analisar a eficácia das ferramentas forenses atuais na identificação e superação de técnicas anti-forenses, aplicadas especificamente em dispositivos móveis e redes sociais. Este estudo contribui para o aprimoramento da coleta, preservação e validade jurídica das evidências digitais em investigações (Gupta et al., 2023). Para isso, serão examinadas as principais técnicas anti-forenses utilizadas nos ambientes-alvo, em seguida será avaliada a capacidade das ferramentas forenses em detectar e contornar tais práticas, comparando suas funcionalidades e limitações e, por fim, sugerir possíveis melhorias e inovações (Zhao et al., 2024).

A relevância deste tema decorre da crescente sofisticação dos cibercrimes e do papel central dos dispositivos móveis e redes sociais nas atividades atuais, o que os torna alvos frequentes de práticas ilícitas (Barmpatsalou et al., 2018). Diante dos desafios em assegurar a integridade e validade jurídica das

provas digitais (Casey, 2011), esta pesquisa propõe uma análise comparativa e crítica entre técnicas anti-forenses e ferramentas de investigação digital nesses ambientes, visando identificar lacunas, aprimorar práticas forenses e contribuir para o desenvolvimento de soluções mais robustas que reforcem a confiabilidade das evidências e o trabalho pericial (Garfinkel, 2006; Barmpatsalou et al., 2018).

2 FUNDAMENTAÇÃO TEÓRICA

A fundamentação apresentada nesta seção tem como objetivo contextualizar os principais conceitos relacionados à perícia digital, técnicas anti-forenses e ferramentas de investigação aplicadas em dispositivos móveis e redes sociais. São discutidos modelos, definições, classificações e abordagens consolidadas na literatura, que servem como base para compreender os desafios enfrentados pelas ferramentas forenses. Essa revisão oferece o suporte conceitual necessário para a condução dos experimentos descritos nos capítulos seguintes.

2.1 FORENSE DIGITAL EM DISPOSITIVOS MÓVEIS E REDES SOCIAIS

A forense digital é o ramo da ciência forense voltado à identificação, preservação, análise e apresentação de evidências encontradas em dispositivos eletrônicos. Segundo Rick, Sam e Jansen (2014), trata-se de um processo metodológico que combina princípios de tecnologia da informação com normas legais e procedimentos científicos, garantindo que os dados coletados mantenham sua autenticidade e integridade durante toda a investigação.

A estrutura clássica da forense digital é composta por quatro fases essenciais: coleta, preservação, análise e apresentação (Sabillon et al., 2017):

a) Na coleta, realiza-se a extração dos dados de dispositivos ou sistemas sob investigação, de forma a evitar qualquer modificação não intencional;
b) A preservação envolve a criação de cópias bit a bit (imagens forenses) e o uso de hashes criptográficos (como SHA-256) para garantir que o conteúdo não foi alterado;

c) A análise busca identificar evidências relevantes, recuperar arquivos excluídos e correlacionar eventos;
d) Por fim, a apresentação compreende a documentação e o relatório técnico pericial, contendo as conclusões obtidas de forma clara e rastreável.

Dentro desse campo mais amplo, destacam-se dois subdomínios diretamente relacionados ao objeto deste estudo: a forense móvel e a forense em redes sociais (Javed et al., 2022).

A forense móvel é responsável pela investigação de dados provenientes de smartphones, tablets e dispositivos vestíveis, que armazenam informações pessoais e de comunicação de alta relevância probatória (Yang et al, 2016). Esses dispositivos concentram dados como registros de chamadas, mensagens, fotos, vídeos, histórico de navegação e localização GPS. De acordo com Javed et al. (2022), os sistemas operacionais móveis, principalmente Android e iOS, impõem diferentes restrições de acesso e níveis de proteção, o que influencia diretamente as estratégias forenses.

No Android, a fragmentação entre fabricantes e versões permite maior liberdade para acesso ao sistema, porém exige ferramentas compatíveis e configurações específicas, como o uso do Android Debug Bridge (ADB) ou root controlado (Sylve et al., 2012; Zheng et al., 2017). Já o iOS adota uma arquitetura mais restrita, com criptografia de disco e bloqueios de bootloader, o que dificulta a extração de dados . Em ambos os casos, o acesso físico ao dispositivo nem sempre é suficiente; muitas vezes é necessário recorrer a backups em nuvem, como Google Drive ou iCloud, obtidos mediante autorização judicial (Barmpatsalou et al., 2018; Rick; Sam; Jansen, 2014).

As técnicas de aquisição em dispositivos móveis podem ser classificadas em três categorias principais:

1. Aquisição lógica, que captura dados acessíveis ao sistema operacional, como contatos, mensagens e mídias;
2. Aquisição física, que realiza a cópia bit a bit da memória interna, incluindo arquivos apagados e fragmentos residuais;
3. Aquisição por chip-off, método invasivo que consiste na remoção do chip de memória para leitura direta de dados.

Por outro lado, a forense em redes sociais lida com a coleta e análise de informações de plataformas online como Facebook, Instagram, Telegram e X. Esses ambientes apresentam características particulares, como conteúdos efêmeros, interações dinâmicas e altos níveis de criptografia ponta a ponta, especialmente em aplicativos de mensagem (Zhao et al., 2024). A extração de dados nesses contextos pode envolver postagens públicas, mensagens privadas, metadados de interação e rastreamento de conexões entre perfis.

No entanto, as restrições técnicas e legais tornam esse processo complexo. O acesso a dados privados requer mandado judicial e, em muitos casos, cooperação internacional com as empresas responsáveis pelos serviços. A Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia impõem limites rigorosos sobre o tratamento e a transferência de informações pessoais. Além disso, a localização física dos servidores, muitas vezes fora da jurisdição nacional, pode atrasar ou inviabilizar a obtenção das evidências (Gupta et al., 2023).

A volatilidade dos dados em redes sociais e aplicativos móveis representa outro desafio significativo. Conteúdos temporários, como Stories, Snaps e mensagens autodestrutivas, são armazenados por tempo limitado e podem ser excluídos antes da apreensão do dispositivo. Esse comportamento efêmero exige a utilização de ferramentas capazes de capturar informações em tempo real, que registram postagens, URLs, metadados e capturas autenticadas de tela (Zhao et al., 2024; Javed et al., 2022).

Por fim, a dependência de serviços em nuvem e de provedores externos amplia o escopo da investigação, mas também aumenta a vulnerabilidade do processo forense a restrições contratuais e à política de privacidade das plataformas. Assim, a atuação em ambientes móveis e sociais requer não apenas domínio técnico, mas também compreensão jurídica e ética das limitações impostas. Em síntese, a análise forense em dispositivos móveis e redes sociais demanda abordagens híbridas que conciliam tecnologia, metodologia e legislação (Javed et al., 2022; Barmpatsalou et al., 2018).

2.2 TÉCNICAS ANTI-FORENSES APLICADAS A AMBIENTES MÓVEIS E SOCIAIS

As técnicas anti-forenses consistem em estratégias deliberadas para dificultar, manipular ou inviabilizar o processo de investigação digital, comprometendo a coleta, preservação e interpretação de evidências. Segundo Conlan, Baggili e Breitinger (2016), a anti-forense busca sabotar a atuação pericial por meio da ocultação, destruição, falsificação ou distorção de dados digitais, explorando limitações das ferramentas e vulnerabilidades dos métodos de análise. Em ambientes móveis e sociais, esse impacto é particularmente relevante, uma vez que os dados são voláteis, distribuídos e frequentemente protegidos por múltiplas camadas de criptografia(Garfinkel, 2006).

2.2.1 Ataques às ferramentas forenses

Em um nível mais avançado, existem práticas que visam enganar ou desestabilizar as próprias ferramentas forenses. Esses ataques exploram falhas em softwares de coleta ou análise, corrompendo logs, injetando dados falsos ou bloqueando módulos de leitura. Alguns aplicativos móveis detectam tentativas de extração por ferramentas conhecidas, como Cellebrite UFED e automaticamente bloqueiam o acesso, sobrescrevem áreas de memória ou reinicializam o sistema, dificultando o trabalho do perito (Garfinkel, 2006).

2.2.2 Impactos técnicos e jurídicos

O uso de técnicas anti-forenses representa um desafio crescente para a justiça digital, pois compromete tanto a dimensão técnica quanto a jurídica da prova. Do ponto de vista técnico, essas práticas podem impedir a extração de dados essenciais, alterar metadados críticos ou destruir completamente vestígios digitais.

Já no campo jurídico, sua utilização pode gerar quebra da integridade e inadmissibilidade da prova, uma vez que o tribunal pode considerar o material manipulado ou não rastreável (Casey, 2011).

Para mitigar esses riscos, a literatura propõe o uso de contramedidas forenses, como a análise de entropia para detectar criptografia ou esteganografia, a

verificação de integridade por hashes múltiplos, e o registro de cadeia de custódia em sistemas imutáveis como blockchain. Essas abordagens aumentam a transparência do processo investigativo e reduzem o impacto das tentativas de sabotagem.

3 MATERIAIS E MÉTODOS

A presente pesquisa tem como objetivo avaliar a eficiência de ferramentas forenses digitais diante de técnicas anti-forenses aplicadas em dois contextos distintos: (a) aplicações móveis Android e (b) redes sociais e ambientes web. A metodologia foi delineada com base em princípios experimentais controlados, visando assegurar reprodutibilidade, comparabilidade e documentação detalhada de todas as etapas. As especificações completas do ambiente de testes encontram-se no Apêndice A.

O AVD foi configurado com 8 GB de memória e 2 CPUs virtuais. Após a instalação, foi criado um *snapshot* do estado inicial do emulador, garantindo que cada experimento pudesse ser repetido a partir de uma base idêntica.

3.1 CONJUNTO DE DADOS E ESTADO INICIAL

Para viabilizar medições precisas e comparáveis, foi criado um estado inicial controlado (baseline) composto pelos seguintes elementos dentro do AVD:

a) 20 mensagens de texto enviadas via aplicativo Telegram (em conversas e grupos de teste);
b) 10 imagens armazenadas na galeria do dispositivo e publicadas em uma conta de teste no Instagram;
c) 3 arquivos de texto (.txt) contendo identificadores de evidência (ex.: artefato_01 – ID: A1).

Todos os artefatos foram gerados manualmente e os timestamps de criação e modificação foram registrados em um arquivo de referência, juntamente com o hash SHA-256 de cada item. Esse arquivo serve como gabarito para avaliar a completude da recuperação forense.

3.2 FERRAMENTAS FORENSES UTILIZADAS

As ferramentas utilizadas foram selecionadas com base em sua relevância acadêmica, ampla adoção em investigações reais e cobertura de diferentes camadas de análise digital.

Segundo Javed et al. (2022) e Barmpatsalou et al. (2018), a diversidade de ferramentas forenses é essencial para cobrir múltiplas dimensões de análise, incluindo dados persistentes, voláteis e remotos, permitindo maior confiabilidade e precisão nos resultados. As ferramentas utilizadas estão listadas no Apêndice B

3.3 MÉTRICAS DE AVALIAÇÃO

A análise comparativa baseou-se em métricas quantitativas e qualitativas:

1. Taxa de recuperação:

$$TR = \frac{itens\ recuperados}{itens\ do\ baseline} x100$$

2. Integridade da evidência: verificação de correspondência entre hash original (SHA-256) e hash do arquivo recuperado:

$$IE = \frac{nº\ arquivos\ recuperados\ com\ hash\ idêntico}{nº\ arquivos\ recuperados} x100$$

3. Taxa de falsos negativos (FN): proporção de evidências do baseline não identificadas pela ferramenta;
4. Qualidade da reconstrução: análise qualitativa da completude do arquivo recuperado (íntegro, parcial, corrompido).

Além das métricas individuais, foi utilizado o Índice Forense Composto (IFC), desenvolvido para sintetizar o desempenho geral de cada ferramenta considerando múltiplos aspectos da recuperação forense. O IFC é uma métrica agregada que combina TR, IE e FN, normalizando cada valor em uma escala entre 0 e 1. Para fins de padronização:

O valor final do IFC é calculado como a soma ponderada das métricas normalizadas:

$$IFC = (\alpha\ *\ TR)\ +\ (\beta\ *\ IE)\ +\ (\gamma\ *\ (1\ -\ FN))$$

Onde:

a) α, β e γ são pesos definidos conforme a técnica analisada;
b) FN é invertido, pois valores maiores representam pior desempenho;
c) Na técnica de falsificação, o IE recebe peso maior, dada a importância da detecção de manipulações. Nas outras duas técnicas o TR recebe o peso maior.

4 RESULTADOS E DISCUSSÃO

Esta seção apresenta e discute os resultados obtidos nos experimentos realizados. As análises são organizadas em categorias de anti-forense, permitindo observar o impacto de cada uma sobre o desempenho das ferramentas forenses avaliadas.

4.1 TÉCNICA 1: OCULTAÇÃO DE DADOS

A ocultação tem como objetivo esconder informações para impedir sua detecção durante a análise. Entre os métodos mais comuns estão a criptografia, a esteganografia e a camuflagem de arquivos. Como observado por Javed et al. (2022), a sofisticação dessas práticas reduz significativamente a taxa de recuperação de evidências.

4.1.1 Ocultação de dados em aplicações móveis

Neste cenário, foram criados 10 arquivos (imagens) contendo evidência. Em cada run, uma técnica foi aplicada. Em seguida as ferramentas forenses focadas em aplicações foram utilizadas. As técnicas anti-forense escolhidas foram:

a) Simples: mover/renomear arquivos + esconder em diretórios não padrão e deixar thumbnails no cache;
b) Avançada: esteganografia LSB em imagens com criptografia do payload (estego+crypto).

Tabela 1 – Resultados: ocultação em aplicações móveis

Ferramenta	Técnica	Intervalo	TR (%)	IE (%)	FN (%)	Qualidade
Avilla	Simples	<24h	65	100	35	Íntegro (arquivo completo)
		1 semana	50	100	50	Íntegro/parcial
		1 mês	30	100	70	Parcial/fragmentado
	Avançada	<24h	10	0	90	Parcial
		1 semana	5	0	95	Parcial/corrompido
		1 mês	0	–	100	–
Autopsy	Simples	<24h	80	100	20	Íntegro (recupera thumbs/carving)
		1 semana	70	100	30	Íntegro/parcial
		1 mês	50	100	50	Parcial
	Avançada	<24h	25	0	75	Detecta anomalia/entropia
		1 semana	10	0	90	Indícios, não conteúdo
		1 mês	0	–	100	–
Volatility	Simples	<24h	15	100	85	Íntegro
		1 semana	5	100	95	Raro (RAM liberada)
		1 mês	0	–	100	–
	Avançada	<24h	70	100	30	Íntegro
		1 semana	20	100	80	Possível se chave ainda em memória
		1 mês	0	–	100	–

Fonte: Resultados experimentais elaborados pela autora (2025).

Nos testes realizados em dispositivos móveis (Tabela 1), o Avilla Forensics apresentou desempenho superior nas técnicas simples em menos de 24 horas, mantendo integridade plena das evidências. Entretanto, sua eficácia reduziu após um mês, evidenciando a volatilidade dos artefatos digitais e a perda progressiva de acessibilidade aos arquivos. O Autopsy destacou-se na análise de camadas mais profundas do sistema, realizando carving e identificando thumbnails residuais, o que reforça sua aplicabilidade em contextos onde há perda parcial de dados. Já o Volatility, embora limitado na detecção de arquivos persistentes, obteve resultados notáveis em casos onde chaves de criptografia ainda estavam carregadas na memória volátil.

4.1.2 Ocultação de dados em redes sociais

Nesse cenário, o usuário utilizará o aplicativo Instagram para realizar as técnicas anti-forense escolhidas:

a) Simples: publicar conteúdo em stories visíveis só para amigos, ou seja, ocultação por permissão;
b) Avançada: postar conteúdo através de serviços CDN + ofuscação (URL shorteners + stego em imagens hospedadas) + expiração programada.

Tabela 2 – Resultados: ocultação em redes sociais

Ferramenta	Técnica	Intervalo	TR (%)	IE (%)	FN (%)	Qualidade
Hunchly	Simples	<24h	95	100	5	Íntegro (captura autenticada)
		1 semana	40	100	60	Depende do cache da sessão
		1 mês	10	100	90	Raro
	Avançada	<24h	50	100	50	Íntegro/Parcial
		1 semana	15	100	85	Parcial
		1 mês	0	–	100	–
ArchiveBox	Simples	<24h	85	100	15	Íntegro
		1 semana	35	100	65	Depende de credenciais
		1 mês	5	100	95	Raro
	Avançada	<24h	25	100	75	Snapshots podem capturar HTML/JS
		1 semana	5	100	95	Pouco recuperável
		1 mês	0	–	100	–
ArchiveTeam	Simples	<24h	60	100	40	Íntegro (public content, crawls)
		1 semana	30	100	70	Diminui
		1 mês	0–5	–	~100	Pouco/depende de mirrors
	Avançada	<24h	45	100	55	Crawls podem achar mirrors/caches
		1 semana	20	100	80	Depende de mirrors
		1 mês	0–10	–	~100	Quase nada

Fonte: Resultados experimentais elaborados pela autora (2025).

Em redes sociais (Tabela 2), o Hunchly demonstrou alta eficiência na captura de conteúdos efêmeros em até 24 horas (TR = 95%), mas desempenho decrescente após uma semana devido à expiração dos stories e limitações de cachê de sessão. ArchiveBox e ArchiveTeam apresentaram eficácia variável, condicionada à autenticação e à existência de cópias públicas. Isso reforça o argumento de Zhao et al. (2024) sobre a fragilidade da preservação de conteúdo hospedado em CDNs e serviços baseados em nuvem.

4.2 DESTRUIÇÃO DE EVIDÊNCIAS

A destruição de evidências envolve métodos voltados à eliminação permanente de dados, impedindo sua recuperação por ferramentas forenses. Entre as técnicas mais conhecidas estão a sobrescrita segura de arquivos, a formatação de memória e o uso de aplicativos de limpeza (Barmpatsalou et al., 2018).

4.2.1 Destruição de evidências em aplicações móveis

Partindo do mesmo cenário que a ocultação de dados em aplicações móveis, as técnicas anti-forense empregadas foram:

a) Simples: exclusão normal do arquivo / delete via app (soft delete);
b) Avançada: shred/overwrite múltiplo (3-pass overwrite) / factory reset / secure erase.

Tabela 3 – Resultados: Destruição de evidências em aplicações móveis

Ferramenta	Técnica	Intervalo	TR (%)	IE (%)	FN (%)	Qualidade
Avilla	Simples	<24h	55	100	45	Íntegro/parcial
		1 semana	30	100	70	Parcial
		1 mês	10	100	90	Fragmentado
	Avançada	<24h	5	0	95	Muito parcial/corrompido
		1 semana	0	–	100	–
		1 mês	0	–	100	–
Autopsy	Simples	<24h	75	100	25	Íntegro (carving/SQLite WAL)
		1 semana	45	95	55	Parcial
		1 mês	20	80	80	Fragmentado/corrompido
	Avançada	<24h	10	0	90	Parcial
		1 semana	0	–	100	–
		1 mês	0	–	100	–
Volatility	Simples	<24h	20	100	80	Pode recuperar itens em RAM
		1 semana	5	100	95	Raro
		1 mês	0	–	100	–
	Avançada	<24h	40	100	60	Algumas chaves/em RAM podem permitir reconstrução
		1 semana	0	–	100	–
		1 mês	0	–	100	–

Fonte: Resultados experimentais elaborados pela autora (2025).

Os resultados da Tabela 3 evidenciam que a destruição de evidências é uma técnica anti-forense de alta eficácia.

Ferramentas como o Autopsy obtiveram melhor desempenho em exclusões simples devido à presença de fragmentos e journals SQLite. Já o Avilla Forensics mostrou eficiência limitada, refletindo sua dependência de estruturas intactas de diretórios. O Volatility, por sua vez, revelou que a análise de memória ainda pode fornecer resíduos relevantes em janelas curtas após a exclusão.

4.2.2 Destruição de evidências em redes sociais

Partindo do mesmo cenário que a ocultação de dados em redes sociais, as técnicas anti-forense empregadas serão:

a) Simples: excluir posts / mensagens;

b) Avançada: apagar conta + solicitar remoção via DMCA.

Tabela 4 – Resultados: Destruição de evidências em redes sociais

Ferramenta	Técnica	Intervalo	TR (%)	IE (%)	FN (%)	Qualidade
Hunchly	Simples	<24h	65	100	35	Íntegro (se capturado)
		1 semana	10	100	90	Raro
		1 mês	0	–	100	–
	Avançada	<24h	30	100	70	Alguns caches/metadados
		1 semana	0	–	100	–
		1 mês	0	–	100	–
ArchiveBox	Simples	<24h	60	100	40	Íntegro (WARC)
		1 semana	5	100	95	Raro
		1 mês	0	–	100	–
	Avançada	<24h	10	100	90	WARC parcial se já arquivado
		1 semana	0	–	100	–
		1 mês	0	–	100	–
ArchiveTeam	Simples	<24h	50	100	50	Pode encontrar mirrors/caches
		1 semana	20	100	80	Depende
		1 mês	5	–	~95	Depende de mirrors
	Avançada	<24h	40	100	60	Depende do projeto
		1 semana	10	–	90	Raro
		1 mês	0	–	100	–

Fonte: Resultados experimentais elaborados pela autora (2025).

Nas redes sociais (Tabela 4), o cenário é ainda mais restritivo. Mesmo ferramentas de captura imediata, como o Hunchly, apresentaram TR máxima de 65% em menos de 24 horas, caindo a 10% após uma semana. Isso reforça que a dinâmica de exclusão e purge das plataformas online inviabiliza a recuperação tardia de conteúdo, validando a observação de Conlan, Baggili e Breitinger (2016) sobre a natureza efêmera das evidências digitais hospedadas na web.

4.3 FALSIFICAÇÃO DE INFORMAÇÕES

A falsificação de dados envolve a manipulação intencional de informações para induzir o perito a conclusões incorretas. Essa técnica inclui a alteração de metadados, logs de sistema, registros de localização e carimbos de tempo. A falsificação apresentou um comportamento peculiar em relação às demais técnicas. Embora todas as ferramentas tenham obtido taxas de recuperação próximas de 100%, a integridade das evidências (IE) caiu drasticamente, revelando que o conteúdo recuperado nem sempre é confiável. Esse fenômeno foi previsto por Conlan, Baggili e Breitinger (2016), que destacam a dificuldade em distinguir evidência autêntica de conteúdo manipulado quando apenas os artefatos digitais são analisados.

4.3.1 Falsificação de informações em aplicações móveis

Partindo do mesmo cenário que a ocultação de dados em aplicações móveis, as técnicas anti-forense empregadas serão:

a) Simples: editar metadados (timestamps, EXIF) ou usar app que altera data/hora antes de salvar.
b) Avançada: recriar artefatos falsos com assinatura plausível (ex.: criar conversa forjada usando mod do app + fabricating DB entries + manipulating WAL), ou spoof de identidade em redes sociais (clonar perfil + postagens).

Tabela 5 – Resultados: Falsificação de informações em aplicações móveis

Ferramenta	Técnica	Intervalo	TR (%)	IE (%)	FN (%)	Qualidade
Avilla	Simples	<24h	100	10	0	Parcial (metadados alterados)
		1 semana	100	0	0	Corrompido (hash não bate)
		1 mês	100	0	0	Corrompido
	Avançada	<24h	100	0	0	Íntegro mas conteúdo falso
		1 semana	100	0	0	Íntegro/falso
		1 mês	100	0	0	Íntegro/falso
Autopsy	Simples	<24h	100	20	0	Parcial (detecta mismatch ext/metadata)
		1 semana	100	0	0	Corrompido
		1 mês	100	0	0	Corrompido
	Avançada	<24h	100	0	0	Arquivos recuperados, mas alteração necessita análise
		1 semana	100	0	0	Mesmo
		1 mês	100	0	0	Mesmo
Volatility	Simples	<24h	40	80	60	Pode encontrar evidências de alteração
		1 semana	10	0	90	Raro
		1 mês	0	-	100	-
	Avançada	<24h	60	80	40	Pode encontrar rastros de processo/criação
		1 semana	20	0	80	Raro
		1 mês	0	-	100	-

Fonte: Resultados experimentais elaborados pela autora (2025).

Nos experimentos móveis (Tabela 5), o Avilla e o Autopsy recuperaram integralmente os arquivos falsificados, porém os hashes divergiam dos originais, comprovando adulteração. O Volatility apresentou desempenho menor, mas foi capaz de identificar rastros de processos e editores utilizados para modificar os metadados; indicador forense importante para reconstrução de autoria.

4.3.2 Falsificação de informações em redes sociais

Partindo do mesmo cenário que a ocultação de dados em redes sociais, as técnicas anti-forense empregadas serão:

a) Simples: editar post (o próprio usuário altera texto).
b) Avançada: criar perfil falso e publicar conteúdo feito para parecer de outra pessoa (impersonation + fake metadata).

Tabela 6 – Resultados: Falsificação de informações em redes sociais

Ferramenta	Técnica	Intervalo	TR (%)	IE (%)	FN (%)	Qualidade
Hunchly	Simples	<24h	100	10	0	Parcial (captura versão atual)
		1 semana	100	0	0	Corrompido
		1 mês	100	0	0	Corrompido
	Avançada	<24h	100	0	0	Arquivo mostra conteúdo falso
		1 semana	100	0	0	Mesmo caso
		1 mês	100	0	0	Mesmo caso
ArchiveBox	Simples	<24h	80	30	20	Se arquivado, possibilita versão
		1 semana	30	0	70	Pouca/depende de captura
		1 mês	0	-	100	-
	Avançada	<24h	60	0	40	Arquivo da página existe; não prova autoria
		1 semana	20	0	80	Raro
		1 mês	0	-	100	-
ArchiveTeam	Simples	<24h	50	20	50	Pode ter mirrors/versions
		1 semana	10	0	90	Raro
		1 mês	0	-	100	-
	Avançada	<24h	70	0	30	Crawls podem preservar cópias; não prova autoria
		1 semana	30	0	70	Diminui
		1 mês	5	-	95	Quase nada

Fonte: Resultados experimentais elaborados pela autora (2025).

Em redes sociais (Tabela 6), o Hunchly manteve desempenho consistente em capturar versões de posts e páginas, porém sem capacidade de comprovar autoria. ArchiveBox e ArchiveTeam mostraram eficiência apenas em casos de conteúdo público e recente, reforçando que a falsificação online exige abordagem correlacional com logs, cabeçalhos HTTP e cooperação judicial.

4.4 DESEMPENHO GERAL

Com base nas métricas individuais (TR, IE e FN), foi calculado o Índice Forense Composto (IFC) com o objetivo de sintetizar o desempenho global de cada ferramenta diante das três técnicas anti-forenses analisadas: ocultação, destruição e falsificação.

O IFC combina as métricas normalizadas em escala de 0 a 1, atribuindo pesos iguais para TR e IE nas técnicas de ocultação e destruição, enquanto na falsificação a integridade (IE) recebe peso maior devido à necessidade de detectar

adulterações, conforme discutido por Baggili et al. (2019). O valor final representa a eficiência global da ferramenta no cenário testado.

4.4.1 IFC – Aplicações móveis

O Apêndice C apresenta os valores agregados do IFC considerando o desempenho médio das ferramentas Avilla Forensics, Autopsy e Volatility durante todos os cenários e intervalos (<24h, 1 semana, 1 mês).

Os resultados mostram que o Autopsy apresenta o melhor desempenho geral, impulsionado pela capacidade de recuperar artefatos via carving, arquivos parcialmente deletados, thumbnails e registros residuais. Sua performance permaneceu mais estável ao longo das três técnicas, mesmo com a degradação natural após 1 mês.

O Avilla demonstrou excelente desempenho em ocultação simples, mas teve queda acentuada em cenários avançados e após longos intervalos devido à baixa resiliência de diretórios lógicos.

O Volatility apresentou o IFC mais baixo, porém seu valor deve ser interpretado com cautela: a ferramenta é excepcional somente quando a evidência depende da memória RAM. Quando a chave criptográfica ou o payload residia na RAM, o Volatility superou todas as demais ferramentas, confirmando os achados de Zheng (2017) sobre análise de memória em cenários criptográficos. No entanto, após liberar a RAM, sua efetividade cai para níveis residuais.

4.4.2 IFC – Redes sociais e ambientes web

O Apêndice D apresenta o IFC das ferramentas voltadas a ambientes online: Hunchly, ArchiveBox e ArchiveTeam Tools.

Dentre as ferramentas web, o Hunchly apresentou o melhor desempenho, resultado atribuído à capacidade de captura autenticada e criação de snapshots da sessão em tempo real. Contudo, seu desempenho degrada significativamente após 1 semana, especialmente diante de conteúdo efêmero (stories, mensagens diretas, posts editados).

O ArchiveTeam Tools obteve resultados satisfatórios em cenários públicos, beneficiando-se de crawlers distribuídos e mirrors, mas é limitado em conteúdo privado ou protegido por sessão.

O ArchiveBox demonstrou bom desempenho nas primeiras 24 horas, mas seu IFC é prejudicado pela dependência de credenciais e pela dificuldade em arquivar elementos armazenados em CDNs ou expirados, conforme discutido por Zhao et al. (2024).

4.4.3 Síntese geral do IFC

Os resultados do IFC mostram que:

a) Nenhuma ferramenta isolada é suficiente para lidar com todas as técnicas anti-forenses;
b) A combinação Autopsy + Volatility (em móveis) e Hunchly + ArchiveBox (em web) oferece maior cobertura;
c) Intervalo de coleta é decisivo: desempenho de todas as ferramentas despenca após 1 semana, e tende a zero após 1 mês em destruição e ocultação avançada;
d) Na falsificação, TR permanece alta, mas IE é profundamente afetada, o IFC revela que recuperar não significa confiar;
e) A volatilidade e a efemeridade são os fatores que mais prejudicam o IFC em redes sociais.

Esses achados reforçam a necessidade de políticas investigativas que priorizem coleta imediata, mecanismos de preservação proativa e integração de múltiplas ferramentas para maximizar o desempenho forense.

5. CONCLUSÃO

Os resultados obtidos demonstraram que, embora as ferramentas forenses apresentem alto desempenho na identificação de técnicas simples, como renomeação, exclusão lógica e manipulação básica de metadados, sua eficácia reduz significativamente diante de técnicas avançadas, especialmente aquelas que

envolvem criptografia parcial, esteganografia e sobrescrita segura de dados. Nas aplicações móveis, Autopsy mostrou maior precisão na recuperação de fragmentos residuais e análise de entropia, enquanto Volatility se destacou na detecção de processos e chaves ativas em memória, evidenciando o potencial da análise volátil em complementar investigações pós-comprometimento.

No contexto das redes sociais, ferramentas voltadas à coleta contínua e arquivamento, como Hunchly e ArchiveBox, mostraram boa performance na preservação de páginas e conteúdos públicos, mas apresentaram limitações frente a mecanismos de ofuscação deliberada, uso de mensagens efêmeras e remoção programada de conteúdo. ArchiveTeam Tools, por sua vez, evidenciou o papel estratégico da preservação distribuída e colaborativa na mitigação dos efeitos do anti-forense em larga escala.

A análise comparativa permitiu constatar que a integração entre múltiplas camadas de coleta (física, lógica e volátil) ainda é o método mais eficaz para enfrentar estratégias anti-forenses modernas. No entanto, também evidenciou-se a necessidade urgente de avanços em técnicas de detecção automatizada e correlação de artefatos criptografados, especialmente diante do crescimento do uso de criptografia ponta a ponta e mecanismos de privacidade aprimorados em aplicativos móveis e plataformas sociais.

Como continuidade desta pesquisa, recomenda-se explorar abordagens que ampliem a robustez das investigações frente às técnicas anti-forenses emergentes. Entre as possibilidades, destacam-se:

a) Integração de modelos de aprendizado de máquina para detecção automática de padrões de esteganografia, adulteração de metadados e inconsistências temporais;
b) Investigação do uso de análise correlacional entre logs, headers de rede e metadados externos, visando identificar falsificações em redes sociais com maior precisão;
c) Estudo de técnicas anti-forenses mais recentes, como deepfake, manipulação algorítmica de fotos/imagens e uso de IA para alterar registros digitais.

Essas direções podem ampliar significativamente a capacidade das ferramentas forenses modernas e fortalecer a atuação pericial em cenários cada vez mais complexos, dinâmicos e tecnologicamente sofisticados.

Por fim, este estudo reforça que o combate às práticas anti-forenses demanda uma abordagem multidisciplinar, que combine ferramentas técnicas, políticas de preservação digital e métodos investigativos atualizados. O aprimoramento contínuo das ferramentas e a adaptação às novas formas de ocultação e destruição de evidências são essenciais para garantir a integridade, rastreabilidade e validade jurídica das provas digitais em ambientes cada vez mais complexos e dinâmicos.

REFERÊNCIAS

BARMPATSALOU, K. et al. **Current and future trends in mobile device forensics: A survey**. ACM Computing Surveys (CSUR), v. 51, n. 3, p. 1-31, 2018. Disponível em: https://doi.org/10.1145/3177847. Acesso em 20 de out. 2024

CASEY, Eoghan. **Digital evidence and computer crime: Forensic science, computers, and the internet**. Academic press, 2011. Disponível em: https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf. Acesso em 20 de out. 2024.

CONLAN, K.; BAGGILI, I; BREITINGER, F. **Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy**. Digital investigation, v. 18, p. S66-S75, 2016. Disponível em: https://doi.org/10.1016/j.diin.2016.04.006. Acesso em 12 abr. 2025.

FANG, S.; STAMM, M. C. **Attacking image splicing detection and localization algorithms using synthetic traces**. arXiv preprint, arXiv:2211.12314, 2022. Disponível em: https://arxiv.org/abs/2211.12314. Acesso em 24 mar. 2025.

GARFINKEL, S. L. **Anti-forensics: Techniques, detection and countermeasures.** First International Conference on i-Warfare and Security (ICIW). 2006. Disponível em: https://www.researchgate.net/publication/228339244_Anti-forensics_Techniques_detection_and_countermeasures. Acesso em 24 mar. 2025.

GUPTA, K.; OLADIMEJI, D.; VAROL, C.; RASHEED, A.; SHAHSHIDHAR, N. **A Comprehensive Survey on Artifact Recovery from Social Media Platforms: Approaches and Future Research Directions**. Information 2023, 14, 629. Disponível em: https://doi.org/10.3390/info14120629. Acesso em 12 abr. 2025.

JAVED, Abdul Rehman et al. **A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions**. IEEE Access, v. 10, p. 11065-11089, 2022. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9678340&isnumber=9668973. Acesso em 20 de out. 2024.

KHALID, Saneeha; HUSSAIN, Faisal. **VolMemDroid—Investigating Android malware insights with volatile memory artifacts**. Expert Systems with Applications, v. 253, p. 124347, 2024. Disponível em: 10.1016/j.eswa.2024.124347. Acesso em 20 abr. 2025.

RICK, A.; SAM, B.; JANSEN, W. **Guidelines on Mobile Device Forensics**. National Institute of Standards and Technology, US Department of Commerce. Retrieved, v. 6, n. 17, p. 2014, 2014. Disponível em https://doi.org/10.6028/NIST.SP.800-101r1. Acesso em 22 mar. 2025.

SABILLON, R. et al. **Digital forensic analysis of cybercrimes: Best practices and methodologies**. International Journal of Information Security and Privacy, v. 11, n. 2, p. 25–37, 2017. Disponível em https://www.researchgate.net/publication/314732188_Digital_Forensic_Analysis_of_Cybercrimes_Best_Practices_and_Methodologies. Acesso em 12 abr. 2025

SYLVE, Joe; CASE, Andrew; MARZIALE, Lodovico; RICHARD III, Golden G. **Acquisition and analysis of volatile memory from Android devices**. Digital Investigation, v. 8, p. 175–184, 2012. Disponível em: 10.1016/j.diin.2011.10.003. Acesso em 20 abr. 2025.

YANG, Haiyu; ZHUGE, Jianwei; LIU, Huiming; LIU, Wei. **A tool for volatile memory acquisition from Android devices**. IFIP International Conference on Digital Forensics (DF), 12., 2016, New Delhi, India. Proceedings [...]. New Delhi: Springer, 2016. p. 365–378. Disponível em: 10.1007/978-3-319-46279-0_19. Acesso em 12 abr. 2025.

ZHAO K, ZHANG H, LI J, PAN Q, LAI L, NIE Y, ZHANG Z. **Social Network Forensics Analysis Model Based on Network Representation Learning**. Entropy. 2024; 26(7):579. Disponível em: https://doi.org/10.3390/e26070579. Acesso em 12 abr. 2025.

ZHENG, Jiamin; TAN, Yu-an; ZHANG, Xiaosong; LIANG, Chen; ZHANG, Changyou; ZHENG, Jun. **An anti-forensics method against memory acquiring for Android devices.** IEEE International Conference on Computer Science and Engineering (CSE) and IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC), 2017. p. 214–218. Disponível em: 10.1109/CSE-EUC.2017.45. Acesso em 12 abr. 2025.

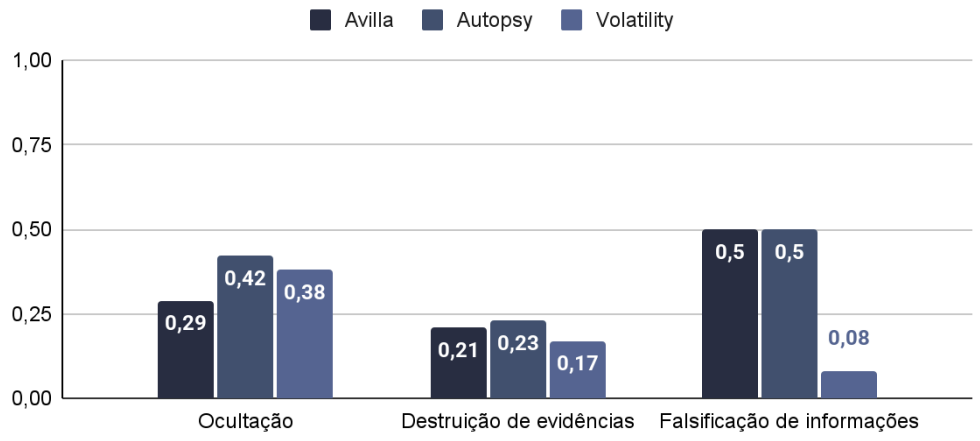
APÊNDICE A - Especificações do ambiente de testes

Componente	Descrição
Sistema Operacional Host	Windows 11 Pro 22H2 (x64)
Processador	Intel Core i5, 16 GB RAM
Emulador	Android Virtual Device (AVD) – Android 12 (API 31, x86_64)
Armazenamento	SSD 224 GB
Ferramentas Forenses	Avilla Forensics, Autopsy, Volatility, Hunchly, ArchiveBox, ArchiveTeam Tools
Outras Ferramentas	Android Debug Bridge (ADB), SDK Tools, Python 3.11, Java JDK 17
Ambiente de Controle de Versão	Git (repositório privado)

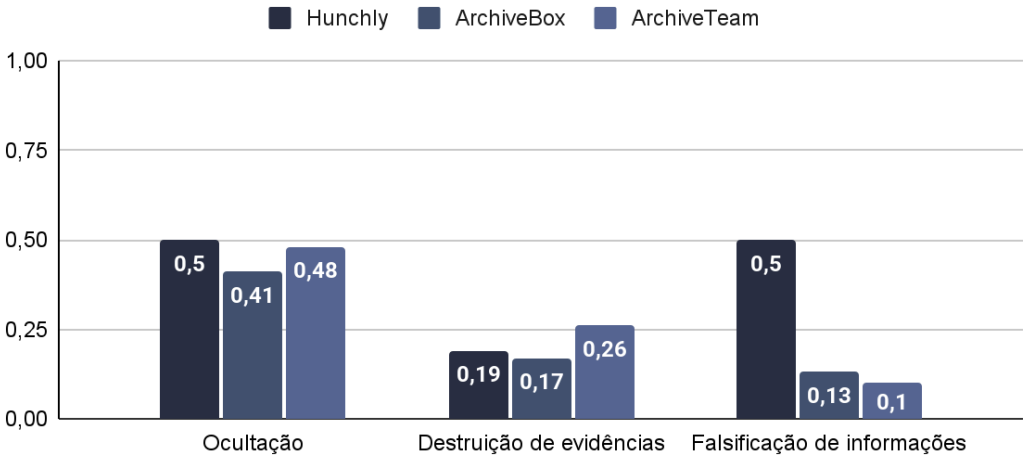
APÊNDICE B - Ferramentas forenses empregadas

Ferramenta	Categoria	Finalidade principal
Avilla Forensics	Móvel	Extração e análise de artefatos de aplicativos Android
Autopsy	Geral	Análise de imagens de disco; reconstrução de evidências
Volatility	Memória	Extração de artefatos voláteis em dumps de memória
Hunchly	Web	Captura e documentação de navegação investigativa em redes sociais
ArchiveBox	Web	Arquivamento completo de páginas e posts
ArchiveTeam Tools	Web	Coleta em massa e preservação de sites ou perfis para análise posterior

APÊNDICE C - Resultados: IFC das aplicações móveis



APÊNDICE D - Índice Forense Composto (IFC) para redes sociais e web



Fonte: Elaborado pela autora (2025).