Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

CONSIDERAÇÕES INICIAIS

Versa o presente Parecer Técnico, por solicitação da SR. LUCAS SANCHES PROMESSIA, inscrito no CPF nº 443.342.918-05, candidato a Prefeito Municipal de Guarulhos, Estado de São Paulo, o exame pericial e análise técnica acerca da evidência digital (vídeo), oriundo de sua vinculação e divulgação na Rede Social www.youtube.com, e empregado para acusar LUCAS SANCHES de atos de corrupção.

1 PROTOCOLO DO EXAME PERICIAL

Considerando a fragilidade das evidências digitais, faz-se necessário seguir rigorosamente um padrão de condutas quanto a seu devido tratamento, no intuito em garantir a integridade e autenticidade, os quais são requisitos mínimos para a prova digital possuir valor probatório juridicamente. Neste sentido, em todo o trabalho pericial, devem ser obedecidas as metodologias em conformidade ao que regula a Norma ABNT NBR ISO/IEC 27037:2013. A norma possui por objetivo qualificar a evidência digital como material probante, pois ao tratar de Evidências Digitais é imprescindível seguir os protocolos, pois eles irão conferir admissibilidade, relevância e força probatória.

No Brasil, o ato normativo que tem maior amplitude é a obra denominada “Procedimento Operacional Padrão: Perícia Criminal”, publicada pelo Ministério da Justiça, através da Secretaria Nacional de Segurança Pública - portaria nº 82 de 16 de julho de 2014 da SENASP/MJ. Esse documento traz uma padronização mínima para as perícias criminais em todo território nacional e lança luz sobre a área de Computação Forense.

O presente trabalho também se baseou sobre as mais atuais referências bibliográficas da doutrina nacional, que versam sobre o tema Ciências Forenses, Computação Forense e Perícia Digital, dando-se destaque ao livro de maior relevância, **Tratado de Computação Forense** (ISBN 978-85-7625-335-8) da Millennium Editora, escrito em 2016 por vários autores e colaboradores, sendo a grande maioria Peritos Criminais da Polícia Federal, reconhecidos nacionalmente e internacionalmente.

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

Importante destacar também, que todo o procedimento pericial digital requer (04) quatro etapas, conforme Rodrigo Barbosa e Luiz Eduardo Gusmão mencionam na obra Tratado de Computação Forense (2016:91), descrevendo as fases básicas do exame pericial, como sendo:

- **Preservação e Coleta dos Dados**: Possui como objetivo principal em garantir que a evidência digital não sofra alterações durante a realização do exame;
- **Extração e Indexação dos Dados**: Visa a identificação dos dados coletados;
- **Análise**: Cuja finalidade é identificar nos arquivos questionados informações relevantes ao fato que está sob investigação;
- **Apresentação**: Refere-se ao modo como o perito irá formalmente relatar suas conclusões ao final dos exames.

1.1 Tratamento Da Evidência Digital Utilizada Como Meio De Prova

A Evidência Digital pode facilmente ser alterada, adulterada ou destruída devido ao tratamento incorreto. É altamente recomendado que os indivíduos que irão realizar o tratamento da Evidência Digital sejam competentes para identificar e administrar os riscos e consequências advindos de possíveis linhas de conduta quando tratam com a evidência.

Em casos em que a investigação verifica a necessidade em apurar a dinâmica dos eventos registrados em câmeras de monitoramento (Circuito Interno de Monitoramento) em arquivos de vídeo, estes devem seguir rigorosamente um padrão de condutas quanto a seu devido tratamento, visando garantir a integridade e autenticidade nos arquivos apurados na persecução penal, garantindo um suporte jurídico que contribuirá para obter sua admissibilidade, força probatória e relevância em processos judiciais ou criminais. Durante a condução da colheita de elementos e informações de prova, estas, necessitam estar em conformidade ao que regula a Norma ABNT NBR ISO/IEC 27037:2013, visando a garantia de integridade sobre as provas

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

obtidas, para evitar que estas sejam invalidados por dúvidas sobre eventual manipulação ou contaminação do material questionado. Para isso, deve-se ter o devido cuidado no manuseio dos equipamentos e mídias recebidas para análise, tais procedimentos devem garantir que:

- Nenhuma evidência seja alterada ou destruída (garantia de integridade);
- Seja estabelecida e mantida a Cadeia de Custódia;
- Caso o equipamento esteja em uso, o tempo de intervenção seja o menor possível;
- Informações não pertinentes ao escopo da investigação não sejam divulgadas (princípios éticos e legais);
- Não seja criada alguma condição que possa inviabilizar uma verificação futura (possibilidade de auditoria);
- Todo o processo seja documentado para permitir a sua reprodução futura (possibilidade de auditoria).

Neste sentido, em demandas que envolvam a utilização de evidências digitais como meio de prova, estas, devem ser tratados com especial atenção, principalmente nos casos relacionados a atividades criminosas. Tomando-se os devidos cuidados, desde a coleta e/ou busca e apreensão sobre os dispositivos questionados, tem-se uma fonte valiosíssima de provas judiciais a serem utilizadas durante a persecução penal.

1.2 Requisitos Para o Manuseio Da Evidência Digital

Conforme regula a Norma ABNT NBR ISO/IEC 27037:2013, Evidência Digital é governada por três princípios fundamentais: **Relevância, Confiabilidade e Suficiência**.

Estes três princípios são importantes para todas as investigações, não apenas para que aquelas evidências digitais sejam admitidas nos tribunais. A evidência digital é relevante quando se destina a provar ou refutar um elemento de um caso

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

específico que está sendo investigado. O significado geral do princípio “para garantir que a evidência digital seja o que pretende ser” é amplamente defendido.

No que compete ao princípio de Confiabilidade, a norma recomendada que todos os processos utilizados no manuseio da potencial Evidência Digital sejam passíveis de auditoria e repetições. Havendo (04) quatro aspectos-chave no manuseio da Evidência Digital: Auditabilidade, Justificabilidade e Repetibilidade ou Reprodutibilidade, dependendo das circunstâncias particulares:

- **Auditabilidade:** Possui o intuito de determinar se o método científico, técnica ou o procedimento foi adequadamente seguido. É altamente recomendado que os processos realizados sejam documentados para uma avaliação nas atividades realizadas;
- **Repetibilidade:** Este conceito é considerado quando os mesmos resultados de testes são produzidos utilizando os mesmos procedimentos e métodos de medição, utilizando os mesmos instrumentos e sob as mesmas condições; e pode ser repetido a qualquer tempo depois do teste original;
- **Reprodutibilidade:** Este conceito é válido quando os mesmos resultados são produzidos utilizando diferentes instrumentos, diferentes condições; e a qualquer tempo. Exemplo: Comparando as *strings* de *Hash*;
- **Justificabilidade:** Este conceito tem como objetivo justificar todas as ações e métodos utilizados para o tratamento da evidência digital. A justificativa será demonstrando que a decisão foi a melhor escolha para obter toda a potencial evidência digital.

1.3 Preservação das Evidências Digitais

Segundo a Norma ABNT NBR ISO/IEC 27037:2013, preservação é todo o processo que visa manter e proteger a integridade e/ou a condição original da potencial evidência digital. Visando assegurar a integridade da evidência, a norma recomenda o uso da função de *Hash,* uma vez que a *Hash* é impressão digital eletrônica do arquivo digital, empregada em Forense Digital para comprovar se determinada cópia de um

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

arquivo ou se determinada versão de um arquivo confere com a versão original. Serve para averiguar a integridade de uma evidência. E quando associado a atividade pericial, é a garantia que a prova digital possui valor probatório juridicamente.

2 OBJETO DO EXAME

Ao signatário, fora disponibilizado o link de acesso ao vídeo divulgado na Rede Social Youtube.com, e utilizado na acusação contra LUCAS SANCHES.

> O YouTube foi o primeiro site de compartilhamento de vídeos em grande escala na Web e está disponível em mais de 100 países, 80 idiomas, com mais de 2 bilhões de usuários, segundo dados do próprio YouTube. O serviço foi criado por três ex-funcionários do PayPal – Chad Hurley, Steve Chen e Jawed Karim – em fevereiro de 2005. A Google comprou o site em novembro de 2006 por US$ 1,65 bilhão; desde então o YouTube funciona como uma das subsidiárias da Google. E é considerado o segundo maior buscador da internet. O YouTube é o segundo maior mecanismo de busca do mundo, por meio da sua busca interna, perdendo apenas para o Google, a quem pertence e o segundo site mais visitado, ficando atrás apenas do Google segundo dados de 2021.

2.1 Material Questionado

Consiste no vídeo divulgado na Rede Social Youtube.com, sob a URL de acesso “https://www.youtube.com/watch?v=R3xqXtyMxnw”.

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

2.1.1 Metodologia de Preservação

Objetivando garantir a integridade e autenticidade da evidência digitai inspecionada durante o trabalho pericial, foram extraídos os códigos *hash* do arquivo objeto deste trabalho pericial, conforme padroniza a Norma ABNT NBR ISO/IEC 27037:2013. A norma recomenda que seja extraída a função de *hash*, uma vez que é considerada uma impressão digital eletrônica do arquivo, que por sua vez, garante que o mesmo arquivo possa ser auditado.

Arquivo Questionado	Algoritmos de Hash	
R3xqXtyMxnw.mp4	SHA1	d81f9bc57eff3b4d291101cdccc8fdcbdcb77cb3
	SHA256	af3418928fe308eae6243a9614d2245b702cdd6f400894e8f89cc13f6a2520bb

Tabela 1 - Algoritmos de *hash* sobre os arquivos em vídeo.

4 SEGMENTAÇÃO DO MATERIAL EXAMINADO

4.1 Aspectos Gerais Sobre Vídeos Digitais

Uma imagem digital é composta pelo conjunto de milhares de *pixels. Pixel* é o menor elemento formador de uma imagem digital. Quanto maior o número de *pixels* utilizados para formar uma imagem, melhor será a qualidade da imagem em casos de ampliação.

De modo geral, um arquivo de vídeo digital é formado por uma sequência de imagens (fotogramas) ou quadros (*frames*), gravados sequencialmente num intervalo de tempo fixo, que, quando exibidos sequencialmente produzem movimento na cena.

O termo quadros por segundo ou *frames* por segundo, refere-se à cadência de gravação de um dispositivo, como uma câmera de celular, uma câmera profissional

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

ou mesmo uma câmera de monitoramento de trânsito, usualmente as câmeras fotográficas digitais filmam a uma taxa de 15, 25 ou 30 quadros por segundo (*frames* por segundo ou fps) para compor um vídeo digital, indicando o número de imagens (fotogramas) que tal dispositivo digital consegue registrar durante determinado intervalo de tempo.

4.3 Instrumental Aplicado à Análise

Durante a condução dos exames periciais, bem como reprodução com segurança dos arquivos digitais, foi produzida uma cópia de segurança sobre o conteúdo examinado e foram utilizados os seguintes equipamentos de *hardware:*

- Notebook: DELL Inspiron 5480 – Processador Core i7-8565U e Memória RAM 24GB;

No decorrer de todo o processo de exame pericial, foram utilizados os *softwares*:

- **HashCalc (2.02):** *Software* empregado na fase inicial do trabalho, utilizado na análise e extração dos algoritmos de *hash* para o arquivo questionado. O *software* permite reconhecer os algoritmos de *hash* para arquivos, *strings* (frases ou palavras) e hexadecimais;
- **Image J (1.54c):** Trata-se de um *software* de processamento de imagem baseado em Java, o que permite que ele seja executado em Linux, Mac OS X e Windows. É um programa de domínio público, utilizado no processamento de imagens científicas produzido pelo National Institute of Health (NIH, EUA). O ImageJ pode ser usado para exibir, editar, analisar, processar, salvar e imprimir imagens, apresentando diversos recursos para tratamento de imagens que podem ser utilizados para análise de imagens por microscopia, portanto, com grande aplicação em áreas forenses, médicas, biológicas e de materiais.

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

- **FFmpeg (N-104583-ge5367b481b-20211118):** Consistem em uma biblioteca com um amplo conjunto de funções e ferramentas que permitem a codificação, decodificação, e análise de diferentes padrões de vídeo.
- **Youtube-dl:** Trata-se de uma ferramenta de linha de comando baseada em *Python* que permite baixar vídeos do Youtube, Dailymotion, Photobucket, Facebook, Yahoo, Metacafe, Depositfiles e alguns outros sites semelhantes. Ele é escrito em linguagem de programação *pygtk* e requer um interpretador *Python* para executar este programa. Deve ser executado em qualquer sistema baseado em Unix, Windows ou Mac OS X.

5 METODOLOGIA APLICADA AO EXAME

Como metodologia de análise, o relator extraiu todos os *frames* (imagens) do vídeo objeto do exame, às quais, foram examinadas individualmente os trechos de interesse pericial, ampliando e aplicando técnicas de software para ressaltar os pontos de interesse pericial.

Os exames apresentados no presente Parecer Técnico, estão em conformidade a metodologia elaborada pelo Scientific Working Group on Digital Evidence (SWDE). Criado nos Estados Unidos em 1999, este grupo de trabalho foi encarregado em elaborar recomendações, princípios e definições para a Computação Forense. O Grupo desenvolve padrões de consenso, diretrizes e melhores práticas voltadas a Comunidade Forense, fornece recomendações para atividades de desenvolvimento de pesquisa e avança o estado da ciência de maneira ética. O SWGDE é composto por um Conselho Executivo, sete comitês permanentes e comitês ad-hoc nomeados conforme sua necessidade. Os comitês permanentes são: Forense de Áudio, Forense Computacional, Forense em Imagem, Forense em Fotografia, Padrões de Qualidade e Forense em Vídeo.

É posição do SWGDE que quaisquer alterações em uma imagem feitas por meio de processamento de imagem são aceitáveis em aplicações forenses, desde que os seguintes critérios sejam atendidos:

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

- A imagem original é preservada e os processos são executados em uma cópia de trabalho;
- As etapas de processamento sejam documentadas;
- Aprimoramento de imagem, de maneira suficiente para permitir que uma pessoa com treinamento comparável em compreender as etapas executadas, as técnicas utilizadas e extrair informações comparáveis da imagem.
- O resultado final é apresentado como um processamento da imagem.

5.1 Análise Acerca dos Metadados do Arquivo

Arquivos de multimídia tais como vídeos, podem revelar dados técnicos sobre o arquivo, como dados de localização geográfica, data e hora de criação e modificação do arquivo (quando produzida), etc. Estes dados são conhecidos como Metadados, e apresentam-se como elementos fundamentais na sustentação sobre a confiança na autenticidade de arquivos digitais, onde, é preciso haver metadados suficientes, tais como data de criação do arquivo, entre outros.

Metadados ou Metainformação, conceitualmente são definidos como “dados utilizados para descrever a estrutura de um dado principal”. São todos os dados descritivos de um documento arquivo, sobre autor, data de criação, local de criação, conteúdo, forma, dimensões e outras informações são metadados.

Na prática, são dados técnicos incorporados em arquivos digitais, em arquivos de multimídia podemos destacar (câmera usada, data de criação da fotografia ou vídeo, formato, tamanho do arquivo, esquema de cor etc.), ou seja, informações que são adicionadas sobre aquele arquivo e que exercem a função descritiva. Estruturalmente, podemos organizar os metadados em ao menos três tipos:

Metadados Descritivos: É a face mais conhecida dos metadados, são eles que descrevem um recurso com o propósito de identificação; podem incluir elementos tais como título, autor, resumo, palavras-chave e identificador.

Metadados Estruturais: São informações que documentam os recursos mais complexos, compostos por vários elementos, devem ser recompostos e

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

ordenados. Por exemplo, como as páginas de um livro, digitalizadas separadamente, são vinculadas entre si e ordenadas para formar um capítulo.

Metadados Administrativos: Fornecem informações que apoiam os processos de gestão do ciclo de vida dos recursos informacionais. Incluem, por exemplo, informações sobre como e quando o recurso foi criado e a razão da sua criação. Nessa categoria, estão metadados técnicos que explicitam as especificidades e dependências técnicas do recurso.

Ainda, segundo o SWGDE os metadados representam uma parte importante das imagens, especialmente para verificação de integridade. Metadados podem ajudar a estabelecer a proveniência das imagens; no entanto, pode ser editado, intencionalmente ou acidentalmente ou perdido. Isto pode impactar a capacidade de estabelecer a procedência das imagens após o fato.

5.2 Investigação Tecnológica Sobre os Eventos

Investigação Tecnológica é o conjunto de recursos e procedimentos, baseados na utilização da tecnologia, que possuem o intuito de proporcionar uma maior eficácia na investigação criminal, principalmente por intermédio da inteligência cibernética, dos equipamentos e *softwares* e ferramentas específicos que permitem a análise de grande volume de dados, a identificação de vínculos entre alvos ou na obtenção de informações impossíveis de serem agregadas de outra forma, da extração de dados de dispositivos eletrônicos, das novas modalidades de afastamento de sigilo e da utilização das fontes abertas (OSINT).

O processo de investigação digital empregado no presente capítulo, baseou-se na metodologia OSINT (*Open Source Intelligence*), que envolve o processo de coleta, análise e uso de dados de fontes públicas para propósitos inteligentes. OSINT é uma forma de gerenciamento de coleta de inteligência que localiza, seleciona e extrai informações de fontes abertas, como Instagram, Youtube, entre outros, e por fim, analisa as informações para produzir inteligência de forma que podem ser empregadas em processos de investigação criminal.

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

5.2.1 Mapeamento de Conteúdo

Uma vez constatada a existência de conteúdo compartilhado em Redes Sociais (Instagram, Youtube, entre outros), o primeiro passo é a apresentação completa do *link* de acesso (URL) a respeito do conteúdo publicado. Para torna-se necessário elaborar o “mapeamento de conteúdo”, que objetiva a apresentação de seu conteúdo.

5.2.2 Prova de Materialidade

Independente do contexto investigativo, a existência de conteúdo compartilhado em Redes Sociais, torna-se fundamental a produção de uma prova formal sobre a sua materialidade, ou seja, o que de fato ocorreu e consta na publicação, bem como os demais dados que referenciem a URL em pauta.

Tecnicamente, em eventos ocorridos nas mais diversas plataformas virtuais, toda a Prova de Materialidade deve conter ao menos as informações:

- Data, horário e padrão de fuso horário de acesso ao link/URL da publicação;
- Descrição da página eletrônica denunciada, bem como o seu conteúdo;
- Endereço da página investigada (URL);

Adicionando aos apontamentos acima, quando o conteúdo irregular é identificado em Redes Sociais, deve-se referenciar outros pontos:

- Perfil do responsável pela publicação do conteúdo;
- Identificador Único sobre o perfil responsável pelo conteúdo;
- Coleta e apresentação do conteúdo, seja na forma de imagem, áudio ou vídeo.

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

5.3 Análise Holística

A visão holística possui por definição observar ou analisar algo ou alguma área de forma global, ou seja, como um todo e não de maneira fragmentada. Durante esta etapa do exame, foram abordados aspectos gerais no que tange a observação dos pontos de interesse inserido ao escopo da perícia, por meio de uma metodologia perceptivo-visual.

6 O PERITO

Vinícius Machado de Oliveira, brasileiro, natural de Brasília – DF, CPF 80906320097; Habilitado para atuar como Auxiliar da Justiça nos Tribunais de Justiça dos Estados: AM, BA, ES, GO, MA, MG, MT, MS, PB, PE, PR, PI, RS, RO, RR, SC, SP e no DF. Cadastrado na Associação Nacional dos Peritos em Computação Forense (APECOF), sob o registro nacional n 2023809256.

Formado em Técnico em Telecomunicações; Graduado em Gestão em Tecnologia da Informação pela Faculdade UNIP Interativa; e como complemento em sua formação, concluído os cursos:

- Computação Forense (Academia de Forense Digital);
- Forense em Memória (Academia de Forense Digital);
- Técnicas de Investigação com OSINT (Academia de Forense Digital);
- Forense em Dispositivo Móveis (Academia de Forense Digital);
- Introdução à Perícias de Áudio (Academia de Forense Digital);
- Transcrição Fonográfica, Textualização e Análise de Conteúdo (Academia de Forense Digital);
- Prosopografia Forense – Apresentação e Treinamento de Medidas Faciais (PAROLE);
- Gimp Edição De Imagens Para Fins Forenses (PAROLE);
- Análise Fonético-Forense – Uma Tarefa de Comparação de Locutor;
- Análise Acústica Vocal – Teórico/Prático (SERfono);

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

- Curso de Investigação de Crimes Cibernéticos (W&B Gestão Educacional);
- Curso Remoção de Conteúdo na Internet (W&B Gestão Educacional);
- Análise Forense de *Malware* (Academia de Forense Digital);
- Avilla Forensics 3.5 - Treinamento Oficial (Academia de Forense Digital);
- IPED Forensics - do Zero ao Avançado (Academia de Forense Digital).

Bem como as Certificações;

- Computer Forensics Foundation Certification – Itcerts Inc.;
- Certified ISO/IEC 27001 Auditor – Certiprof;
- Certified LGPD Foundation (LGPDF) – Certiprof;
- AccessData Certified Investigator – AccessData;
- Certified Secure Computer User V2 (Cscu) – Ec-Council;

7 DOS EXAMES

7.1 Análise Acerca dos Metadados do Arquivo

Todo arquivo ou registro digital, tal como um arquivo em vídeo, ao ser concebido, agrega informações de data e hora de criação, extensão, resolução, tamanho do arquivo, entre outros. Em Computação Forense, estes dados são descritos como metadados, e dependendo da configuração do aparelho gravador, aquele responsável pelo registro em vídeo, podem conter dados sensíveis como: horário e data de criação (*Mactimes*), marca e modelo do aparelho, dados de localização geográfica (latitude e longitude), bem como demais características da câmera como ISO, exposição e demais configurações técnicas sobre o registro. A *timeline* é uma forma cronológica de apresentar o tempo, e a análise da linha do tempo pode indicar uma prova em um evento de edição em arquivos digitais. São chamados de *Mactimes* os campos que armazenam os registros relativos à data de criação e modificação em arquivos digitais. Dessa forma todo o evento relacionado a modificações em um arquivo digital provocará uma referência na sua estrutura de dados, alterando seus metadados, o que indicará alterações em sua linha de tempo (*timeline*).

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

Mediante ao exposto, valendo-se do *software* ffmpeg, os arquivos em vídeo questionados foram submetidos a análise de seu metadados, conforme descritos, conforme ilustrado na Figura 1.

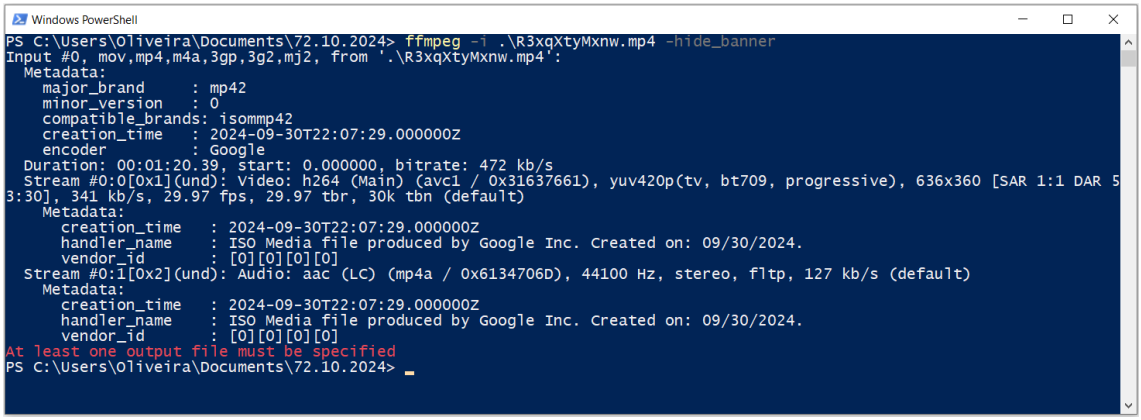

Figura 1 – Amostragem dos metadados do arquivo “R3xqXtyMxnw.mp4”.

Importante destacar que, o arquivo em vídeo questionado possui origem desconhecida, visto que, trata-se do fruto de compartilhamento na rede social youtube.com, onde não há como garantir a sua integridade e autenticidade, pois o conteúdo pode ter sido alterado ou manipulado antes de ser publicado, além de não existir uma forma confiável de verificar a Cadeia de Custódia do material.

7.2 Investigação Tecnológica Sobre os Eventos

Objetivando obter elementos de prova, vinculado na Rede Social Youtube.com, e valendo-se da metodologia OSINT (*Open Source Intelligence*), este signatário procedeu com a coleta, análise e uso de dados de fontes públicas para propósitos inteligentes, por meio da coleta de informações em fontes abertas.

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

7.2.1 Mapeamento de Conteúdo

Uma vez constatada a existência de conteúdo compartilhado em Redes Sociais, tal como Youtube.com (de fonte aberta), este signatário iniciou com a recolha e preservação das informações relevantes ao presente processo de investigação digital.

A partir da apresentação do canal ou vídeo a ser investigado, deve-se reconhecer o “ID” sobre o Canal responsável pelo conteúdo. Cada canal possui um identificador único no Youtube, que por sua vez deve ser apresentado junto com o Canal investigado. Atualmente, existem várias ferramentas web para se identificar o “Youtube ID” sobre qualquer Canal no Youtube, onde, aqui, será ilustrada a ferramenta “Find any YouTube Channel ID“, disponível na URL “https://commentpicker.com/youtube-channel-id.php”.

7.2.2 Prova de Materialidade

Capturar e preservar o conteúdo alvo de análise é uma parte essencial da maioria das investigações digitais, e neste sentido, valendo-se da ferramenta Youtube-dl, este signatário procedeu com a Coleta Forense não somente do material em vídeo compartilhado na URL “https/www.youtube.com/watchv=R3xqXtyMxnw”, mas também dos registros de metadados relacionados a postagem na Rede Social Youtube.com. A coleta se deu por meio da Distribuição Linux Kali, e no momento da coleta da evidência digital, foi acrescentada string “–write-info-json”, visto que este parâmetro indica também a captura dos metadados do vídeo em um arquivo “.json”.

- **ID:** "R3xqXtyMxnw";
- **Title:** "EXCLUSIVO! Lucas Sanches é flagrado em esquema de corrupção e desvio de dinheiro público";
- **Channel_url:** “https://www.youtube.com/@DiarioSP”;
- Channel_ID: UCJLZgAoasOr0UBLsiwqjBnA;
- **YouTube handle / custom URL**: "@diariosp";
- **Extractor**: "youtube",
- **Extractor_key**: "Youtube",

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

- **Channel description**: " Canal de vídeos do jornal Diário de São Paulo www.spdiario.com.br".

7.3 Análise Holística

Na condução da análise holística, inserido aos achados periciais acerca do arquivo em vídeo “R3xqXtyMxnw.mp4”, foram extraídos e posteriormente examinados os *frames* que compõem o arquivo em vídeo questionado. Os *frames* do arquivo questionado foram obtidos por meio do *software* ffmpeg, sob a linha de comando “*ffmpeg -i R3xqXtyMxnw.mp4 img%06d.png*”, totalizando um montante em (2409) dois mil quatrocentos e nove arquivos sob a extensão “.png”.

No que compete aos achados de interesse pericial acerca do arquivo em vídeo questionado, lista-se elementos que atestam os indícios de manipulação no arquivo de vídeo, como cortes abruptos, alterações na sequência temporal e inconsistências visuais que comprometem sua integridade original.

O vídeo é iniciado (Frame “img000001.png”) em “tela cheia”, quando é possível identificar os carimbos de marca, data e horário, atribuídos pelo sistema empregado na câmera de monitoramento, conforme destacado na Figura 2.

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

Figura 2 – Frame inicial (img000001.png).

No entanto, em certos momentos, ocorrem interrupções ou saltos na sequência temporal, evidenciando edições ou manipulações no conteúdo original. Na sequência dos eventos demonstrados no vídeo, observa-se que fora intencionalmente aplicado um efeito de *zoom* sobre os eventos que ocorrem no ambiente (Figura 3), o que torna invisível o carimbo de data e hora no canto inferior direito da tela, o que inviabiliza a possibilidade em atestar de forma contínua e sincronizada com a sequência dos eventos ocorridos em cena.

Figura 3 – Frame img000346.png.

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

Ao longo da análise do vídeo, percebe-se que há cortes evidentes na sequência, com transições abruptas entre cenas, indicando a remoção de partes do conteúdo original. Essas interrupções quebram a fluidez natural do vídeo, indicando que ele foi intencionalmente editado ou manipulado, conforme demonstrado através da Figura 4.

Figura 4 – Frame img000550.png.

Adicionalmente, ao observar o vídeo questionado, pode-se atestar que a narrativa em áudio que ilustra os eventos ocorridos em cena, tenta imputar ao SR. LUCAS SANCHES, por ter saído do ambiente e voltando com sacolas de dinheiro, conforme abaixo transcrito:

Início aos 37 segundos: *"Lucas acompanha tudo de perto, saindo e voltando do ambiente com sacolas de dinheiro em espécie, desviados de verbas públicas".*

Todavia, objetivando a descontextualização dos eventos ocorridos em cena, valendo-se da remoção de partes do conteúdo original, por meio de interrupções na continuidade nas imagens capturadas no vídeo original, ao analisar a sequência do vídeo, observa-se uma inconsistência notável que imputa ao SR. LUCAS SANCHES características de duas pessoas diferentes. Em determinado momento, LUCAS SANCHES aparece se deslocando para o exterior da sala (Figura 5), porém o indivíduo

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

que posteriormente adentra ao ambiente segurando uma sacola (Figura 6), possui características fisionômicas distintas a de LUCAS SANCHES, o que sugere que houve uma edição ou manipulação para criar a ilusão de continuidade, utilizando imagens de indivíduos diferentes, mas tentando atribuir a ação a um único personagem. Isso compromete a autenticidade do material e levanta suspeitas sobre sua integridade.

Figura 5 – Frame img001139.png.

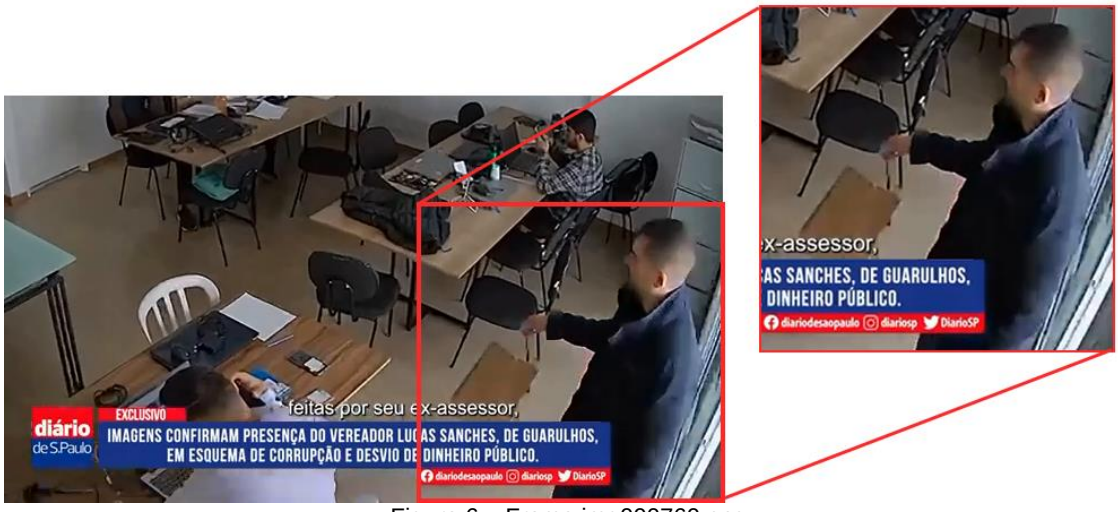

Figura 6 – Frame img000760.png.

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

Por fim, durante a análise do vídeo, constatou-se que o fluxo de áudio foi completamente removido nos trechos de interesse, resultando em uma gravação sem som. Essa ausência de áudio compromete a avaliação completa do conteúdo, dificultando a verificação de possíveis diálogos ou outros elementos sonoros que poderiam fornecer informações relevantes para atestar a veracidade de seu conteúdo.

8 CONCLUSÃO

Como resultado da minuciosa análise referente aos registros de vídeos disponibilizados para o exame, em especial ao arquivo em vídeo “R3xqXtyMxnw.mp4” e obedecendo as melhores práticas em conformidade ao que regula a Norma ABNT NBR ISO/IEC 27037:2013, foram analisados os vários pontos que se apresentam como de interesse ao escopo do presente trabalho pericial.

Neste sentido, restaram demonstradas as evidências de que o registro em vídeo questionado, e de origem desconhecida, fora produzido de maneira fraudulenta, visto que consiste da manipulação, cortes e inserção de elementos estranhos ao contexto original. Tais alterações, além da remoção de áudio, atestam que o vídeo foi editado com o objetivo de distorcer os fatos apresentados, comprometendo sua integridade e autenticidade como prova. Portanto, resta claro que o material em questão não pode ser considerado confiável.

CONSIDERAÇÕES FINAIS

Este trabalho técnico foi elaborado em (21) vinte e uma folhas impressas somente no anverso, (06) seis figuras digitalizadas e (01) uma tabela. A última folha segue assinada utilizando Certificado Digital.

Perito: Vinícius Machado de Oliveira
E-mail: vinicius.oliveira@oliveiraperito.com.br
www.oliveiraperito.com.br

Porto Alegre, 01 de outubro de 2024.

OliveiraPerito
Computação Forense e Perícia Digital

Assinado de forma digital por VINICIUS MACHADO DE OLIVEIRA:80906320097
DN: c=BR, o=ICP-Brasil, ou=VideoConferencia, ou=00250354000194, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=(em branco), cn=VINICIUS MACHADO DE OLIVEIRA:80906320097
Dados: 2024.10.01 19:39:11 -03'00'

Vinícius Machado de Oliveira
Assistente Técnico – Computação Forense Digital