Data Sanitization Evaluation in Donated Computers During the COVID-19 Pandemic: A Case Study at IFSP Hortolândia

Arthur de Oliveira[1], Fernando Sambinelli[2]

[1]Federal Institute of Education, Science and Technology of São Paulo (IFSP)
Hortolândia Campus – SP – Brazil

o.arthur@aluno.ifsp.edu.br, sambinelli@ifsp.edu.br

Resumo. *This study evaluates the effectiveness of data sanitization procedures on IT equipment donated to the Federal Institute of São Paulo (IFSP) Hortolândia campus during the COVID-19 pandemic. Using forensic computing techniques, some donated computers were examined, revealing the presence of sensitive personal data belonging to public servants from the donor agencies. This discovery highlights a significant failure in the data sanitization process conducted by the federal donor agency, emphasizing the urgent need for compliance with Brazilian regulations such as Normative Instruction No. 01/2010 and the General Data Protection Law (LGPD - Lei Geral de Proteção de Dados Pessoais). The study underscores the importance of adopting rigorous data sanitization practices, providing continuous training to staff, and conducting regular audits to ensure the security and privacy of information in public agencies.*

1. Introduction

A substantial volume of confidential, secret, and sensitive information is stored in millions of mass storage devices, such as hard drives. All organizations and individuals using computers will inevitably need to dispose of them at some point due to equipment obsolescence. Many of these organizations or individuals will choose to sell, donate, or trade these computers. However, the problem is that many of these devices have disks in a state where the information contained within can be recovered [Yusof et al. 2019]. Concerns about the risk of leaking sensitive user data are so significant that many data centers worldwide opt to destroy storage devices instead of repurposing or donating them [McManus 2023].

Hard drives provide primary mass storage for operating systems used in computers. These systems protect user data against accidental deletion through various mechanisms, such as moving deleted files to recycling bins or trash folders and providing commands to recover deleted data. Furthermore, even after a user effectively deletes a file, this operation only removes the pointers to the file blocks, links that allow the file system to reference the file. This type of deletion is faster and facilitates subsequent file restoration because the data remains on the disk. However, these files, whose pointers have been removed, are not secure and can be recovered using data recovery techniques such as data carving [Meyer and Roy 2023]. Deleting both the pointers and the file data is an example of a secure disk sanitization technique [Hands and Coughlin 2023].

The importance of disk sanitization is highlighted by various studies and practices in forensic computing. Residual data can be recovered by attackers, compromising the security and privacy of organizations' and individuals' information [Casey 2011][Nelson 2018][Meyer and Roy 2023]. Additionally, proper sanitization promotes the safe reuse of devices, aligning with circular economy practices and sustainability [Hands and Coughlin 2023].

Several international organizations establish rigorous standards for disk sanitization, including the National Institute of Standards and Technology (NIST) in the United States, which issued the Guidelines for Media Sanitization (NIST 800-88) to meet this need. NIST 800-88 defines data sanitization as the set of methods for eradicating data on a disk, including block-by-block overwriting, internal secure disk wiping, and physical, chemical, thermal, or magnetic destruction. Another internationally recognized data sanitization standard is DoD 5220.22-M, established by the United States Department of Defense. Specifically, DoD 5220.22-M is a standard that defines methods and procedures for the secure removal of data from electronic media, such as hard drives, magnetic tapes, and other storage devices.

In the context of the Brazilian Federal Public Administration, Normative Instruction No. 01/2010 (*Instrução Normativa nº 01/2010*) of the Secretariat of Logistics and Information Technology [Governo Federal do Brasil 2010] establishes that IT equipment must undergo a data sanitization process before being donated or discarded. This process is essential to prevent the leakage of sensitive information and ensure compliance with the General Data Protection Law (LGPD - *Lei Geral de Proteção de Dados Pessoais*) [Governo Federal Brasileiro 2018].

During the COVID-19 pandemic, the Federal Institute of São Paulo (IFSP) at the Hortolândia campus received several laptops and computers through donations from other Brazilian federal agencies to help students without adequate resources access remote classes. These devices were formatted and received new Windows operating system installations by the campus's IT team, but they were never used by the students. This case study aimed to evaluate whether the computers donated to the IFSP underwent any data sanitization process at the originating institution.

2. Methodology

To evaluate the effectiveness of data sanitization on the computers received as donations from other federal agencies by the Federal Institute of Education, Science, and Technology of São Paulo (IFSP) during the COVID-19 pandemic, a rigorous forensic computing approach was adopted, adhering to the guidelines established by the ISO/IEC 27037 standard [International Organization for Standardization 2012]. This standard provides guidelines for the identification, collection, acquisition, and preservation of digital evidence, ensuring the integrity and authenticity of information throughout the investigative process.

2.1. Device Selection

Initially, two computers donated to IFSP by different federal agencies were randomly selected to compose the study sample. This selection was made to ensure minimal representativeness while preserving the necessary methodological rigor for an initial exploratory analysis.

2.2. Forensic Image

The forensic image of the hard drives from the computers was conducted using FTK Imager software, version 4.5. This software is widely recognized and utilized in the field of forensic computing due to its ability to create exact forensic images of hard drives, preserving the integrity of the original data [Nikkel 2016]. During this process, strict procedures were followed to ensure the chain of custody and prevent any modification of the original data. Figure 1 illustrates the forensic image creation process for one of the devices.

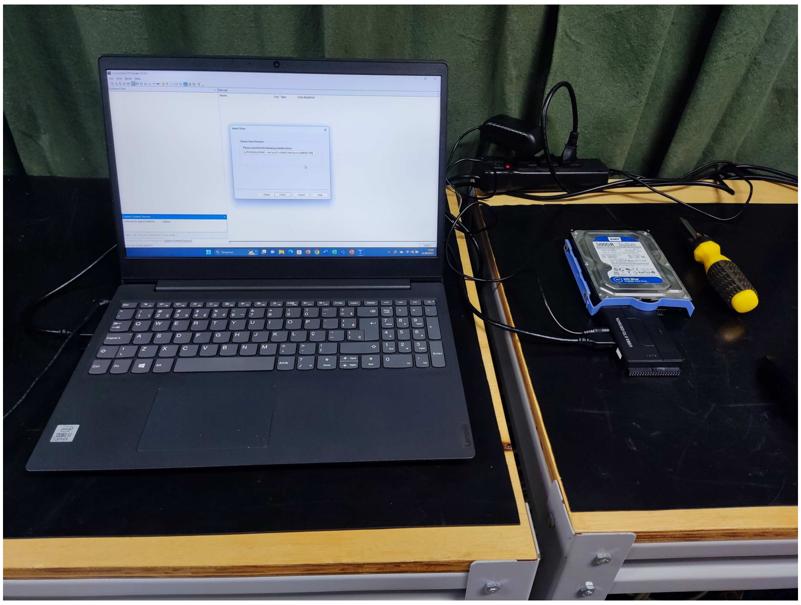


Figure 1. During the Forensic Image Creation Process

The forensic image creation process involved three steps. First, the computer hard drives were connected to a dedicated forensic workstation. Then, the FTK Imager tool was used to create a bit-by-bit image of each hard drive. Finally, the checksums (hashes) generated before and after image creation were verified to ensure no data alteration occurred.

2.3. Data Carving Analysis

After creating the forensic images, they underwent detailed data carving analysis using Autopsy software, version 4.21. Data carving is an advanced data recovery technique that allows the identification and extraction of files and file fragments, even if they are deleted or not referenced by an active file system [Meyer and Roy 2023]. This technique was applied to identify traces of data that could be related to the donor agencies of the equipment and evaluate the effectiveness of the previously performed data sanitization processes.

The data carving analysis was conducted in three phases. First, the forensic images were loaded into the Autopsy software. Then, data carving algorithms were applied to identify possible deleted file fragments. Subsequently, the results were manually inspected to verify the presence of sensitive data, including documents, images, emails, and other types of files that could contain personal or institutional information.

2.4. Verification and Validation Procedures

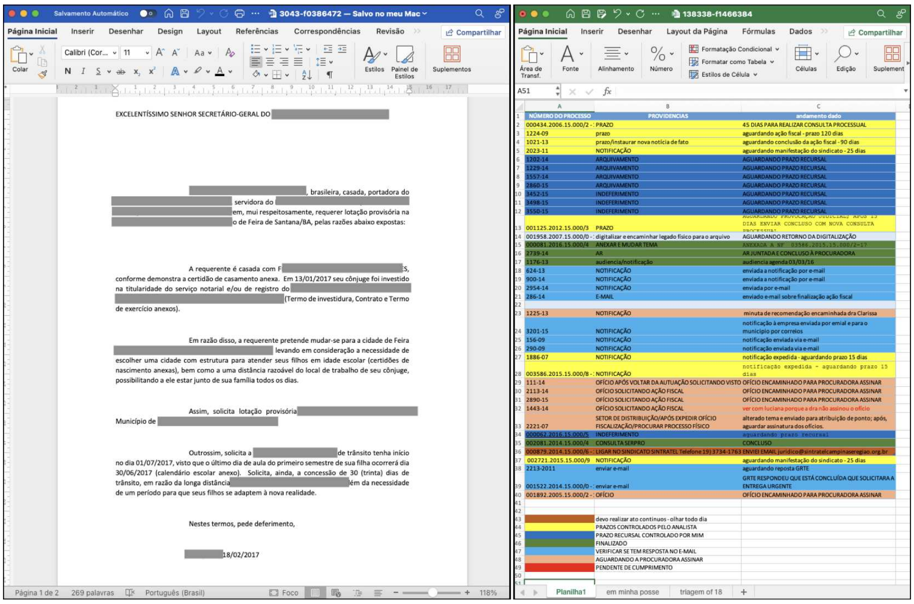
To ensure the accuracy and reliability of the results, additional verification and validation procedures were undertaken. The logs generated during the creation of the forensic images and the data carving analysis were reviewed. Checksums of the recovered files were compared with known checksums, where available, to confirm the integrity of the recovered data. Detailed documentation of the entire process was also compiled, including screenshots and reports generated by the software used.

2.5. Ethical and Legal Considerations

Throughout the process, ethical and legal considerations associated with handling sensitive data were rigorously observed. The research team ensured that all practices complied with current privacy and data protection policies, respecting the rights of the individuals and institutions involved.

3. Results

The forensic analysis revealed the presence of residual data on one of the examined computers. Figure 2 illustrates some of the evidence identified during the inspection. Among the data found were work management documents and drafts of official letters, indicating that the sanitization process was not adequately performed by the donor agency.



EXCELENTÍSSIMO SENHOR SECRETÁRIO-GERAL DO [redacted]

[redacted], brasileira, casada, portadora do [redacted] servidora do [redacted] [redacted]em, mui respeitosamente, requerer lotação provisória na [redacted]o de Feira de Santana/BA, pelas razões abaixo expostas:

A requerente é casada com F[redacted]S, conforme demonstra a certidão de casamento anexa. Em 13/01/2017 seu cônjuge foi investido na titularidade do serviço notarial e/ou de registro do [redacted] [redacted](Termo de investidura, Contrato e Termo de exercício anexos).

Em razão disso, a requerente pretende mudar-se para a cidade de Feira [redacted] levando em consideração a necessidade de escolher uma cidade com estrutura para atender seus filhos em idade escolar (certidões de nascimento anexas), bem como a uma distância razoável do local de trabalho de seu cônjuge, possibilitando a ele estar junto de sua família todos os dias.

Assim, solicita lotação provisória[redacted] Município de [redacted]

Outrossim, solicita a [redacted]de trânsito tenha início no dia 01/07/2017, visto que o último dia de aula do primeiro semestre de sua filha ocorrerá dia 30/06/2017 (calendário escolar anexo). Solicita, ainda, a concessão de 30 (trinta) dias de trânsito, em razão da longa distância[redacted]lém da necessidade de um período para que seus filhos se adaptem à nova realidade.

Nestes termos, pede deferimento,

[redacted]18/02/2017

	A	B	C
1	NÚMERO DO PROCESSO	PROVIDENCIAS	andamento dado
2	000434.2006.15.000/2 - :	PRAZO	45 DIAS PARA REALIZAR CONSULTA PROCESSUAL
3	1224-09	prazo	aguardando ação fiscal - prazo 120 dias
4	1021-13	prazo/instaurar nova notícia de fato	aguardando conclusão da ação fiscal - 90 dias
5	2023-11	NOTIFICAÇÃO	aguardando manifestação do sindicato - 25 dias
6	1202-14	ARQUIVAMENTO	AGUARDANDO PRAZO RECURSAL
7	1229-14	ARQUIVAMENTO	AGUARDANDO PRAZO RECURSAL
8	1557-14	ARQUIVAMENTO	AGUARDANDO PRAZO RECURSAL
9	2860-15	ARQUIVAMENTO	AGUARDANDO PRAZO RECURSAL
10	3452-15	INDEFERIMENTO	AGUARDANDO PRAZO RECURSAL
11	3498-15	INDEFERIMENTO	AGUARDANDO PRAZO RECURSAL
12	3550-15	INDEFERIMENTO	AGUARDANDO PRAZO RECURSAL
13	001125.2012.15.000/3	PRAZO	AGUARDANDO PROVOCAÇÃO JUDICIAL; APÓS 15 DIAS ENVIAR CONCLUSO COM NOVA CONSULTA PROCESSUAL
14	001958.2007.15.000/0 - :	digitalizar e encaminhar legado físico para o arquivo	AGUARDANDO RETORNO DA DIGITALIZAÇÃO
15	000081.2016.15.000/4	ANEXAR E MUDAR TEMA	ANEXADA A NF 03586.2015.15.000/2-17
16	2739-14	AR	AR JUNTADA E CONCLUSO À PROCURADORA
17	1176-13	audiencia/notificação	audiencia agenda 03/03/16
18	624-13	NOTIFICAÇÃO	enviada a notificação por e-mail
19	900-14	NOTIFICAÇÃO	enviada a notificação por e-mail
20	2954-14	NOTIFICAÇÃO	enviada por e-mail
21	286-14	E-MAIL	enviado e-mail sobre finalização ação fiscal
22			
23	1225-13	NOTIFICAÇÃO	minuta de recomendação encaminhada dra Clarissa
24	3201-15	NOTIFICAÇÃO	notificação à empresa enviada por emial e para o municipio por correios
25	156-09	NOTIFICAÇÃO	notificação enviada via e-mail
26	290-09	NOTIFICAÇÃO	notificação enviada via e-mail
27	1886-07	NOTIFICAÇÃO	notificação expedida - aguardando prazo 15 dias
28	003586.2015.15.000/8 - :	NOTIFICAÇÃO	notificação expedida - aguardando prazo 15 dias
29	111-14	OFÍCIO APÓS VOLTAR DA AUTUAÇÃO SOLICITANDO VISTO	OFÍCIO ENCAMINHADO PARA PROCURADORA ASSINAR
30	2113-14	OFÍCIO SOLICITANDO AÇÃO FISCAL	OFÍCIO ENCAMINHADO PARA PROCURADORA ASSINAR
31	2890-15	OFÍCIO SOLICITANDO AÇÃO FISCAL	OFÍCIO ENCAMINHADO PARA PROCURADORA ASSINAR
32	1443-14	OFÍCIO SOLICITANDO AÇÃO FISCAL	ver com luciana porque a dra não assinou o ofício
33	2221-07	SETOR DE DISTRIBUIÇÃO/APÓS EXPEDIR OFÍCIO FISCALIZAÇÃO/PROCURAR PROCESSO FÍSICO	alterado tema e enviado para atribuição de ponto; após, aguardar assinatura dos ofícios.
34	000062.2016.15.000/5	INDEFERIMENTO	aguardando prazo recursal
35	002081.2014.15.000/4	CONSULTA SERPRO	CONCLUSO
36	000879.2014.15.000/6 - :	LIGAR NO SINDICATO SINTRATEL Telefone 19) 3734-1763	ENVIEI EMAIL juridico@sintratelcampinaseregiao.org.br
37	002721.2015.15.000/9	NOTIFICAÇÃO	aguardando manifestação do sindicato - 25 dias
38	2213-2011	enviar e-mail	aguardando reposta GRTE
39	001522.2014.15.000/0 - :	enviar e-mail	GRTE RESPONDEU QUE ESTÁ CONCLUÍDA QUE SOLICITARA A ENTREGA URGENTE
40	001892.2005.15.000/2 - :	OFÍCIO	OFÍCIO ENCAMINHADO PARA PROCURADORA ASSINAR
41			
42			
43	🟫	devo realizar ato continuos - olhar todo dia	
44	🟨	PRAZOS CONTROLADOS PELO ANALISTA	
45	🟦	PRAZO RECURSAL CONTROLADO POR MIM	
46	🟩	FINALIZADO	
47	🟦	VERIFICAR SE TEM RESPOSTA NO E-MAIL	
48	🟧	AGUARDANDO A PROCURADORA ASSINAR	
49	🟥	PENDENTE DE CUMPRIMENTO	
50			

Figure 2. Personal documents recovered from the hard drive

No residual data traces were found in the second computer analysis. This indicates that, for this device, the new Windows image installation, performed as soon as the equipment was received at IFSP, effectively overwrote the personal data of the former user or that the sanitization process was successfully executed, meeting the expected standards of data security and privacy.

4. Conclusion

Data sanitization is an essential component to ensure the security and privacy of information stored on electronic devices, particularly in the context of disposing or donating equipment by federal agencies. The case study conducted at the Federal Institute of Education, Science, and Technology of São Paulo (IFSP) evidenced the failure in the sanitization process of one of the analyzed computers, resulting in the exposure of sensitive data, including work management documents and drafts of official letters.

These findings underline the critical importance of adhering to specific regulations, such as Normative Instruction No. 01/2010, and the LGPD, which aim to protect the personal data of public servants. Non-compliance with these standards not only compromises information security but can also lead to severe legal and institutional consequences. The study emphasizes the need to implement rigorous data sanitization techniques, in accordance with international standards and best practices in digital forensics [Meyer and Roy 2023].

Furthermore, it is imperative to conduct regular audits and provide continuous training to the teams responsible for data sanitization. These steps are fundamental to ensure that proper practices are consistently followed, minimizing the risk of exposing sensitive data and ensuring compliance with existing legislation.

References

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.

Governo Federal Brasileiro (2018). Lei geral de proteção de dados pessoais (LGPD). Presidência da República.

Governo Federal do Brasil (2010). Instrução normativa nº 01, de 17 de janeiro de 2010. Ministério do Planejamento, Orçamento e Gestão.

Hands, J. and Coughlin, T. (2023). New IEEE media sanitization specification enables circular economy for storage. *Computer*, 56(1):111–116.

International Organization for Standardization (2012). ISO/IEC 27037:2012 - Guidelines for identification, collection, acquisition, and preservation of digital evidence. IEC.

McManus, S. (2023). Why millions of usable hard drives are being destroyed. `https://www.bbc.com/news/business-65669537`. August.

Meyer, A. and Roy, S. (2023). *Evaluating Deleted File Recovery Tools per NIST Guidelines: Results and Critique*, chapter Chapter 2, pages 13–49.

Nelson, B. (2018). *Guide to Computer Forensics and Investigations*. Cengage Learning.

Nikkel, B. (2016). *Practical Forensic Imaging*. No Starch Press.

Yusof, N. A. B., Abdullah, S. N. H. B. S., bin Md Senan, M. F. E., binti Zainal Abidin, N. Z., and Sahri, M. B. (2019). Data sanitization framework for computer hard disk drive: A case study in malaysia. *International Journal of Advanced Computer Science and Applications*, 10(11).