SCIENTIA PLENA
www.scientiaplena.org.br
VOL. 18, NUM. 8 2022
doi: 10.14808/sci.plena.2022.084815

Análise forense do smartwatch Samsung Galaxy Watch Active 2

Forensic analysis of Samsung Galaxy Watch Active 2 smartwatch

I. J. M. Fonseca[1]*; R. F. Zampolo[1,2]

[1]*Programa de Pós-Graduação em Ciências Forenses/Universidade do Sul e Sudeste do Pará, 68505-080, Marabá-PA, Brasil*
[2]*Faculdade de Eng. da Computação e Telecomunicações/Laboratório de Processamento de Sinais/Instituto de Tecnologia/Universidade Federal do Pará, 66075-110, Belém-PA, Brasil*

**idelvandroe@unifesspa.edu.br*
(Recebido em 05 de dezembro de 2021; aceito em 02 de julho de 2022)

A Internet das Coisas (*Internet of Things - IoT*) é um paradigma bem conhecido que define um ambiente dinâmico e inter-relacionado de dispositivos de computação com diferentes componentes para uma conectividade perfeita e transferência de dados. O campo da tecnologia vestível é um dos mais populares nos dias de hoje e prevê-se que continue em expansão devido a demandas crescentes. Coletar dados para análise forense digital em IoT é um desafio, pois os dispositivos não são criados com essa preocupação, resultando em pouca ou nenhuma padronização dos dados e grande dispersão de informações no ecossistema da Internet das Coisas. Além disso, há atualmente poucos softwares capazes de apoiar o perito criminal nesse tipo de situação. Este trabalho reúne ferramentas e procedimentos para análise de evidências forenses em *smartwatches*, mais especificamente no Samsung *Galaxy Watch Active* 2. Na parte experimental, procedeu-se à extração de dados sem o acesso de superusuário (root) do sistema. Ferramentas do fabricante do dispositivo foram utilizadas na conexão e extração de arquivos, e software de código aberto na análise subsequente. Mesmo sem o acesso de superusuário, foi possível recuperar informações relevantes para investigações forenses: lista de contatos e registros de chamada são algumas das evidências restauradas.
Palavras-chave: Internet das coisas, *smartwatches*, análise forense.

The Internet of Things (IoT) is a well-known paradigm that defines a dynamic and interrelated environment of database devices with different components for seamless connectivity and data transfer. The field of wearable technology is one of the most popular fields today and is expected to continue to grow due to increasing demands. Collecting data for digital forensic analysis in IoT is a challenge, as the devices are not created with this concern, which yields little or no standardization of data and great dispersion of information in the Internet of Things ecosystem. Furthermore, there are few softwares capable of supporting the criminal expert in this type of situation. This work addresses tools and procedures for analyzing forensic evidence in smartwatches, more specifically the Samsung Galaxy Watch Active 2. In the experimental part, data extraction was carried out without superuser access to the system. Device manufacturer tools were used for connecting and extracting files, and open source software for further analysis. Even without superuser access, it was possible to retrieve information relevant to forensic investigations: contact list, and call logs are some of the recovered evidence.
Keywords: Internet of things, smartwatches, forensic analysis.

1. INTRODUÇÃO

As tecnologias digitais estão transformando a maneira como vivemos. Exemplos relevantes no âmbito deste trabalho são a inteligência artificial, computação em nuvem, e a internet das coisas (IoT, do inglês *internet of things*) [1]. Os sistemas IoT mostram-se mais vulneráveis a invasores, principalmente devido ao fato de que, ao construir um dispositivo IoT, os fabricantes costumam dar grande ênfase ao custo, tamanho e usabilidade, enquanto os aspectos de segurança e uso forense tendem a ser negligenciados [2].

A Internet das Coisas é um paradigma que define um ambiente dinâmico e inter-relacionado de dispositivos de computação com diferentes componentes para uma conectividade perfeita e transferência de dados. Alguns exemplos típicos de objetos IoT incluem dispositivos vestíveis (como relógios e óculos inteligentes); sistemas de monitoramento de saúde; fechaduras

residenciais eletrônicas; sensores de temperatura, gás ou luz ambiente; veículos inteligentes; drones e dispositivos industriais de automação e logística [2].

Coletar dados para análise forense digital em IoT é um desafio: os dispositivos não são criados com essa preocupação; há pouca ou nenhuma padronização no formato de dados; é grande a dispersão de informações no ecossistema da Internet das Coisas; e há baixa variedade de softwares com capacidade para apoiar o trabalho do perito forense nesse tipo de situação. Para Li et al. (2019) [3], as ferramentas/métodos de extração de dados podem ser classificados em cinco níveis: manual, lógico, hex *dumping*/JTAG, *chip-off* e micro-leitura. Para dispositivos IoT que não são suportados por ferramentas forenses existentes, principalmente, deve-se considerar a cooperação do proprietário do dispositivo ou do provedor de serviços no processo de análise do material apreendido.

A forense digital pode ser definida como o estudo de evidências geradas em dispositivos digitais relacionados a crimes. Atualmente, tais dispositivos não se restringem apenas ao computador. Os procedimentos padrão para que uma operação pericial seja bem sucedida e, portanto, aceitável em âmbito jurídico, devem envolver a definição de quais os dispositivos digitais relacionados ao crime (eletrodomésticos, automóveis, leitores de *tags*, nós sensores, implantes médicos, dispositivos vestíveis e uma infinidade de outros equipamentos inteligentes), coleta de provas digitais de forma comprovável, análise e preservação de evidência, e relato sistematizado e claro da evidência [4].

Segundo Dias (2019) [5], a IoT, por fornecer potencialmente uma fonte de evidências mais rica que dispositivos eletrônicos não conectados, trouxe novos fatores que afetaram o ambiente de investigação, especialmente na forma como se interage com os dados. Os principais desafios enfrentados pela perícia forense em IoT são:

a **Dados distribuídos**. Os dados são distribuídos em muitos locais, em sua maioria fora do controle do usuário, podendo estar em um *smartphone*, na nuvem ou em *sites* de terceiros.

b **Tempo de permanência da informação**. Devido a limitações de memória, o tempo de armazenamento nos dispositivos é curto; os dados são sobrescritos com facilidade e com frequência.

c **Segurança dos dispositivos**. Evidências em dispositivos IoT podem ser alteradas ou excluídas devido à falta de mecanismos de segurança, podendo comprometer a qualidade da prova e até mesmo anulá-la em um tribunal. Falta de atualização nos dispositivos, em geral, resultam em vulnerabilidades que podem ser exploradas por *hackers*.

d **Variedade de tipos de dispositivos**. Identificar todos os dispositivos IoT relevantes na cena de um crime é difícil: muitos são pequenos, potencialmente inúteis para elucidar eventos de interesse ou podem estar simplesmente desligados. Além disso, extrair evidências desses dispositivos é complexo devido à diversidade de fornecedores, plataformas, sistemas operacionais e hardware.

e **Formatos de dados**. Os formatos dos dados gerados pelos dispositivos não correspondem normalmente aos formatos dos dados salvos na nuvem. Além disso, os dados podem ser processados em diferentes locais antes do armazenamento.

Identificar, coletar, interpretar e apresentar os dados de dispositivos distintos pode ser difícil, especialmente quando tais dados são combinados ou mesclados, pois, nesse caso, sua relevância para uma investigação pode ser ainda maior que se considerados isoladamente [6].

Durante esta pesquisa não foram encontrados trabalhos, documentos ou patentes que padronizem ou apresentem metodologia para tratar crimes digitais em dispositivos vestíveis. Na computação forense, são definidas etapas para a realização de uma perícia que são identificação, preservação, análise e apresentação [5].

Para Austen (2015) [7], os principais dispositivos vestíveis são os rastreadores *fitness* e os *smartwatches*, que monitoram a saúde e dão acesso a alguns serviços online, e que em um curto intervalo de tempo pode haver mais de meio bilhão de dispositivos conectados.

Smartwatches estão superando, em preferência junto ao consumidor, produtos vestíveis outrora de grande popularidade, como rastreadores *fitness*, cuja função principal agora é apenas

um dos recursos disponíveis de um *smartwatch*. Em sua matéria para a empresa de pesquisa CCS Insight, Jijiashvili (2018) [8] diz que as vendas de rastreadores *fitness* caíram 23% em 2017, em contraste com as vendas de *smartwatches* que dispararam. Outro instituto de pesquisa, o Statista, observa que o número de vendas de *smartwatches* aumenta a cada ano, mais do que dobrando desde 2014 até recentemente.

Foi mostrado que dados como mensagens, informações de saúde e condicionamento físico, e-mails, contatos, eventos e notificações são acessíveis a partir de *smartwatches*, cujo valor forense é, portanto, digno de investigação [9]. Sunardi et al. (2021) [10] afirmam que os *smartwatches* são equipados com recursos semelhantes aos dos *smartphones*, como aplicativos de mensagens instantâneas e redes sociais. Embora seja uma facilidade para o usuário, os aplicativos trazem também novas oportunidades para criminosos no ambiente virtual.

A perícia forense digital mostrou-se crucial na investigação de um caso envolvendo uma estudante de medicina de 19 anos, Maria Ladenburger, assassinada em outubro de 2016 na Alemanha. O aplicativo de dados de saúde no iPhone do suspeito foi usado para correlacionar evidências do caso com registros de períodos e intensidades de atividade física [11].

O uso disseminado de *smartwatches* apresenta uma gama de novos desafios aos peritos forenses, já que o crescimento do uso de dispositivos vestíveis se traduz em sua maior presença em casos civis e criminais. Os departamentos de polícia estão descobrindo, por exemplo, que vítimas, suspeitos e testemunhas tendem a possuir em torno de três dispositivos inteligentes cada, levando a uma maior quantidade de dados pessoais sendo criados, modificados e acessados. Ou seja, mais fontes de evidências a serem analisadas [9].

Os estudos forenses sobre dispositivos vestíveis concentram-se, em grande parte, na análise de *smartwatches*. Para que a coleta de evidências seja possível, são necessários, além do *smartwatch* sob análise, um *smartphone*, um computador e acesso a um serviço de nuvem, nos casos em que se tem acesso às credenciais do investigado a este tipo de ambiente. Kits de desenvolvimento de software (do inglês *software development kit*, SDK) ou interfaces de programação de aplicações (do inglês *application programming interface*, API) fornecidos pelo fabricante do *smartwatch* também são usados [11]. Ainda em Kang et al. (2020) [12], é dito que a pulseira inteligente Fitbit pode ter seus dados acessados na nuvem, e extraídos por meio de API Web disponibilizada, mediante conhecimento das credenciais da conta do usuário.

Este trabalho detalha ferramentas e procedimentos para a extração de dados sem a necessidade de acesso físico (*chip off*) ou de superusuário (root) ao sistema operacional em dispositivos vestíveis, especificamente *smartwatches*. Este artigo demonstra que é viável a aquisição de dados de valor forense em *smartwatches* com o uso de *software* gratuito.

2. MATERIAL E MÉTODOS

O trabalho concentra-se na apresentação de procedimentos para extração de possíveis evidências forenses de dispositivos vestíveis (*wearables*), mais especificamente relógios inteligentes (*smartwatches*). Pretende-se demonstrar que, mesmo de maneira isolada, sem análise do aparelho telefônico ao qual está pareado e sem acesso *root* ao sistema, é possível encontrar evidências relevantes para uma investigação.

Para a prova de conceito, foram utilizados um relógio Samsung *Watch Active* 2, um *notebook*, e os *softwares* SDB (*Smart Development Bridge*), *Tizem Studio* e *Autopsy* (Tabela 1). O dispositivo da Samsung foi escolhido devido a dois fatores: primeiro, a marca esteve entre as cinco principais empresas de dispositivos vestíveis por volume de remessa, no quarto trimestre de 2020, segundo o IDC (Figura 1); o segundo fator foi a disponibilidade de um *smartwatch* do referido modelo.

Tabela 1: Recursos utilizados para conexão, extração e análise dos dados.

Ferramentas	Funcionalidades
Notebook - 8 Gb de RAM, SSD 250 Gb, Core i7	Instalação e execução das ferramentas de análise forense e conexão com o *smartwatch*.
Roteador sem fio	Realizar ponte para a conexão entre o *smartwatch* e o *notebook*.
Samsung *Galaxy Watch Active* 2	Dispositivo usado no experimento.
Tizen Studio	É um conjunto abrangente de ferramentas para o desenvolvimento de aplicativos nativos e da Web do *Tizen*.
Smart Development Bridge (SDB)	Ferramenta de gerenciamento de dispositivos incluída no *Tizen* SDK
Autopsy	*Software* de código aberto, utilizado para análise dos arquivos.

Company	4Q20 Shipments	4Q20 Market Share	4Q19 Shipments	4Q19 Market Share	Year-Over-Year Growth
1. Apple	55.6	36.2%	43.7	36.2%	27.2%
2. Xiaomi	13.5	8.8%	12.8	10.6%	5.0%
3. Samsung	13.0	8.5%	10.8	9.0%	20.5%
4. Huawei	10.2	6.7%	9.5	7.9%	7.6%
5. BoAt	5.4	3.5%	0.9	0.8%	470.1%
Others	55.8	36.4%	42.9	35.6%	30.0%
Total	**153.5**	**100.0%**	**120.7**	**100.0%**	**27.2%**

Figura 1: Cinco principais empresas de dispositivos vestíveis por volume de remessa. Fonte: https://www.idc.com/getdoc.jsp?containerId=prUS47534

O Samsung *Galaxy Watch Active* 2 possui memória de armazenamento de 4 GB, RAM de 1,5 GB, *chipset* Exynos 9110 (10 nm), CPU Dual-core 1,15 GHz Cortex-A53 e sistema operacional *Tizen* OS. O modelo testado é o SM-R820 com a versão 5.5.0.2 do *Tizen* OS.

2.1 Extração de dados

O *Tizen* OS se assemelha a uma distribuição Linux comum: tem o sistema de janela X11 e inclui muitas ferramentas e utilitários de sistema, como cliente de *shell* seguro e *daemon*, cópia segura, *bash*, e gerenciador de pacotes. A estrutura nativa é composta de serviços de sistema e um conjunto de bibliotecas para o desenvolvimento de aplicativos nativos em C ++. Como recurso de segurança, é implementado o uso de *sandbox* por MAC (*media access control*) em nível de *kernel*; e as permissões para aplicativos são semelhantes às encontradas no SO Android, onde o arquivo indica o recurso que o aplicativo tenta acessar [13]. A arquitetura do *Tizen* é apresentada na Figura 2.

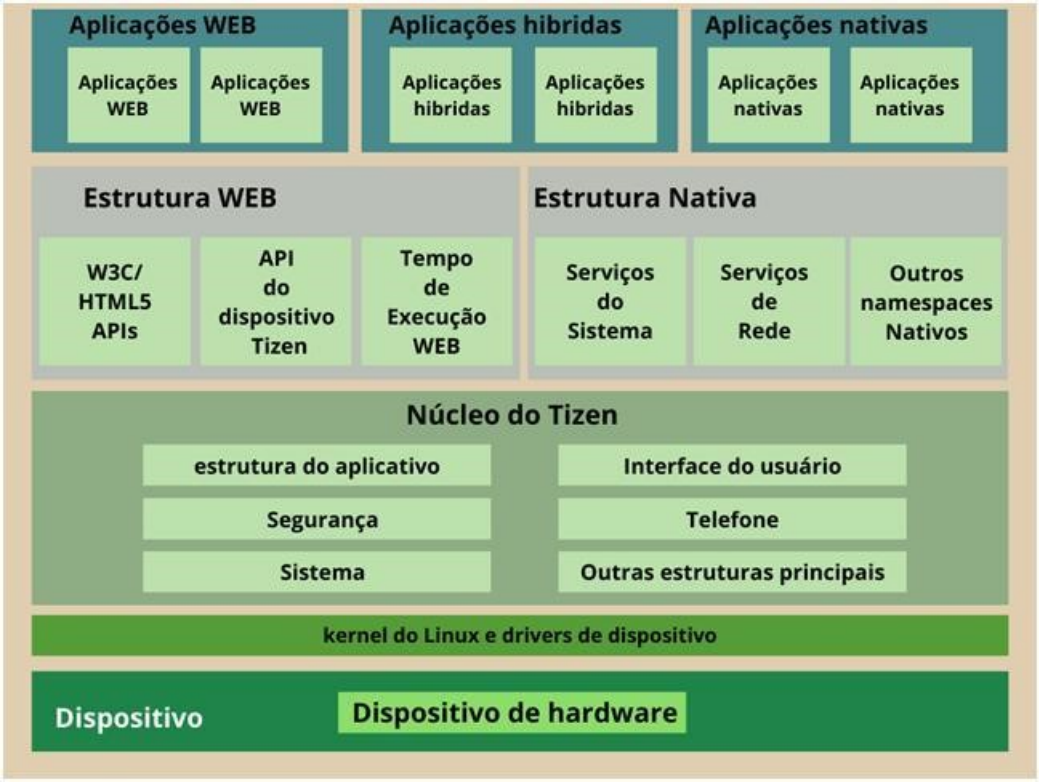

Figura 2: Arquitetura sistema operacional Tizen. Fonte: Baseado em Gadyatskaya et al. (2014) [13].

Ao acessar o dispositivo, identificou-se que o sistema de arquivos do *Tizen* é o sistema de arquivos Ext4. Embora o *kernel* possa ser compilado para suportar outros sistemas de arquivos como JFS, XFS, BTRFS e Reiserfs. Para uma cópia do sistema de forma fidedigna, ou imagem de disco, deve-se indicar a partição /dev do *Tizen*. Normalmente, no sistema Linux, a partição do disco está em /dev/sda, no caso do Samsung a partição está em /dev/mmcblk0p (Figura 3).

```
drwxr-xr-x 2 root root 440 Oct  7 01:51 .
drwxr-xr-x 8 root root 160 Oct  7 01:51 ..
l????????? ? ?    ?      ?            ? afpc
l????????? ? ?    ?      ?            ? boot
l????????? ? ?    ?      ?            ? cm
lrwxrwxrwx 1 root root  15 Oct  7 01:52 csa -> ../../mmcblk0p1
l????????? ? ?    ?      ?            ? csc
l????????? ? ?    ?      ?            ? module
l????????? ? ?    ?      ?            ? nad_fw
l????????? ? ?    ?      ?            ? nad_refer
l????????? ? ?    ?      ?            ? param
l????????? ? ?    ?      ?            ? ramdisk1
l????????? ? ?    ?      ?            ? ramdisk2
l????????? ? ?    ?      ?            ? recovery
l????????? ? ?    ?      ?            ? rootfs
l????????? ? ?    ?      ?            ? smsn
l????????? ? ?    ?      ?            ? steady
l????????? ? ?    ?      ?            ? system-data
l????????? ? ?    ?      ?            ? tup
l????????? ? ?    ?      ?            ? tyd
l????????? ? ?    ?      ?            ? up_param
lrwxrwxrwx 1 root root  16 Oct  7 01:52 user -> ../../mmcblk0p18
sh-3.2$
```

Figura 3: Discos lógicos encontrados no dispositivo analisado.

Para extrair os dados do dispositivo, foi executada sequência de passos indicada no site do fabricante do relógio (Figura 4) que consiste em:

- Conectar o PC host ao ponto de acesso *wireless* via cabo UTP ou Wi-Fi;
- No *smartwatch*, ativar o Wi-Fi;

- Ativar o modo de depuração;
- Conectar o relógio na mesma rede que o *host*;
- Depois de conectado, encontrar o endereço IP que o dispositivo *Galaxy Watch* recebeu do ponto de acesso via DHCP. Este endereço IP será usado durante a conexão SDB.

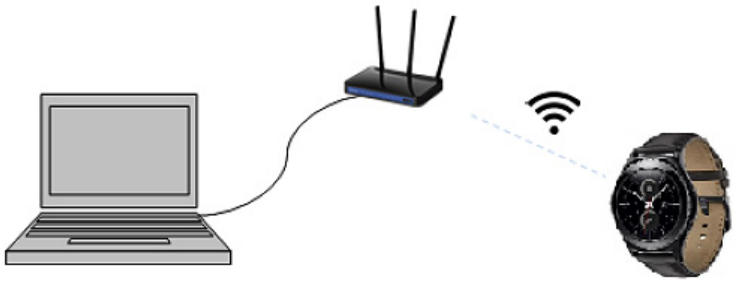

Figura 4: Conectando computador e smartwach Active 2. Fonte: https://developer.samsung.com/galaxy-watch-tizen/testing-your-app-on-galaxy-watch.html

Com o intuito de proteger a integridade dos dados, a rede sem fio utilizada não tinha acesso à internet e foi garantido que o modo avião do dispositivo estivesse ligado, evitando qualquer interferência da rede Bluetooth e NFC (*Near-Field Communication*, ou Comunicação por campo de proximidade (CCP)). Apenas o Wi-Fi foi habilitado para fins de comunicação, já que o dispositivo não fornece portas de conexão física para carregamento ou extração de quaisquer dados do usuário. As medidas foram tomadas de acordo com os procedimentos descritos no "Procedimento Operacional Padrão (POP): Perícia Criminal" [14] e adaptados para o uso de *smartwatches*, já que o documento é de 2013 e seu foco eram aparelhos celulares.

Para a extração dos dados, foram utilizadas as ferramentas *Tizen Studio* e SDB (a primeira fornece os *drivers* para que a conexão via SDB funcione). O *smartwatch* foi conectado usando o IP atribuído e a porta 26101 por meio dos comandos SDB. Conforme mostrado na Figura 5, a porta 26101 é padrão para conexão com este dispositivo. Para usar o SDB, é necessário iniciar o servidor SDB e, em seguida, utilizar o comando <sdb connect EndereçoIP:26101>. Após isso, é aberto um terminal para o dispositivo, e ainda podem-se listar os dispositivos conectados com o comando <sdb devices>.

```
C:\tizen-studio\tools>sdb.exe start-server
* Server is not running. Start it now on port 26099 *
* Server has started successfully *

C:\tizen-studio\tools>sdb.exe connect 192.168.0.103
connecting to 192.168.0.103:26101 ...
device unauthorized. Please approve on your device.

C:\tizen-studio\tools>sdb.exe connect 192.168.0.103
192.168.0.103:26101 is already connected

C:\tizen-studio\tools>sdb.exe devices
List of devices attached
192.168.0.103:26101     device          SM-R820

C:\tizen-studio\tools>
```

Figura 5: Sequência para ter acesso via linha de comando ao Samsung Galaxy Active 2.

Por se tratar de um sistema baseado no sistema operacional Linux, após a conexão estabelecida, o comando <sdb shell> foi executado para que um terminal interativo fosse aberto. Já que a maioria dos comandos Linux funciona no dispositivo, foi possível identificar algumas

pastas e caminhos importantes de arquivos e discos dentro do sistema. A Figura 6 mostra a lista de diretórios do usuário e suas permissões.

```
C:\tizen-studio\tools>sdb.exe shell
sh-3.2$ ls -al
total 52
drwxr-x---  11 owner system_share       4096 Jan  3  2020 .
drwxr-xr-x   5 root  root               4096 Jan  3  2020 ..
drwxr-x---   6 owner system_share       4096 Jan  3  2020 .applications
drwxrwxr-x   6 owner users              4096 Jan  6  2021 .cache
drwxrwxr-x   4 owner users              4096 Aug 24  2020 .config
drwxr-xr-x   2 owner users              4096 Jan  3  2020 .dotnet
drwxr-xr-x   3 owner users              4096 Jan  3  2020 .pki
drwxr-x--- 166 owner system_share      12288 Jan 22  2021 apps_rw
drwxrwxr-x   7 owner users              4096 Aug 24  2020 data
drwxrwsrwx  12 root  priv_mediastorage  4096 Jan  6  2021 media
drwxrwxr-x   7 owner users              4096 Aug 24  2020 share
sh-3.2$
```

Figura 6: Arquivos de usuários e suas permissões.

Além dos arquivos dos usuários foi possível reconhecer pastas, arquivos ocultos, e dispositivos de armazenamento. No caminho <dev/disk/by-partlabel/> encontram-se as partições e pastas com arquivos do usuário, mas não há possibilidade de acesso ou cópia sem acesso root ao sistema, como mostra a Figura 7.

```
sh-3.2$ cd /dev/disk/by-partlabel/
afpc         cm           csc          nad_fw       param        ramdisk2     rootfs       steady       tup          up_param
boot         csa          module       nad_refer    ramdisk1     recovery     smsn         system-data  tyd          user
sh-3.2$ cd /dev/disk/by-partlabel/
sh-3.2$ ls -al
ls: cannot access ramdisk1: Permission denied
ls: cannot access tup: Permission denied
ls: cannot access ramdisk2: Permission denied
ls: cannot access param: Permission denied
ls: cannot access nad_refer: Permission denied
ls: cannot access rootfs: Permission denied
ls: cannot access tyd: Permission denied
ls: cannot access smsn: Permission denied
ls: cannot access module: Permission denied
ls: cannot access csc: Permission denied
ls: cannot access steady: Permission denied
ls: cannot access boot: Permission denied
ls: cannot access system-data: Permission denied
ls: cannot access nad_fw: Permission denied
ls: cannot access cm: Permission denied
ls: cannot access afpc: Permission denied
ls: cannot access up_param: Permission denied
ls: cannot access recovery: Permission denied
total 0
```

Figura 7: Arquivos, pastas e partições do usuário, mas apenas com acesso para usuários root.

Também não foi possível fazer uma imagem do dispositivo, pois isso também exigiria acesso de root. Apesar disso, muitos arquivos puderam ser copiados, através do comando <sdb -s EndereçoIP:26101 pull /opt/usr/home/owner location/on/pc/nomepasta>.

3. RESULTADOS E DISCUSSÃO

3.1 Artigos Relacionados

Os relógios inteligentes têm sido submetidos a poucos estudos forenses por terem pouco tempo de uso massivo. No entanto, já é grande o número de trabalhos sobre análise forense realizadas em diversos dispositivos digitais, variando desde filmadoras digitais, até consoles de videogame. Outros estudos concentraram sua atenção em sistemas operacionais específicos, principalmente nos dois mais populares em dispositivos móveis: iOS e Android [15].

No que diz respeito à análise forense em *smartwatches*, os trabalhos de pesquisa publicados atualmente concentram-se em aparelhos representativos do atual estado tecnológico, tais como o *Apple Watch* ou o Samsung *Gear*, e na avaliação de artefatos que podem ser encontrados em seus sistemas (*watchOS* e Android, respectivamente). Esses estudos apresentam análise dos arquivos encontrados nos relógios inteligentes, além do processo de aquisição em si [9].

Em Kim et al. (2022) [16], a extração de dados foi realizada no dispositivo Apple Watch série 5, e teve apenas alguns dados sendo extraídos por meio de técnicas forenses de acesso direto. Portanto, para este dispositivo, foram utilizadas técnicas forenses indiretas para a extração dos dados armazenados no *smartphone* que estava emparelhado com o *smartwatch*. Para a obtenção dos dados armazenados no telefone, são necessários privilégios de administrador do sistema.

O modelo Amazfit Stratos 3 pode ser conectado a um PC usando um cabo USB de carregamento fornecido pelo fabricante. Como o Amazfit tem seu sistema operacional baseado no Android, é compatível com o ADB (Android Debug Bridge). Além disso, a estrutura de diretórios, os nomes dos arquivos, etc., podem ser obtidos sem privilégios de administrador. No entanto, podem ocorrer problemas de permissão, devido a aquisição de dados ser restrita [17].

Apesar de haver alguns trabalhos mostrando aquisição e análise dos dados de dispositivos vestíveis do tipo *smartwatch*, não foram identificadas nesta pesquisa técnicas que destacam a extração de dados exclusivamente *standalone* deste tipo de dispositivo, que é o cerne do procedimento usado neste trabalho.

3.2 Análise dos Resultados

Mesmo sem privilégio de root, foi possível ter acesso à lista de contatos, ao registro de chamadas, às atividades gravadas em aplicativos de monitoramento de atividades físicas (neste caso em específico, via aplicativo strava (www.strava.com)), a lembretes, fotos de alguns contatos, além de dados referentes às bandeiras e nome dos cartões de crédito usados pelo usuário. A obtenção dessas informações foi realizada pelo *software Autopsy* (Figuras 8 a 13).

Informações sobre contatos foram encontradas em um arquivo do tipo .db, comumente encontrado em aplicações que utilizam SQLite. O arquivo .contacts-csv.db, localizado na pasta /.applications/dbspace/privacy, permite acesso a toda lista de contatos salva no telefone (tabela *contacts*), mesmo se esta tiver sido apagada do aparelho telefônico. Também é possível verificar data (dia, mês e ano) e horário (hora, minuto e segundo) em que ligações foram recebidas (tabela *phonelogs*), além do número e nome de quem fez a ligação, podendo-se criar uma linha do tempo desse tipo de evento (Figura 8).

Table phonelogs 500 entries Page 1 of 6 Export to CSV

id	number	minmatch	sim_id	log_type	data2	formatted_address	log_time_msec	call_start_time_msec
4787	09198[redacted]	1777025	1	1	00Vitor[redacted]	091 98177-[redacted]5	2021/10/21 20:09:40	2021/10/21 20:09:18
4722	09399[redacted]	2235236	1	2	00Manuella[redacted]	093 99223-[redacted]6	2021/10/15 16:16:56	2021/10/15 16:15:01
4730	09399[redacted]	2235236	1	2	00Manuella[redacted]	093 99223-[redacted]6	2021/10/17 19:03:53	2021/10/17 19:03:02
4712	09399[redacted]	2136869	1	2	00Locay Aluguel de Carros	093 99213-[redacted]9	2021/10/15 13:59:34	2021/10/15 13:58:45
4726	09399[redacted]	2136869	1	2	00Locay Aluguel de Carros	093 99213-[redacted]9	2021/10/15 16:45:51	2021/10/15 16:44:53
4715	08009[redacted]	9792020	1	2	00Localiza Aluguel de Carros	0800 979 2[redacted]	2021/10/15 14:07:14	2021/10/15 14:03:11
4714	09399[redacted]	2338595	1	2	00Brasil Aluguel de Veículos	093 99233-[redacted]5	2021/10/15 14:01:37	2021/10/15 14:01:37
4711	09433[redacted]	3247422	1	2	00Azul Cargo Express	094 3324-[redacted]	2021/10/15 10:11:24	2021/10/15 10:11:24
4694	09498[redacted]	1986438	1	1	00Am[redacted]	094 98198-[redacted]8	2021/10/11 15:30:24	2021/10/11 15:29:32
4708	09498[redacted]	1986438	1	1	00Am[redacted]	094 98198-[redacted]8	2021/10/14 18:07:53	2021/10/14 18:07:37
4709	09498[redacted]	1986438	1	1	00Am[redacted]	094 98198-[redacted]8	2021/10/14 18:25:46	2021/10/14 18:25:38
4727	09498[redacted]	1986438	1	1	00Am[redacted]	094 98198-[redacted]8	2021/10/16 15:57:07	2021/10/16 15:56:19
4728	09498[redacted]	1986438	1	2	00Am[redacted]	094 98198-[redacted]8	2021/10/16 16:13:05	2021/10/16 16:13:00
4729	09498[redacted]	1986438	1	2	00Am[redacted]	094 98198-[redacted]8	2021/10/17 15:51:39	2021/10/17 15:51:31

Figura 8: Registros de chamadas e linha do tempo.

Na pasta /apps_rw/com.samsung.samsung-pay-app/data/.pref foi possível localizar um arquivo de texto que contém informações do nome, bandeira e dos quatro últimos números do cartão de crédito utilizado no relógio (Figura 9). Para constituir prova, este arquivo deve ser

melhor analisado e combinado com outros artefatos, visto que não foi encontrado um registro de compras, apenas informações básicas do cartão. Também foram encontrados arquivos do tipo SQLite para os lembretes criados com o assistente de voz: o arquivo .reminder.db, localizado na pasta /apps_rw/com.samsung.w-reminder/data, tabela *reminderInstance* (Figura 10).

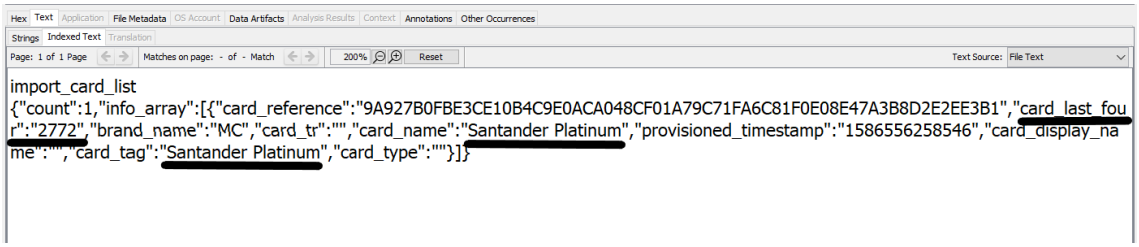

Figura 9: Nome, bandeira e quatro últimos números do cartão de crédito adicionados no aplicativo de pagamento.

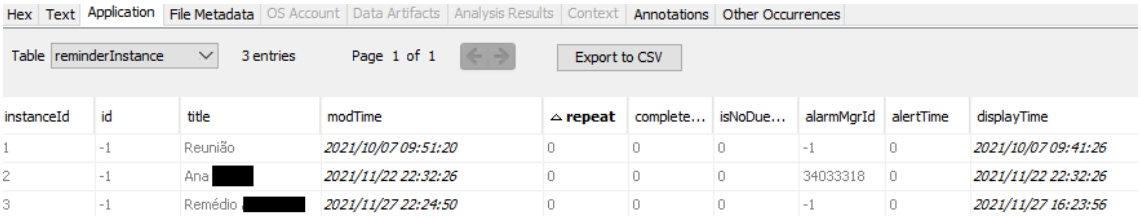

Figura 10: Lembretes criados usando o assistente de voz.

Na Figura 11, são apresentados os treinos gravados (registro de atividades físicas) pelo aplicativo Strava, instalado no *smartwatch.* O arquivo do tipo SQLite strava_database.db contém uma tabela que apresenta o histórico de todos os treinos salvos no aplicativo, na qual é possível identificar o tipo de atividade, a data, tempo de duração da atividade e a distância (em quilômetros) percorrida.

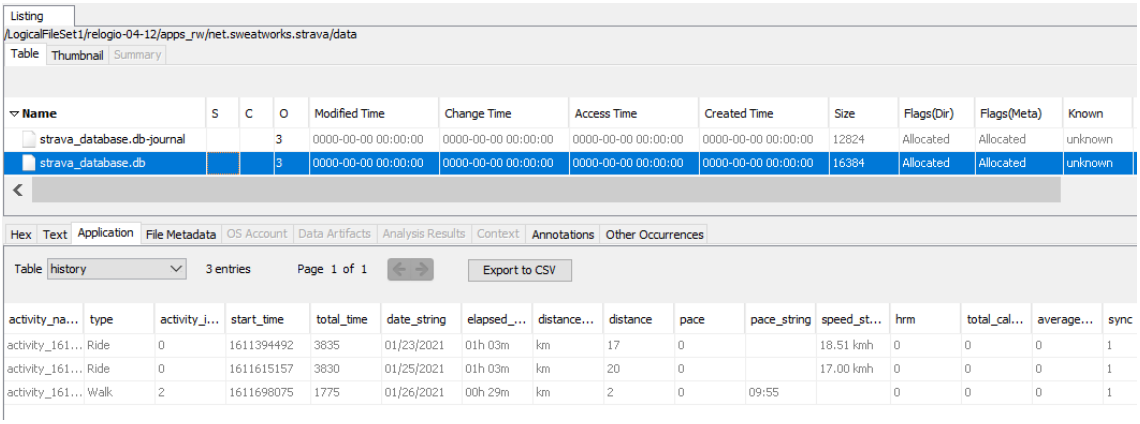

Figura 11: Atividades gravadas pelo aplicativo Strava.

Lembretes que foram adicionados e sincronizados com o Google Agenda também foram identificados na pasta /apps_rw/com.samsung.w-calendar2/data/ no arquivo .calendar_comsumer.db-journal. Neste, é possível identificar o conteúdo do lembrete e a data, grifadas em vermelho na Figura 12.

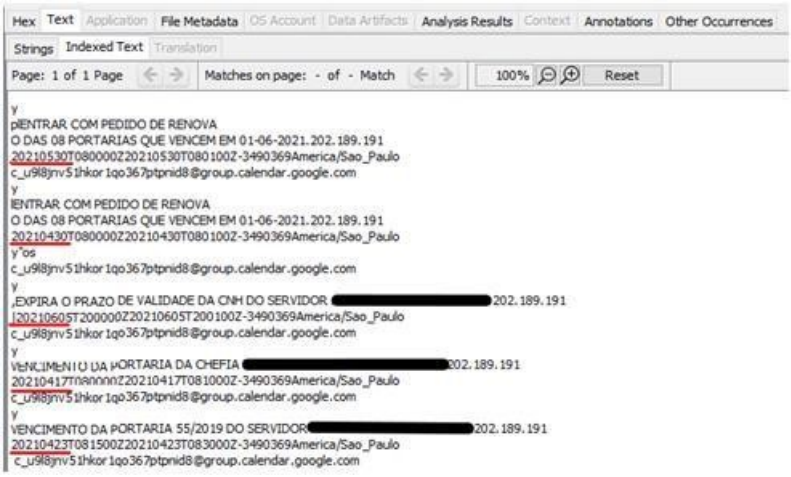

Figura 12: Lembretes do Google Agenda.

Outros arquivos foram encontrados e que podem ter valor forense, tal como imagens com mensagens de aplicativos (Figura 13).

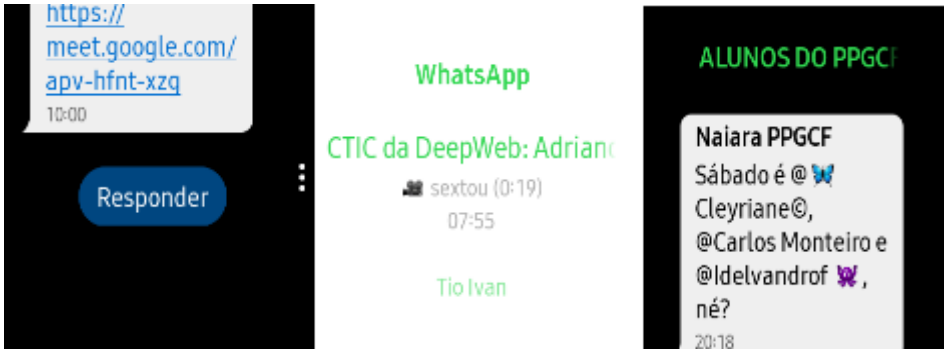

Figura 13: Notificações de aplicativos de mensagem.

Um resumo descritivo das informações extraídas do dispositivo analisado é apresentado na Tabela 2.

A relevância das informações que puderam ser extraídas do modelo analisado, mesmo se considerarmos as capacidades limitadas dos *smartwatches*, sugere a importância de maiores investimentos no desenvolvimento de técnicas de análise forense para esse tipo de dispositivo. Suas diversas funcionalidades estão associadas à geração de dados potencialmente valiosos em investigações criminais. A aquisição e análise de dados provenientes de *smartwatches* oferecem, por exemplo, uma via indireta para a obtenção parcial de dados armazenados em *smartphones* bloqueados ou danificados, desde que haja vínculo entre os dois equipamentos.

Tabela 2: Resumo dos principais arquivos e diretórios encontrados e extraídos sem acesso root ao smartwatch.

Arquivo ou diretório	Dados disponíveis
.contacts-svc.db	Arquivo de banco de dados que contém várias tabelas, como *contacts* e *phonelogs*, compreendendo todos os contatos da agenda e os registros de chamada, respectivamente.
strava_database.db	Arquivo de banco de dados com todos os exercícios registrados no aplicativo.
.reminder.db	Arquivo de banco de dados que contém os lembretes criados com uso do assistente de voz do dispositivo.
.calendar_consumer.db-journal	Arquivo que contém os lembretes do Google Agenda.
com.samsung.samsung-pay-app	Diretório em que se encontram vários arquivos, em sua maioria criptografados ou ilegíveis, mas dos quais foi possível extrair dados da bandeira e o nome do cartão de crédito usado pelo usuário.
com.samsung.w-home	Diretório no qual são encontradas várias imagens, dentre elas, fotos de contatos e notificações de aplicativos de mensagens
com.samsung.weather	Diretório no qual se pode obter informações sobre o clima, dando a possibilidade de indicar em que cidade o usuário encontra-se ou já passou.

4. CONCLUSÃO

Em geral, as investigações em dispositivos vestíveis são complementares, visto que a maior parte desses dispositivos precisa de um *smartphone* para prover a totalidade das suas funções. Este trabalho mostrou que mesmo em uma análise individual, e sem acesso de superusuário (root), é possível conseguir informações importantes e com valor forense. A análise feita com os dados extraídos de um *smartwatch* sugere que esse tipo de equipamento tem grande potencial de contribuição para investigações forenses, seja como fonte de evidências, ou de indicações para que peritos possam apresentar fatos ordenados temporalmente que, mesmo não sendo provas, podem inspirar aos investigadores direções a serem seguidas.

Para trabalhos futuros, pretende-se fazer o acesso com privilégio de root, visando ampliar o conjunto de informações com valor forense passíveis de serem extraídas do Samsung *Galaxy Active* 2. Além disso, será levada em consideração a manutenção da cadeia de custódia através de procedimentos destinados para dispositivos móveis, no intuito de validá-los em dispositivos vestíveis, em particular os relógios inteligentes.

5. REFERÊNCIAS

1. Nascimento JBD, Souza CLD, Serralvo FA. A systematic review of smart cities and the internet of things as a research topic. Cad EBAPE.BR. 2019 Oct-Dec;17(4):1115-30. doi: 10.1590/1679-395174442x
2. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys Tutorials. 2020;22(2):1191-221. doi: 10.1109/COMST.2019.2962586
3. Li S, Choo KR, Sun Q, Buchanan WJ, Cao J. IoT forensics: amazon echo as a use case. IEEE Internet Things J. 2019 Aug;6(4):6487-97. doi: 10.1109/JIOT.2019.2906946
4. Atlam HF, Hemdan EED, Alenezi A, Alassafi MO, Wills GB. Internet of Things forensics: A review. Internet of Things. 2020;11:100220. doi: 10.1016/j.iot.2020.100220
5. Dias MAA. Internet das Coisas: Novos desafios na análise forense. Parcerias Estratégicas. 2020;24(48):33-54.
6. Quick D, Choo KR. IoT device forensics and data reduction. IEEE Access. 2018;6:566-74. doi: 10.1109/ACCESS.2018.2867466
7. Austen K. The trouble with wearables. Nature. 2015;525(7567):22. doi: 10.1038/525022a

8. Jijiashvili G. Apple watch and hearables to fuel growth in wearables. CCS insight [Internet]; 2018 [citado 12 mai 2022]. Disponível em: https://www.ccsinsight.com/blog/apple-watch-and-hearables-to-fuel-growth-in-wearables/
9. Gregorio J, Alarcos B, Gardel A. Forensic analysis of nucleus RTOS on MTK smartwatches. Digital Investigation. 2019;29:55-66.
10. Sunardi S, Riadi I, Triyanto J. Forensics Mobile Layanan WhatsApp pada smartwatch menggunakan metode National Institute of Justice. JOINTECS. 2021;6(2):63-70.
11. British Broadcasting Corporation (BBC). Apple health data used in murder trial. BBC [Internet]; 12 jan 2018 [citado em 12 jan 2022]. Disponível em: https://www.bbc.com/news/technology-42663297
12. Kang S, Kim S, Kim J. Forensic analysis for IoT fitness trackers and its application. Peer-to-Peer Networking and Applications. 2020;13(2):564-73.
13. Gadyatskaya O, Massacci F, Zhauniarovich Y. Security in the Firefox OS and Tizen mobile platforms. Computer. 2014;47(6):57-63.
14. Brasil. Secretaria Nacional de Segurança Pública. Procedimento operacional padrão: Perícia criminal [Internet]. Brasília (DF): Ministério da Justiça; 2013. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2021/02/procedimento-operacional-padrao-pericia-criminal.pdf
15. Moore J, Baggili I, Marrington A, Rodrigues A. Preliminary forensic analysis of the Xbox One. Digital Investigation. 2014;11:S57-65.
16. Kim M, Shin Y, Jo W, Shon T. Digital forensic analysis of intelligent and smart IoT devices. J Supercomputing. 2022. doi: 10.1007/s11227-022-04639-5
17. Kim S, Jo W, Lee J, Shon T. AI-enabled device digital forensics for smart cities. The Journal of Supercomputing. 2022;78(2):3029-44 doi: 10.1007/s11227-021-03992-16