ANÁLISE FORENSE DIGITAL: TÉCNICAS E FERRAMENTAS MODERNAS PARA INVESTIGAÇÃO

Luis Henrique dos Santos Oliveira
Discente
luis.oliveira114@fatec.sp.gov.br

Ana Luiza Godoy Pulcinelli
Orientadora
ana.pulcinelli@fatec.sp.gov.br

RESUMO

Esta pesquisa destaca a forense digital como ferramenta essencial para combater crimes cibernéticos, identificando autores e apoiando vítimas. Frente ao aumento desses crimes e à falta de conhecimento dos usuários, principalmente devido ao "erro humano", são necessárias estratégias eficazes para proteger o ambiente digital. O estudo apresenta conceitos, procedimentos e ferramentas usadas nas investigações digitais. A metodologia é bibliográfica, baseada em fontes recentes e confiáveis. Conclui-se que a forense digital é fundamental na prevenção, investigação e resolução de delitos virtuais. Além disso, enfatiza a importância de investir na capacitação de profissionais e no desenvolvimento de tecnologias, visando antecipar ameaças, responder rapidamente aos incidentes e aumentar a segurança e confiança dos usuários no ambiente digital.

Palavras-chave: Forense Digital. Cibersegurança. Computação Forense.

ABSTRACT

This research highlights digital forensics as an essential tool to combat cybercrimes by identifying perpetrators and supporting victims. Given the rise of these crimes and users' lack of knowledge, mainly due to "human error", effective strategies are needed to protect the digital environment. The study presents concepts, procedures, and tools used in digital investigations. The methodology is bibliographic, based on recent and reliable sources. It concludes that digital forensics are fundamental in preventing, investigating, and resolving virtual crimes. Furthermore, it emphasizes the importance of investing in professional training and technology development to anticipate threats, respond quickly to incidents, and increase user security and trust in the digital environment.

Keywords: Digital Forensics. Cybersecurity. Forensic Computing.

1 INTRODUÇÃO

À medida que o mundo se torna cada vez mais digital, a ocorrência de ataques cibernéticos cresce proporcionalmente, impulsionada por falhas de segurança, vulnerabilidades tecnológicas e erros humanos. De acordo com dados apresentados pelo órgão de inteligência e segurança interna dos Estados Unidos, o *Federal Bureau of Investigation* (FBI), entre os anos de 2018 e 2022, foram reportados 3,26 milhões de ocorrências de crimes cibernéticos para o *Internet Crime Complaint Center* (IC3), o setor do FBI que lida com crimes digitais em sua maioria. O IC3 estima que estas ocorrências registradas no período de 5 anos, contabilizam uma perda de 27,6 bilhões de dólares (FBI, 2022).

Na Europa, a *European Union Agency for Cybersecurity* (ENISA), chama a atenção para um desafio emergente: o uso de inteligências artificiais (IAs) para manipulação de informações, o que representou um risco significativo *para as eleições* europeias de 2024. Segundo dados da ENISA, entre julho de 2022 e junho de 2023, foram registrados 2580 incidentes relacionados a manipulações de informações através de IAs. Desse total, 19% dos ataques tiveram como alvo o setor de administração pública, 8% afetaram o setor de saúde, e 6% foram direcionados aos setores de manufatura, transporte e finanças combinados. Os dados revelam uma estratégia focada dos cibercriminosos em atingir funcionários em posições-chave, como políticos, servidores públicos, jornalistas e ativistas, evidenciando um cenário de vulnerabilidade em áreas críticas da sociedade (ENISA, 2023).

Trazendo esse problema para um cenário mais próximo, segundo uma pesquisa realizada pelo laboratório de inteligência e ameaças, FortiGuard Labs, que pertence à empresa Fortinet e publicada pelo CNN, o levantamento feito na América Latina, apontou que o Brasil é o segundo país com mais ataques cibernéticos, atrás somente do México. No primeiro semestre de 2021 no Brasil foram registradas 16,2 bilhões de tentativas de ataques cibernéticos a empresas. Enquanto em 2022, seu primeiro semestre registrou 31,5 bilhões de tentativas de ataques, um aumento de 94% em relação ao ano anterior. Já o México, registrou 85 bilhões de tentativas no mesmo período (CNN Brasil, 2022).

Segundo Alexandre Bonatti, diretor da Fortinet, uma das justificativas para esse aumento significativo de ataques no Brasil, é o baixo investimento em cibersegurança. Bonatti também destaca uma preocupação, que são os ransomwares, que funcionam como um tipo de sequestro de dados, onde os dados da vítima são criptografados e devem-se pagar ao criminoso para recuperar o acesso (CNN Brasil, 2022).

Em 2022, a Secretaria Nacional de Segurança Pública (SENASP), registrou que, no Brasil, houve um prejuízo de 1,2 bilhão de reais devido a fraudes eletrônicas, além de

prejuízos causados por outros tipos de crimes eletrônicos. Considerando este problema alarmante, a Polícia Federal inaugurou a Unidade Especial de Investigação de Crimes Cibernéticos (UEICC). Apesar de ter foco relacionado ao combate de crimes cibernéticos contra instituições bancárias, a UEICC também apresenta repressão contra diversos outros crimes praticados no ambiente digital (MJSP, 2022).

A UEICC é uma iniciativa que nasceu da parceria entre o Ministério da Justiça e Segurança Pública (MJSP) e a Federação Brasileira de Bancos (Febraban) com propósito de trocar informações para facilitar a resolução e a prevenção contra os crimes digitais (MJSP, 2022).

1.1 PROBLEMA DE PESQUISA

A crescente digitalização tem exposto indivíduos e instituições a um número cada vez maior de crimes cibernéticos, evidenciando a fragilidade na segurança digital e a falta de conhecimento adequado para prevenção e mitigação desses ataques. A dificuldade em identificar e rastrear os responsáveis por essas infrações agrava ainda mais o cenário, dificultando processos de responsabilização e reforçando a sensação de impunidade. Essa realidade revela a necessidade urgente de métodos mais eficazes e acessíveis para proteção, investigação e combate aos delitos digitais.

1.2 OBJETIVOS

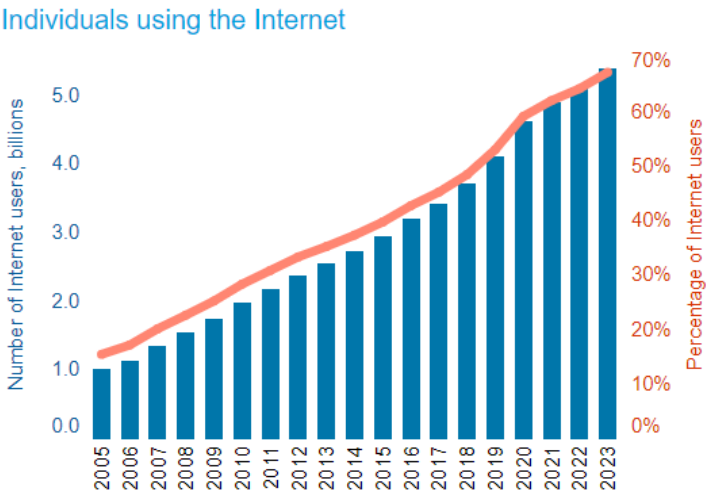
Está pesquisa tem como objetivo dissertar sobre a forense digital, destacando sua importância como ferramenta para identificação, rastreamento e responsabilização dos autores de crimes cibernéticos. Além de apresentar os conceitos mais relevantes relacionados à forense digital, descrever os procedimentos aplicados pelos profissionais da área para a investigação de crimes virtuais, identificar as ferramentas utilizadas no processo de análise e investigação digital e, explicar os principais tipos de crimes cibernéticos enfrentados atualmente.

1.3 JUSTIFICATIVA

A pesquisa está fundamentada na relevância do tema para a segurança digital, na lacuna de conhecimento e na necessidade de estratégias mais eficazes para combater os crimes virtuais. Destacando principalmente a ameaça crescente dos crimes cibernéticos, a necessidade de métodos eficazes para enfrentá-los, a importância da forense digital e a deficiência do conhecimento dos usuários.

2 DESENVOLVIMENTO

Segundo a ITU (*International Telecommunication Union*), 67% da população global possui acesso aos meios digitais. E os dados indicam que a tendência é que este número continue somente a crescer com o passar dos anos. Com base nesse dado, é perceptível como a computação forense se faz cada vez mais necessária no cotidiano da era moderna digitalizada (ITU, 2024).



Fonte: ITU, 2024

É importante primeiro entender o que de fato é a computação forense. A computação forense, é um campo da ciência forense que tem como objetivo investigar crimes cibernéticos, e de acordo com a IBM Brasil (2023), “A computação forense, também conhecidas como forense digitais, ciência forense da computação ou forenses cibernéticos, combina a ciência da computação e a forense legal para coletar evidências digitais de maneira admissível em um tribunal de justiça”.

2.1 FORENSE DIGITAL

Com o surgimento dos computadores pessoais no início da década de 80, a tecnologia tornou-se cada vez mais presente e essencial no cotidiano ao longo dos anos. Criminosos perceberam ali uma oportunidade para agir e começaram a realizar crimes em dispositivos eletrônicos. Isso destacou a importância da computação forense, que precisou evoluir com o tempo, para acompanhar o avanço da tecnologia e dos métodos desenvolvidos pelos criminosos.

A computação forense eventualmente passou a ser chamada de forense digital visto que a computação é uma área que evoluiu rapidamente, considerando que desde seu surgimento no fim do século XX até os dias atuais, passou de máquinas enormes e de pouco acesso, para dispositivos móveis comuns, computadores pessoais e até mesmo a computação em nuvem e a inteligência artificial (AFD, 2023).

Adotando então o termo forense digital, seu significado foi ampliado, para incluir a prática de recuperação, investigação, exame e análise a todo e qualquer dispositivo que armazene dados digitais, sejam esses dispositivos particulares ou corporativos. Sendo assim, a Academia de Forense Digital define este campo como: “um ramo da Computação Forense, utilizada por

Peritos Digitais, para recuperar e investigar materiais encontrados em dispositivos digitais, com o objetivo de identificar evidências digitais, que podem estar relacionados a crimes cibernéticos". (AFD, 2023).

De forma simplificada, a forense digital aplica métodos cientificamente desenvolvidos para lidar com crimes digitais de maneira prática, permitindo a reconstrução dos eventos criminosos, a identificação dos responsáveis e a prevenção de futuros crimes digitais. Entretanto, como afirma o professor Rafael Alcadipani, "Não se trata apenas de compreender o funcionamento de uma nova tecnologia, mas de decifrar a lógica e a motivação que conduzem o criminoso moderno. Para os operadores do direito, a curva de aprendizado é íngreme e urgente" (KONNO JÚNIOR, 2024, p. 8).

2.2 PROCEDIMENTOS ADOTADOS

Nesse cenário, a forense digital exige de profissionais qualificados e grandes investimentos em TI para que possam enfrentar os desafios das perícias. Três fatores são cruciais: o fator humano, que envolve a capacidade de compreender, tratar informações e analisar vestígios através de raciocínio e deduções; o fator tecnológico, que abrange as facilidades e dificuldades impostas pela tecnologia, especialmente no que diz respeito ao tempo e espaço; e o fator legal, que requer que análise dos vestígios cibernéticos siga normas legais, processuais e princípios científicos (VELHO, 2016).

Da mesma forma que em uma cena de crime as evidências físicas devem ser coletadas e tratadas de modo correto e cuidadoso pelos agentes da lei, as provas digitais devem ser recolhidas e armazenadas sem alterações, seguindo o conjunto de norma técnica ABNT NBR ISO/IEC 27037:2013, publicada pela Associação Brasileira de Normas Técnicas (ABNT). Este procedimento é realizado em quatro etapas: Coleta, Exame, Análise e Resultados Obtidos. A Coleta consiste em identificar possíveis fontes de dados ou evidências físicas e registrá-las, sem comprometer sua integridade. O Exame por sua vez, irá extrair informações relevantes dos dados coletados, utilizando de ferramentas adequadas. A Análise gera resultados relevantes e concisos para a investigação através das informações obtidas no Exame. Por fim, os Resultados são apresentados de modo objetivo e claro, para que sejam entendidos por todos os envolvidos no processo (KENT, *et al*, 2006, p. 25-30).

Considerando a variedade de ferramentas disponíveis para os profissionais de forense digital, muitas das quais compartilham o mesmo propósito, tornou-se crucial padronizar certas terminologias no campo. Essa padronização facilita a comunicação entre diferentes ferramentas, softwares e profissionais, independentemente de sua localização no mundo.

Por exemplo, um termo muito comum e importante na área é a função *hash*, que se refere a um algoritmo cujo seu resultado apresenta um valor de tamanho fixo em hexadecimal, esse resultado é irreversível e qualquer alteração afetará a integridade dos dados. Uma de suas utilizações é justamente garantir que dados coletados como evidência não foram alterados. Outro termo importante, é o metadado, que se refere a dados que descrevem informações sobre outros dados, como por exemplo, data e hora de criação de um arquivo e seu tamanho (CSRC, 2024).

Também deve-se destacar o termo, criptografia, esse é o processo de transformar informações legíveis em um formato decodificado que apenas pessoas autorizadas podem acessar. Existem dois tipos principais de criptografia, sendo elas a simétrica onde a mesma chave utilizada para criptografar é utilizada para descriptografar, e o tipo assimétrica, onde é usado um par de chaves, uma para criptografar e outra para descriptografar (CSRC, 2024).

Há também o malware, termo usado para se referir a um software ou firmware destinado a executar um processo não autorizado que terá um impacto adverso na confidencialidade, integridade ou disponibilidade de um sistema de informação. Os malwares, popularmente são chamados de vírus, o que é parcialmente correto, visto que os vírus são um tipo de malware, assim como trojan, ransomware, spyware e adware, também são exemplos de códigos maliciosos, cada um desses tendo uma finalidade diferente e operando de modos distintos (CSRC, 2024).

2.3 FERRAMENTAS UTILIZADAS

Quanto às ferramentas utilizadas, existem muitas opções a serem consideradas, mas uma das quais se destacou bastante no Brasil, foi o IPED Forense (Indexador e Processador de Evidências Digitais), muito utilizada pela Polícia Federal em investigações que repercutiram no passado, como por exemplo o Mensalão e a Operação Lava Jato. Desenvolvido em 2012, pelo Perito Criminal Federal Luís Filipe Nassif, o IPED surgiu como uma ferramenta com foco na eficiência, auxiliando em um ponto crucial para as diversas áreas da forense digital, o tempo (AFD, 2022).

A velocidade de processamento é muito importante para os profissionais e na época, as ferramentas utilizadas realizavam buscas do zero, sem um banco de dados com palavras, atrasando a busca por respostas. Esse foi o diferencial do IPED, após os arquivos serem processados, é criado um catálogo com cada palavra e sua localização nas provas, tornando o processo de busca através de palavras-chave eficazes e eficientes, com resultados instantâneos. Apesar da Polícia Federal utilizar a plataforma desde 2012, somente em 2019 ela foi aberta ao público, ganhando reconhecimento internacional e mundial, sendo considerada uma das melhores ferramentas disponíveis na área (AFD, 2022).

O FTK Imager é mais uma das ferramentas que se destaca na área. Sendo um software gratuito desenvolvido pela *AccessData*, sua função é conseguir evidências através de unidades de armazenamento, utilizado principalmente para adquirir imagens forenses. De modo simples, uma imagem forense, é uma cópia dos dados de um dispositivo de armazenamento. Entretanto, existem muitas possibilidades de cenários e é necessário saber adaptar a ferramenta para cada um deles (Tsukahara, 2023).

O processo começa identificando a origem da evidência para realizar sua aquisição, para isso o FTK Imager conta com algumas opções, como por exemplo, criar uma imagem através de um disco físico inteiro, capturando todas suas possíveis partições, ou então criar uma imagem de uma partição selecionada de um disco físico. Outra possibilidade é selecionar pastas e arquivos individualmente, além de CDs, DVDs, pen drives e outros dispositivos USB. Há também a opção de utilizar filtros no momento da busca, para facilitar a aquisição de evidências. Porém a ferramenta não dispõe de muitos recursos para processar os dados adquiridos, sendo assim necessário utilizar outros softwares com esse propósito, como por exemplo o IPED (Tsukahara, 2023).

A análise forense em memórias voláteis (RAM) é de extrema importância, visto que essas memórias podem conter muitas informações importantes como listas de processos, rastros de malwares, conexões de IP, tanto ativas como finalizadas, chaves de criptografia, entre outras coisas. Sendo assim, outra ferramenta gratuita e de código livre ganha destaque, o Volatility Framework, esta ferramenta é utilizada para a análise da memória volátil. Sendo usado principalmente em ambientes Linux, até mesmo estando presente nativamente em algumas de suas distribuições voltadas para segurança, mas também é possível a utilização da ferramenta em sistemas Windows e MacOS (Rodrigues, 2021).

Um ponto a se falar sobre o Volatility, é a possibilidade de implementação de plug-ins para implementação de ferramentas e recursos que o usuário julgar necessárias para o uso, como por exemplo o *PsTree*, que permite trilhar a origem de um processo e o *PsScan*, que procura e revela processos escondidos dentro de outros processos. Entretanto, para alguns isso é considerado uma desvantagem, visto que em situações de primeiro uso, a instalação dos plug-ins pode ser demorada antes que se consiga efetivamente utilizar a ferramenta. Outro problema envolve uma atualização do software, que quando saiu de sua versão 2.6 para a 3.0, muitos plug-ins considerados importantes se perderam, e mesmo que a comunidade de usuários tenha desempenhado esforços para suprir a ausência desses plug-ins, ainda não se encontram substitutos para todos aqueles que eram considerados importantes (Rodrigues, 2021).

2.4 CRIMES CIBERNÉTICOS

O cibercrime, também conhecido como crime cibernético, refere-se a atividades criminosas realizadas no ambiente digital. De modo geral, essas práticas podem ser classificadas em duas categorias principais: aquelas em que o dispositivo eletrônico é o alvo do ataque, como invasões e sequestro de dados, e aquelas em que o dispositivo é utilizado como ferramenta para a execução de delitos, como fraudes financeiras e disseminação de malware. Assim, o termo "cibercrime" engloba uma ampla e diversificada gama de atividades maliciosas. Diante dessa complexidade, é importante destacar alguns dos principais tipos de crimes cibernéticos que ameaçam a segurança digital, como por exemplo o hacking, o phishing, ransomware, entre outros.

O hacking é um dos crimes mais comuns, que consiste no acesso não autorizado a sistemas digitais, incluindo computadores, dispositivos móveis e redes. Essa atividade criminosa costuma ser acompanhada por ações subsequentes, como roubo de dados e informações confidenciais, espionagem, e a instalação de softwares maliciosos (malwares). Em situações mais graves, os ataques podem atingir proporções nacionais ao comprometer infraestruturas críticas, como sistemas governamentais e redes de comunicação. Além do caráter criminoso, há também casos em que indivíduos realizam o hacking por motivações intelectuais, tratando-o como um desafio técnico e exploratório (CSRC, 2025).

O phishing é um crime cibernético amplamente disseminado, tratando-se de uma técnica de fraude digital que visa obter dados sensíveis, como informações bancárias e credenciais de acesso, por meio de solicitações fraudulentas em e-mails, sites falsos ou mensagens instantâneas. Essa prática se baseia na manipulação psicológica das vítimas, levando-as a fornecer informações pessoais de forma voluntária. Para isso, os criminosos costumam imitar comunicações de instituições confiáveis, como bancos, empresas ou órgãos públicos, criando um falso senso de urgência ou medo. As consequências do phishing podem incluir o comprometimento de contas bancárias, perdas financeiras significativas e até mesmo roubo de identidade (CSRC, 2025).

Já o ransomware é um tipo de malware que criptografa os dados de sua vítima e exige um resgate para restaurar o acesso. Esse tipo de crime em especial, pode ser devastador para empresas, podendo causar paralisações operacionais significativas. O ransomware é uma das formas mais lucrativas de cibercrime, onde os criminosos frequentemente exigem pagamentos em criptomoedas para dificultar o rastreamento. As vítimas que vão desde pequenas empresas até grandes corporações, enfrentam a difícil decisão entre pagar o valor exigido ou renunciar ao acesso aos dados críticos (CSRC, 2025).

Apesar de não ser uma prática exclusiva dos meios digitais, fraudes e roubos de identidades são muito comuns entre os cibercrimes. Com a quantidade de informações pessoais disponíveis online, cibercriminosos podem usar dados roubados para cometer fraudes financeiras, como solicitar empréstimos ou abrir contas no nome da vítima. Este tipo de crime pode ter consequências duradouras na vida das vítimas, como dificuldade em acessar crédito ou danos a reputação financeira. Os criminosos costumam obter esses dados através de outras práticas criminosas, como violações de dados em grande escala, phishing ou compra de dados no mercado clandestino. Combater este tipo de crime requer vigilância constante e medidas de segurança para dados pessoais (ADVBOX, 2024).

Outro cibercrime que vem se tornando cada vez mais comentado nos últimos anos, é o cyberbullying e o assédio online, onde o criminoso utiliza de plataformas digitais para intimidar, ameaçar ou assediar indivíduos. Esta forma de crime pode afetar o bem-estar e a saúde mental de suas vítimas, visto que a natureza anônima da internet algumas vezes incentiva comportamentos agressivos e dificulta identificar e responsabilizar os agressores. Entretanto, esse tipo de crime requer uma abordagem legal para proteger as vítimas (ADVBOX, 2024).

Segundo a Forbes, o Brasil é o quinto pais no mundo que mais atacado por cibercriminosos, onde se destacam crimes como phishing, roubo de dados, fraudes e extorsão, hacking para violação de acesso e infiltração de sistemas, e roubo de propriedade intelectual (FORBES, 2023).

Nos Estados Unidos, segundo dados do FBI, alguns dos crimes mais comuns no país são, phishing, extorsão e roubo de dados, mostrando uma semelhança com os tipos de crimes enfrentados no Brasil e destacando uma tendencia entre os cibercriminosos (FBI, 2022).

4 METODOLOGIA

Para a elaboração deste artigo, foi adotada uma metodologia bibliográfica, com a revisão e análise de fontes diversas, incluindo livros especializados, artigos acadêmicos, publicações em periódicos científicos e materiais disponibilizados por organizações e instituições reconhecidas no campo da forense digital. A seleção das fontes foi criteriosa, priorizando obras de autores renomados e publicações recentes que refletissem os avanços mais atuais em técnicas e ferramentas de análise forense digital. Além disso, foram consultados estudos de caso e relatórios técnicos que ilustram a aplicação prática das metodologias discutidas. Essa abordagem permitiu uma visão abrangente e aprofundada do tema, garantindo a consistência e a relevância das informações apresentadas no artigo.

5 CONSIDERAÇÕES FINAIS

Assim, conclui-se que diante do aumento significativo dos crimes digitais, independentemente de sua natureza, torna-se essencial adotar estratégias eficazes para combatê-los. Nesse contexto, a forense digital desempenha um papel fundamental, tanto na investigação e prevenção desses delitos quanto na garantia de um ambiente digital mais seguro. Além disso, possibilita que as vítimas tenham respaldo adequado ao se tornarem alvos de cibercriminosos. Vale destacar que a principal causa das vulnerabilidades digitais é a falta de conhecimento e o descuido dos usuários, o chamado “erro humano”, onde, em muitos casos, um único clique pode ser suficiente para causar grandes problemas.

Além disso, é fundamental ampliar os investimentos na área, tanto para atrair novos profissionais quanto para desenvolver métodos mais eficazes no combate aos diversos tipos de crimes digitais. Com isso, torna-se possível não apenas antecipar a ocorrência desses delitos, mas também garantir uma resolução mais rápida e eficiente quando eles acontecem. Dessa forma, é possível quebrar o paradigma de que o ambiente digital é inseguro, promovendo mais confiança e proteção para os usuários.

6 REFERÊNCIAS

ADVBOX, **Cibercrime: entenda o que é, quais são os tipos e como prevenir**. Disponível em: https://advbox.com.br/blog/cibercrime/. Acesso em 09 de mai. 2025.

AFD, Academia de Forense Digital. **Forense Digital: Descubra a sua importância!** Disponível em: https://academiadeforensedigital.com.br/forense-digital-descubra-a-sua-importancia/. Acesso em 30 de jul. 2024.

AFD, Academia de Forense Digital. **O Sistema IPED Forense: Processador e Indexador de Evidências Digitais da Polícia Federal**. Disponível em: https://academiadeforensedigital.com.br/sistema-iped-forense/. Acesso em: 18 de jul. 2024.

CNN Brasil. **Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%**. Disponível em: https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/. Acesso em: 17 de jul. 2024.

CSRC, Computer Security Resource Center. **Glossary**. Disponível em: https://csrc.nist.gov/glossary. Acesso em: 09 de mai. 2025.

ENISA. **EU Elections at Risk with Rise of AI-Enabled Information Manipulation**. Disponível em: https://www.enisa.europa.eu/news/eu-elections-at-risk-with-rise-of-ai-enabled-information-manipulation. Acesso em: 18 de jul. 2024.

FBI, Federal Bureau of Investigation. **Internet Crime Report**. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. Acesso em: 17 de jul. 2024.

FORBES, **5 tipos mais comuns de ciberataques que ocorrem no Brasil**. Disponível em: https://forbes.com.br/forbes-tech/2023/05/5-tipos-mais-comuns-de-ciberataques-que-ocorrem-no-brasil/#foto4. Acesso em 09 de mai. 2025.

IBM, Internetional Bussines Machines, Brasil. "**O que é computação forense?".** Disponível em: https://www.ibm.com/br-pt/topics/computer-forensics. Acesso em 17 de jul. 2024.

ITU, International Telecommunication Union. **Statistics: Individuals using the internet**. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. Acesso em 17 de jul. 2024.

KENT, Karen, *et al*. **Guide to Integrating Forensic Techniques into Incident Response**. Gaithersburg, Nist Special Publication, 2006. Disponível em: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf. Acesso em 24 de jul. 2024.

KONNO JÚNIOR, Janio. **Tecnologia Como Garantia de Direitos Fundamentais na Investigação Criminal**. Londrina: Editora Thoth, 2024. Disponível em: https://editorathoth.com.br/produto/tecnologia-como-garantia-de-direitos-fundamentais-na-investigacao-criminal/930. Acesso em 24 de jul. 2024.

MSJP, Ministério da Justiça e Segurança Pública. **Polícia Federal cria Unidade Especial para intensificar a repressão a crimes cibernéticos**, 2022. Disponível em: https://www.gov.br/mj/pt-br. Acesso em 7 de set. 2024.

RODRIGUES, Vladimir. **Introdução ao Volatility 3**. AFD, Academia Forense Digital, 2021. Disponível em: https://academiadeforensedigital.com.br/introducao-ao-volatility-3/. Acesso em 27 de jul. 2024.

TSUKAHARA, João. **FTK Imager: Principais funções de uma das ferramentas forenses mais populares da última década**. AFD, Academia Forense Digital, 2023. Disponível em: https://academiadeforensedigital.com.br/ftk-imager-ferramenta-gratuita-de-forense-digital/. Acesso em 25 de jul. 2024.

VELHO, Jesus Antonio. **Tratado de Computação Forense**. Campinas: Millennium Editora, 2016. Disponível em: https://www.millenniumeditora.com.br/tratado-de-computacao-forense// Acesso em 20 de jul. 2024.