Análise Forense Digital da aplicação *Vivino*

Mestrado em Cibersegurança e Informática Forense (Pós-Laboral) – 2022/2024 – Unidade Curricular: Análise Forense Digital II

Bruno Costa
Escola Superior de Gestão e Tecnologia
Instituto Politécnico de Leiria
Leiria, Portugal
2220560@my.ipleiria.pt

Filipe Bagagem
Escola Superior de Gestão e Tecnologia
Instituto Politécnico de Leiria
Leiria, Portugal
2220558@my.ipleiria.pt

Pedro Marques
Escola Superior de Gestão e Tecnologia
Instituto Politécnico de Leiria
Leiria, Portugal
2220562@my.ipleiria.pt

Rui Pereira
Escola Superior de Gestão e Tecnologia
Instituto Politécnico de Leiria
Leiria, Portugal
2220281@my.ipleiria.pt

***Abstract*— A crescente popularidade e uso de dispositivos móveis e suas aplicações têm levado a um aumento significativo nas investigações forenses relacionadas a essas plataformas. Este projeto relata a análise forense abrangente da aplicação Vivino, com o objetivo de identificar e extrair evidências digitais relevantes para fins de investigação e de obtenção de prova digital forense. Em concreto, pretendeu-se encontrar evidências de recolha e comunicação de informações pessoalmente identificáveis (PII), dados e comunicações que recorrem a protocolos não seguros e dados com valor forense. Após a análise foi possível obter alguns dados relevantes.**

Keywords—android, artefactos, aplicação, vinho

I. INTRODUÇÃO

Este trabalho tem como objetivo apresentar uma abordagem com base em técnicas de Análise Forense e até Engenharia Reversa sobre a aplicação Vivino para Android. Ao aplicar estas técnicas nas aplicações Android, podemos extrair informações com valor forense, identificar possíveis vulnerabilidades e compreender o funcionamento da aplicação em profundidade.

Ao longo deste estudo serão exploradas técnicas de análise estática e dinâmica da aplicação num ambiente Android, recorrendo a diversas ferramentas e utilizando várias técnicas.

Espera-se que os resultados deste trabalho permitam fornecer *insights* sobre o cumprimento da legislação de privacidade e proteção de dados pessoais, e se é possível obter informações com relevância forense, bem como atestar a segurança, eficiência e a confiabilidade desta aplicação.

Apresentamos de seguida uma tabela resumo com dados relevantes da aplicação Vivino para Android.

Package	vivino.web.app
Versão	2023.4.2
Data de publicação	31 de janeiro de 2023, 12:07PM GMT+0000
Url	Link[1]
Mercado	Global
Downloads	mais de 10 milhões
Classificação	4.7
Nº de classificações	184 mil
Diretoria dados privados	/data/data/vivino.web.app
Diretoria dados públicos	Por omissão esta aplicação não guarda dados na diretoria /mnt/sdcard/Android/data/, mas o utilizador tem a possibilidade de exportar dados para esta diretoria.

II. ENQUADRAMENTO DA APLICAÇÃO

"O Vivino permite que as pessoas desfrutem ao máximo do vinho" [1].

O vinho é muito mais do que apenas um grande rótulo; trata-se de uma experiência e comunidade e, claro, do que está dentro da garrafa. É aí que entra o Vivino. Sendo o maior mercado online de vinhos do mundo e a aplicação de vinhos mais transferida, a comunidade do Vivino é composta por mais de 50 milhões utilizadores em todo o mundo, muitos deles consumidores de vinho, que se unem para tornar a compra do vinho mais simples, direta e divertida. O Vivino utiliza dados comunitários para personalizar as recomendações de vinhos de modo a que cada membro da comunidade se sinta confiante nas suas escolhas. Criado para todos os que gostam de vinho - desde consumidores curiosos até aos entusiastas, passando por produtores e comerciantes - a aplicação Vivino está disponível gratuitamente tanto em

[1] https://play.google.com/store/apps/details?id=vivino.web.app&hl=pt_PT&gl=US

dispositivos iOS como Android. O website Vivino.com partilha funcionalidades e dados com esta aplicação móvel.

A empresa foi criada em 2009 e tem sede em São Franscisco, estado da Califórnia, nos Estados Unidos da América. No ano seguinte foi disponibilizado o website e em 2011 as aplicações móveis para o público em geral [2]. O modelo de negócio assenta na utilização da plataforma como "*marketplace*", onde comerciantes e produtores vendem e promovem os seus vinhos junto da comunidade de utilizadores. A empresa gera retorno financeiro através das subscrições pagas que permitem inserir publicidade e promover produtos. Os subscritores beneficiam do acesso a dados estatísticos da plataforma, cujo tratamento de dados se baseia em técnicas de análise de *Big Data* assistidas por inteligência artificial e *machine learning* [3] [4].

A aplicação recorre a tecnologia de reconhecimento de imagem para a identificação de rótulos

Na Tabela 1 são apresentadas informações estatísticas acerca da aplicação Vivino, da empresa que o desenvolve e da comunidade de utilizadores.

Parâmetro	Valor
Colaboradores (em todo o mundo)	300
Vinhos catalogados	16.395.552
Rótulos digitalizados	2.354.304.998
Avaliações submetidas	93.770.965
Classificações submetidas	267.150.048
Preços submetidos	2.063.729
Utilizadores registados	63.717.501
Regiões vinícola	3.468
Adegas registadas	245.637

Tabela 1- Estatísticas relacionadas com o Vivino

Na Figura 1 são apresentadas duas capturas de ecrã a interface de utilizador, onde são apresentadas as principais funcionalidades da aplicação: apresentação de informação referente a um determinado vinho e pesquisa de vinhos através de critérios (neste caso, por gama de preços).

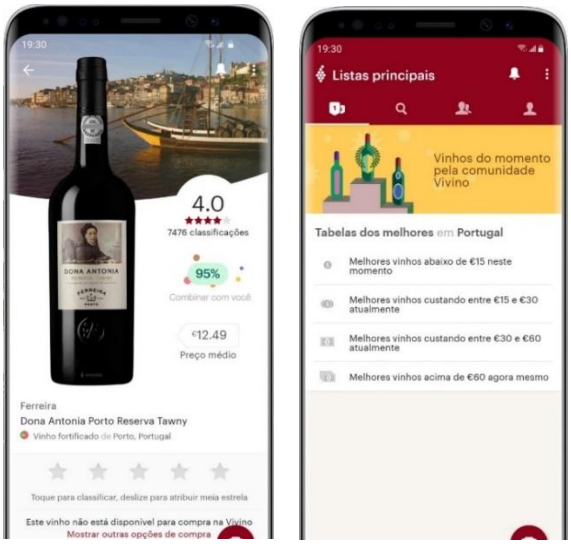

Figura 1 - Capturas de ecrã da aplicação Vivino

III. DESCRIÇÃO DAS FUNCIONALIDADES

A aplicação Vivino assemelha-se a um catálogo interativo de vinhos, cuja informação é atualizada e enriquecida pelos seus utilizadores, nomeadamente consumidores, produtores e comerciantes. As funcionalidades e dados são partilhados com o website "vivino.com".

Na primeira utilização da aplicação móvel é necessário que o utilizador proceda à autenticação com uma conta de utilizador, constituída por endereço de email e password, ou através da utilização de autenticação integrada *OAuth*, através das plataformas Apple, Google, Facebook e Twitter. Caso ainda não se tenha uma conta de utilizador, é possível criar uma através da aplicação móvel ou website, recorrendo aos mecanismos já mencionados.

Após autenticação, é possível pesquisar e inserir informações e classificações acerca de vinhos. Assim, consideram-se como principais funcionalidades:

a) fotografar o rótulo de um vinho;

b) pesquisar por características de um vinho;

c) ver a classificação e comparação do vinho, obtendo opiniões, preços, notas de degustação e sugestões de harmonização;

d) efetuar compras de garrafas (opção não disponível para o mercado português);

e) obter recomendações de vinhos em função dos gostos inseridos;

f) inventariar as garrafas que temos em casa.

IV. DISPONIBILIZAÇÃO DA APLICAÇÃO, VERSÕES E MÓDULOS INSTALADOS

A aplicação Vivino encontra-se disponível no Google Play (Figura 2) através do link:

https://play.google.com/store/apps/details?id=vivino.web.app&hl=pt_PT&gl=US

Figura 2- Google Play - Instalação da aplicação Vivino

Recorrendo aos dados disponibilizados no Google Play, em abril de 2023, a aplicação Vivino apresenta uma excelente classificação, sendo 4,7 em 5, conforme Figura 3, contabilizando mais de 10.000.000 transferências.

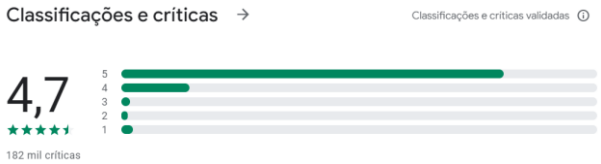

Figura 3- Classificação aplicação Vivino no Google Play

Para instalação da aplicacão Vivino no emulador foi utilizado o APK disponibilizado no site *APK Mirror* (**Erro! A origem da referência não foi encontrada.**), por não ser possível instalar aplicações no emulador através do Google Play. Link do *APK*:

https://www.apkmirror.com/apk/vivino/vivino-wine-scanner/vivino-wine-scanner-2023-4-2-release/

Figura 4- APK Mirror - Página para download da aplicação Vivino

- **Nome do *Package***: vivino.web.app_2023.4.2-2023040299_minAPI24(arm64-v8a,armeabi,armeabi-v7a,x86,x86_64)(nodpi)_apkmirror.com.apk
- **Versão**: 2023.4.2
- **Data**: 31 de janeiro de 2023, 12:07PM GMT+0000
- **Tamanho do Ficheiro**: 77.29 MB

Em termos de classificação de conteúdo, esta aplicação destina-se a Adolescentes ou idades superiores.

Na Google Play pode-se obter as autorizações anunciadas aos utilizadores pela própria aplicação:

- **Armazenamento (**ler os conteúdos da memória USB; alterar ou eliminar o conteúdo da memória USB)
- **Localização (**localização aproximada (baseada na rede); localização exata (baseada no GPS e na rede)
- **Informações da ligação Wi-Fi (**ver ligações Wi-Fi);
- **Fotos/multimédia/ficheiros** (ler os conteúdos da memória USB; alterar ou eliminar o conteúdo da memória USB);
- **Câmara** (tirar fotos e vídeos);
- **Outro** (receber dados da internet; controlar vibração; impedir que o dispositivo entre em inatividade; controlar lanterna; ver ligações de rede; ler configuração de serviços Google; acesso total à rede; Verificação da licença do Google Play).

V. APLICAÇÕES SEMELHANTES

Como aplicação concorrente ao Vivino, foi identificada a Delectable Wine - Scan & Rate, disponível no Google Play.

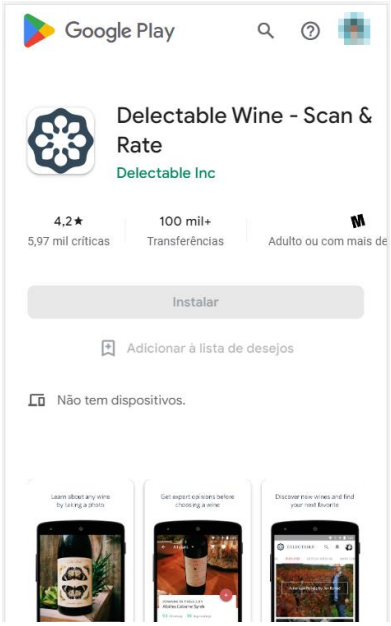

Figura 5 - Instalação Delectable Wine - Scan & Rate

Recorrendo aos dados disponibilizados no Google Play, em abril de 2023, a aplicação *Delectable Wine - Scan & Rate* apresenta uma classificação de 4,2 em 5 e conta com mais 100 000 transferências.

VI. HISTÓRICO DE ANÁLISES FORENSES EFETUADAS AO VIVINO

Das pesquisas efetuadas na internet, através de vários motores de busca, não foi possível obter qualquer registo público de análise forense a esta aplicação.

VII. MÉTODOS E FERRAMENTAS UTILIZADAS

A. Casos de uso

Para a realização da análise foram considerados os seguintes casos de uso, que consideramos ter relevância forense:

1) Criar conta para acesso à aplicação, com inserção de email e password;
2) Aceder a conta de utilizador criada;
3) Listar vinhos com melhor classificação dada pelos utilizadores, por gama de preços;
4) Pesquisar vinhos por diferentes critérios (país/região de origem, tipo, estilo, comida a acompanhar);

5) Adicionar vinho a lista de interesses;
6) Classificar vinho (através de uma escala de 0 a 5, em incrementos de 0,1, com possibilidade de adicionar um comentário);
7) Caracterizar o vinho em função de 4 parâmetros;
8) Adicionar preço (com indicação de quantidade, local e se é oferta limitada no tempo);
9) Adicionar local (solicita acesso à localização atual);
10) Adicionar notas e comentários;
11) Adicionar ao inventário pessoal de vinhos ("Adega");
12) Notificar utilizadores do uso da aplicação, recorrendo a contactos relacionados através da API do Google e contactos do telefone;
13) Parametrizar a conta de utilizador com informação pessoal, tais como primeiro e último nome, país, idioma da aplicação, biografia (campo de texto), website; definições de notificações (novos seguidores, novos amigos, novos "likes", comentários, referências a análises, comentários e fotos), configuração dos alertas por "push" ou envio de email.
14) Parametrizar opções de privacidade, como quem pode ver a minha atividade e utilizadores bloqueados;
15) Parametrizar se as fotografias também são guardadas na galeria local de fotos.

Não foram considerados os seguintes casos de uso:

16) Acesso à aplicação através de conta associada a métodos OAuth (Apple, Google, Facebook, Twitter);
17) Ligação da conta a redes sociais (Apple, Google, Facebook e Twitter) com opção para seguir automaticamente os utilizadores presentes nas listas de contacto destas redes sociais.

B. Instalação do emulador

Para a instalação e configuração do ambiente de análise forense digital a dispositivos móveis *Android* nos computadores pessoais dos elementos do grupo, foi tido em consideração a documentação disponibilizada pelos docentes da presente Unidade Curricular [5].

Recorremos ao software *Android Studio* para virtualizar um dispositivo Android. A versão do *Android Studio* que utilizámos foi 2022.2.1, como representado na Figura 6.

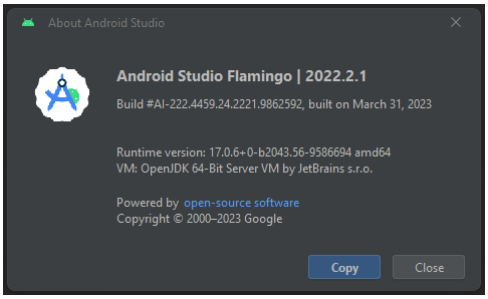

Figura 6 - Versão do Android Studio

Concluída a instalação e configuração inicial do Android Studio, começamos por criar um dispositivo virtual através da opção "AVD Manager" (Figura 7 e Figura 8). Para evitar o consumo excessivo de recursos do equipamento físico (computador), adicionamos um novo perfil de hardware de baixa resolução, nomeadamente:

Resolução do ecrã: 320 x 640 px

Memória RAM: 2048 MB

Input: (*ativar*) "*Has Hardware Buttons (Back/Home/Menu)*" para facilitar a navegação; (*ativar*) "*Has Hardware Keyboard*".

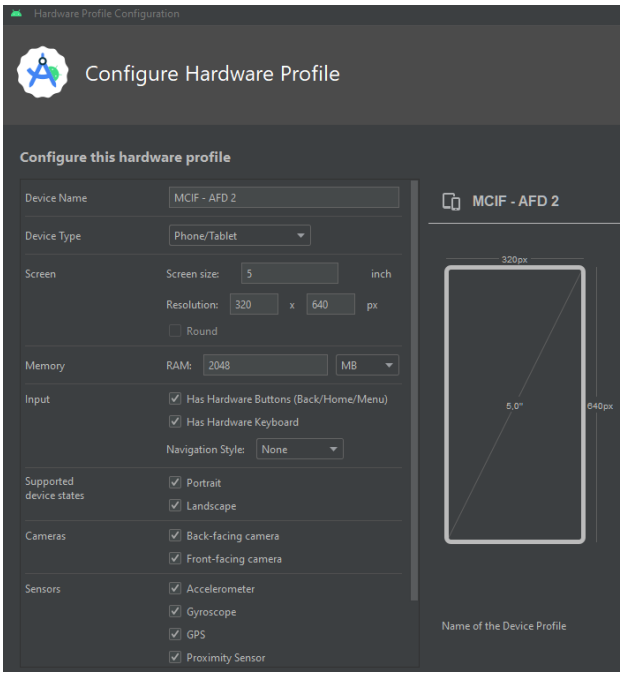

Figura 7 - Criar o perfil de hardware para o emulador

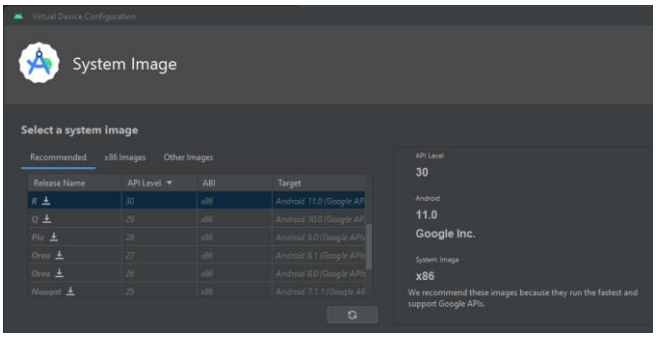

Figura 8 - Imagem Android para o emulador

Após a criação do *virtual device*, o mesmo foi iniciado (Figura 9) para se proceder à instalação do *Vivino* e das restantes aplicações utilizadas para análise.

Figura 9 - Emulador instanciado com a aplicação Vivino

C. *Instalação da aplicação Vivino no emulador*

Conforme referido anteriormente, não é possível instalar aplicação através do Google Play, por essa razão tivemos de realizar o seguinte procedimento:

1. Descarregar a última versão do ficheiro apk disponibilizado no site:

   https://www.apkmirror.com/apk/vivino/

2. Com recurso à aplicação adb.exe, do próprio Android Studio (..\SDK\platform-tools\), procedemos à instalação do ficheiro apk no emulador anteriormente instanciado.

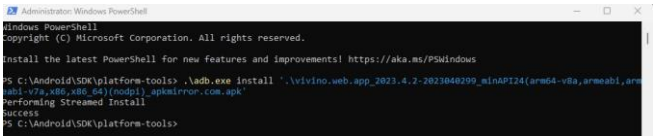

Figura 10 - Instalação do apk (vivino) no emulador

Para se proceder à análise estática e dinâmica foram configuradas um conjunto de aplicações, que são apresentadas nas secções seguintes, para permitir obter mais informações sobre ficheiros e recursos do telemóvel usados e comunicações efetuadas.

D. *Instalação e captura do tráfego HTTP com o HTTP Toolkit, Fiddler e o Frida*

As realizações de testes com as três ferramentas abordadas permitiram que se pudessem analisar as comunicações feitas através de protocolos de comunicação seguros, nomeadamente HTTPS, recorrendo à técnica de *SSL pinning / certificate pinning* [6]. Deste modo é possível saber que dados circulam entre aplicação e serviços externos [7].

1) *HTTP Toolkit*

No caso de uso nº 2, de "aceder a conta do utilizador criada", foi possível aferir através do HTTP Toolkit que os dados de autenticação, nomeadamente password, não se encontra cifrada (Figura 11). Os dados são enviados pelo método POST de HTTP e podem ser identificados vários parâmetros de aplicação, passíveis de serem manipulados. A aplicação relega a proteção da informação para o protocolo da camada superior.

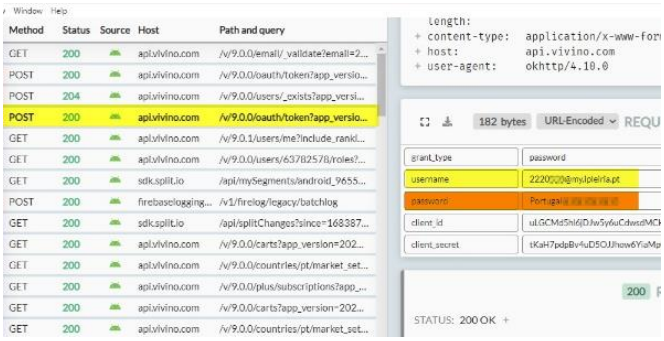

Figura 11 - Autenticação analisada através do HTTP Toolkit

A análise de comunicações foi retomada mais tarde recorrendo ao segundo ambiente de simulação, recorrendo da *Genymotion*.

2) *Fiddler*

A utilização do *Fiddler* foi utilizada no contexto da simulação no *Genymotion*. Foi possível listar os servidores com os quais a aplicação comunicou.

3) *Frida*

Tal como a ferramenta anterior, apesar de se ter feito a instalação da ferramenta utilizando o ambiente simulado com o *Android Studio*, a análise dinâmica recorrendo ao Frida foi efeituada recorrendo ao ambiente do *Genymotion*.

E. *Análise dos timestamp da aplicação*

Para a análise dos *timestamps* encontrados na aplicação em formato *UNIX epoch* foi utilizada a ferramenta Epoch Converter, disponível através do endereço web https://www.epochconverter.com/.

F. *Instalação de ambiente de análise alternativo - Genymotion*

Durante o processo de análise forense foram conhecidas outras ferramentas, que facilitaram a realização de análises estáticas e dinâmicas. Através do *Genymotion* (Figura 12) foi possível efetuar algumas das operações anteriormente efetuadas com o *Android Emulator* do *Android Studio*. A instalação e integração do *Genymotion* com o MobSF foi apresentada no contexto de aula, pelo aluno Miguel Felício, e explorada com recurso a artigos científicos e estudos apresentados na web. A configuração realizada encontra-se documentada no anexo[2].

[2] anexo_configuracao_genymotion.pdf

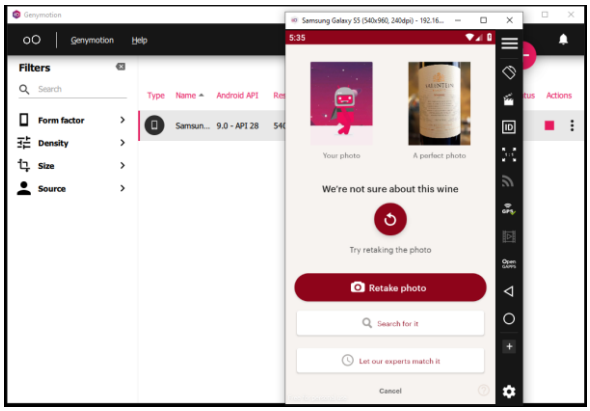

Figura 12 - Interface Genymotion e vista do Vivino no emulador

Através do Genymotion foram realizadas diversas extrações de relatórios, em diferentes fases da utilização da aplicação.

G. Instalação e configuração do simulador de dados GPS

O *Genymotion* tem funcionalidades avançadas, com a simulação do GPS. A aplicação *Vivino* disponibiliza a funcionalidade de georreferenciação para os casos de uso nº 8 (adicionar preço) e nº 9 (adicionar local à ficha do vinho). No entanto, a aplicação não reconheceu as permissões necessárias para acesso ao GPS.

Esta informação pode ser relevante do ponto de vista forense, porque pode atestar que o utilizador estava em determinado local no momento da interação e submissão de dados através da aplicação (considera-se que esta informação pode ser manipulada, caso seja utilizada uma aplicação para gerar dados de localização geográfica por GPS falsos (Figura 13)).

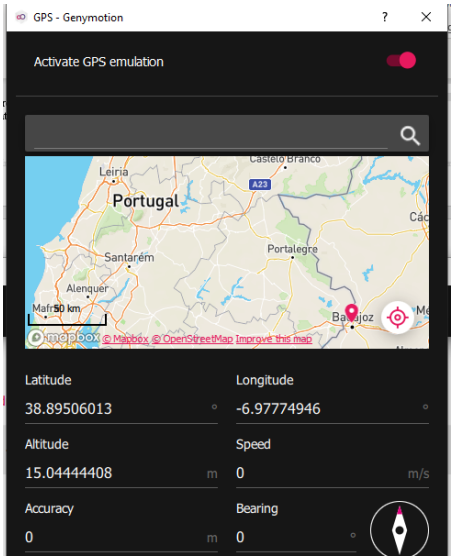

Figura 13 - Manipulação da localização GPS (de Leiria para Badajoz)

Após vários testes sem sucesso no uso do simulador de GPS do *Genymotion*, foram efetuados testes com o emulador do *Android Studio*. Foi possível definir uma localização e utilizar a opção de "selecionar local", para encontrar os locais próximos da localização fornecida que comercializem o vinho pesquisado (Figura 14) .

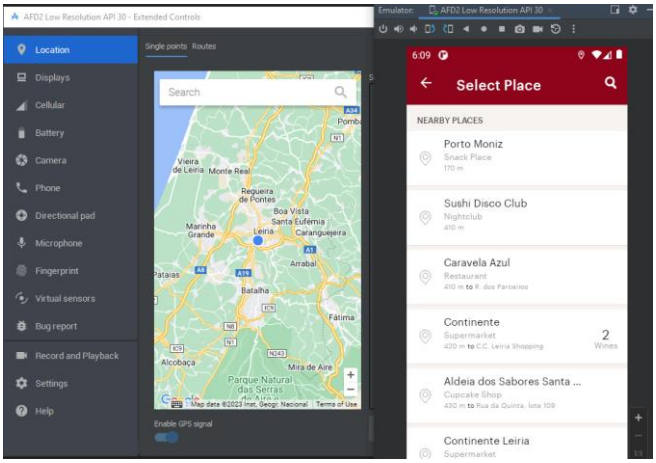

Figura 14 - Localização GPS com Android Studio

H. Instalação e captura de dados utilizando a aplicação ADB-Extractor

Durante a realização do relatório, já depois da utilização das ferramentas abordadas, foi publicado no repositório do LabCIF no *GitHub* uma ferramenta chamada "*ADB-Extractor*", desenvolvida em *Python* por Fabian Nunes, que permite extrair os ficheiros da zona pública, privada e APK de uma determinada aplicação [8]. A aplicação "*ADB-Extractor*" foi testada mas os dados extraídos não acrescentaram informações relevantes aos recolhidos através das outras aplicações utilizadas.

Figura 15 - ADB Extractor

I. Análise ao ficheiro Manifest

Quando a aplicação Vivino precisar de aceder a recursos do dispositivo, terá de solicitar ao utilizador permissões para o fazer, caso não o tenha feito anteriormente. Algumas das permissões são concedidas pelo utilizador durante a instalação da aplicação e outras precisam ser confirmadas

adicionalmente durante a utilização da aplicação. As permissões solicitadas são declaradas no arquivo AndroidManifest.xml, que segue em anexo[3].

Na análise ao ficheiro Manifest.xml (figura 16), destacamos as seguintes permissões:

- Acesso à localização aproximada;
- Acesso à localização exata;
- Acesso à camara;
- Acesso à vibração do dispositivo;
- Acesso ao estado de rede;
- Acesso à Internet;
- Acesso para ativar luz da camara;
- Acesso ao estado do wi-fi
- Acesso a serviços em segundo plano;
- Acesso para postar notificações;
- Acesso ao PowerManager WakeLocks para evitar que o processador suspenda ou o ecrã escureça;

AndroidManifest.xml

```
<manifest
        xmlns:android="http://schemas.android.com/apk/res/android"
        android:versionCode="2023040299"
        android:versionName="2023.4.2"
        android:allowBackup="false"
        android:installLocation="0"
        android:compileSdkVersion="33"
        android:compileSdkVersionCodename="13"
        package="vivino.web.app"
        platformBuildVersionCode="33"
        platformBuildVersionName="13">
        <application
                android:theme="(reference) @0x7f1403d3"
                android:label="(reference) @0x7f130107"
                android:icon="(reference) @0x7f100000"
                android:name="com.vivino.MyApplication"
                android:allowBackup="false"
                android:hardwareAccelerated="true"
                android:largeHeap="true"
                android:supportsRtl="false"
                android:extractNativeLibs="false"
                android:fullBackupContent="true"
                android:resizeableActivity="false"
                android:networkSecurityConfig="(reference) @0x7f170005"
                android:appComponentFactory="androidx.core.app.CoreComponentFactory"
                android:requestLegacyExternalStorage="true">
                <meta-data
                        android:name="com.android.vending.derived.apk.id"
```

Figura 16 - Cabeçalho Android Manifest

O conteúdo de todas as permissões solicitadas ao utilizador da aplicação Vivino estão no anexo[4] .

VIII. AQUISIÇÃO DOS DADOS

A aquisição lógica dos dados teve em consideração diversos casos de uso, agrupando-os, e foi obtida utilizando as ferramentas previamente mencionadas (nomeadamente o *Genymotion* e *MobSF*) em vários momentos temporais:

1) Após instalação da aplicação, sem executar;
2) Primeira execução;
3) Após autenticação do utilizador com conta válida (neste caso, uma conta de utilizador regular da aplicação, com interação com a aplicação ao nível de pesquisas, submissão de classificações e comentários, bem como envio de fotografias de rótulos de garrafas);
4) Após vários casos de uso;
5) Após logoff com primeiro utilizador e login com segundo utilizador.

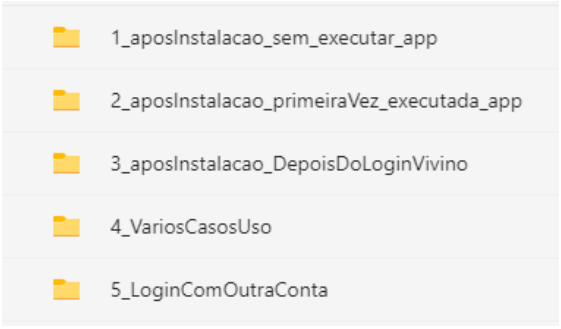

Figura 17 - Pastas com relatórios guardados

Os dados privados constam nas pastas mencionadas na Figura 17 e na Figura 18 é apresentada a estrutura de uma delas com mais detalhe. É possível identificar as pastas onde são guardadas as bases de dados, as imagens, a *cache* (ficheiros temporários), ficheiros referentes às APIs utilizadas (MixPanel, para estatísticas), gestão de tarefas através de filas (*Job Queues*) e sessões ativas com bases de dados remotas.

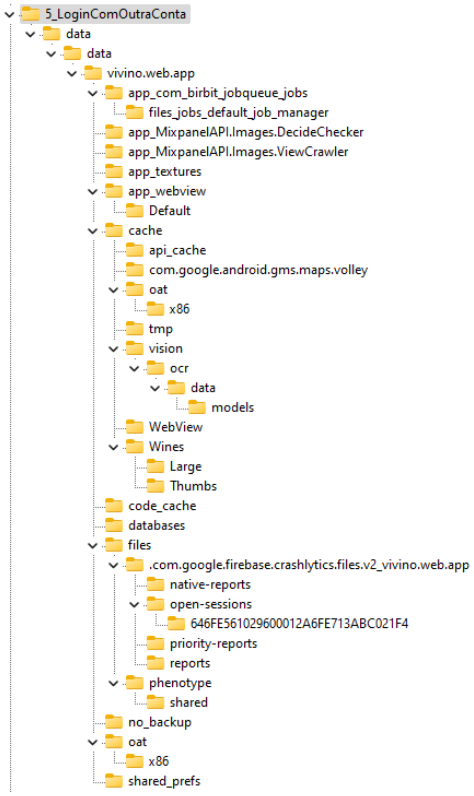

Figura 18 - Estrutura detalhada da diretoria de dados privados no caso de uso nº 5

À medida que foram executados os diversos casos de uso e feita a extração dos dados da pasta privada, a atual extração foi comparada com a anterior (com recurso ferramenta WinMerge). As alterações que ocorreram ao nível de pastas são visíveis na Figura 19, Figura 20, Figura 21 e Figura 22. As diferenças entre pastas estão destacadas e marcadas a amarelo.

[3] anexo_manifest_AppVivino.xml

[4] anexo_Android_Manifest_Vivino.pdf

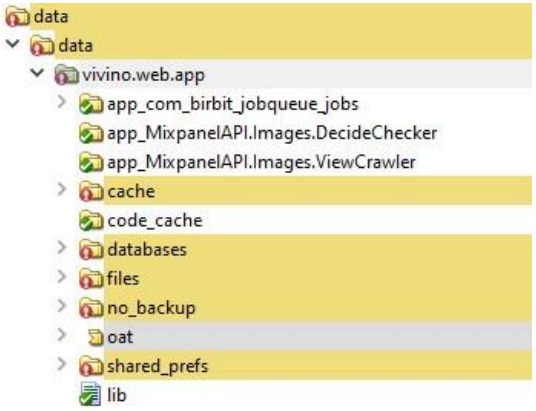

Figura 19 - Diferenças entre momento 1 e 2

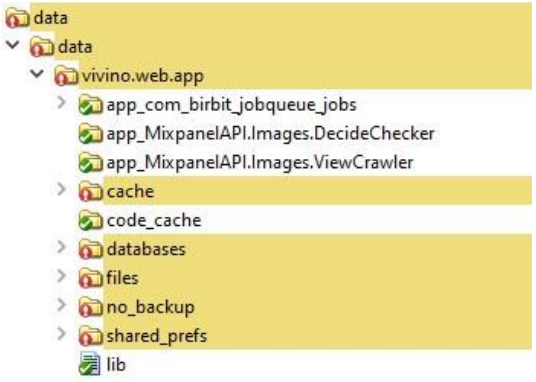

Figura 20 - Diferenças entre momento 2 e 3

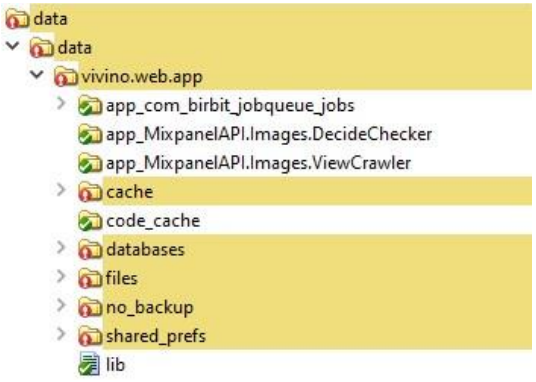

Figura 21 - Diferenças entre momento 3 e 4

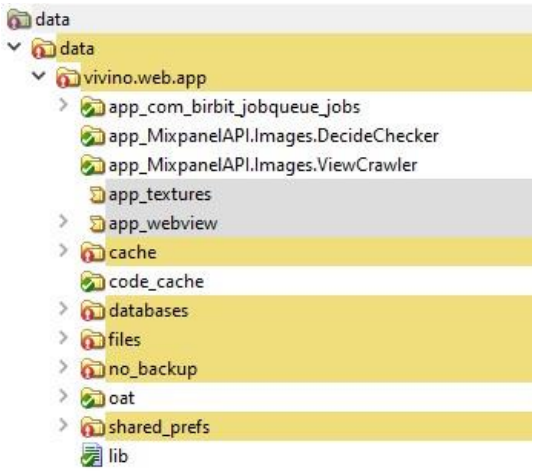

Figura 22 - Diferenças entre momento 4 e 5

O número de pastas e ficheiros presentes nos vários momentos de aquisição, abordados na Figura 17, são expostos na Tabela 2.

Momento/ Número	Pastas	Ficheiros
1º Após instal, sem executar	21 (3,48 MB)	58
2º Após 1ª execução	22 (13,6 MB)	79
3º Após Login	22 (44,7 MB)	720
4º Vários casos de uso	35 (128 MB)	1406
5º Login com outra conta	38 (51,1 MB)	395

Tabela 2 - Números de pastas e ficheiros por momento de aquisição

Podemos concluir desta análise que a estrutura principal das pastas é mantida, sendo afetadas pastas onde constam dados associados ao utilizador que foram obtidos do servidor remoto. Na estrutura principal a pasta "oat", que está diretamente relacionado com as análises efetuadas, nomeadamente ficheiros da ferramenta "Frida".

IX. ANÁLISE DOS DADOS RECOLHIDOS

A. *Análise estática*

Nesta secção apresentamos um resumo e a nossa interpretação da análise realizada através do MobSF e das informações mais críticas encontradas no relatório que segue em anexo[5].

1) Permissões da aplicação

Foram consideradas perigosas 5 permissões pedidas pela aplicação, nomeadamente o acesso a localização aproximada e também exata, camara, memoria interna e externa.

- *android.permission.ACCESS_COARSE_LOCATION*
- *android.permission.ACCESS_FINE_LOCATION*
- *android.permission.CAMERA*
- *android.permission.READ_EXTERNAL_STORAGE*

[5] anexo_estatico_MobSF_vivino.pdf

- *android.permission.WRITE_EXTERNAL_STORAGE*

2) Segurança de rede

Subdomínio images.vivino.com categorizado com severidade *High* devido ao domínio estar a permitir comunicações em Clear Text.

3) Base de dados Firebase

Foi encontrado o link da base de dados central, esta aplicação utiliza a base de dados da Firebase.

- *https://vivino-com-api-project-403647931437.firebaseio.com/*

4) Endereços de email

Foram encontrados emails na aplicação, do quais podemos tirar pelo menos 2 como funcionais e que podem ser utilizados para ataques de engenharia social.

- *support@vivino.com*
- *orders@vivino.com*

5) "Hardcoded secrets"

Foram encontradas algumas chaves hardcoded do qual podemos tirar algumas informações. sabemos que a aplicação utiliza os serviços Stripe para processar pagamentos e temos a sua chave publica [9].

Confirmação do uso de Firebase nomamente. uma chave do API do google, google crash e google maps [10]. Estas chaves é normal estarem publicas, mas podem ser utilizadas para causar disrupção, uso não autorizado ou abuso de serviços [11].

- *"STRIPE_PUBLISHABLE_KEY" : "pk_live_f4BNIfN3nlvNKpyNQx36OAsN"*
- *"com.google.firebase.crashlytics.mapping_file_id" : "00b85cd3867e4543beea01befdf1b9f2"*
- *"firebase_database_url" : https://vivino-com-api-project-403647931437.firebaseio.com*
- *"google_api_key" : "AIzaSyCnAKLXhGW0L33-Ybfy5rfTmTa0DhWGu90"*
- *"google_crash_reporting_api_key" : "AIzaSyCnAKLXhGW0L33-Ybfy5rfTmTa0DhWGu90"*
- *"google_maps_key" : "YOUR_KEY_HERE" "google_maps_sign_key" : "hSrq0Zlakr97f_TUFUHy1Ww0BIY="*
- *"google_maps_v2_api_key" : "AIzaSyB-10yUXwQfYKdyI5jFQ1ElJ5vtKw_SyiY"*

6) Análise do ficheiro vivino.web.wine_list.xml

Na diretoria /data/data/vivino.web.app/shared_prefs identificou-se o ficheiro referido em epígrafe com informação que identifica o utilizador que realizou login na aplicação a última vez, conforme é possível verificar na Figura 23 e 24.

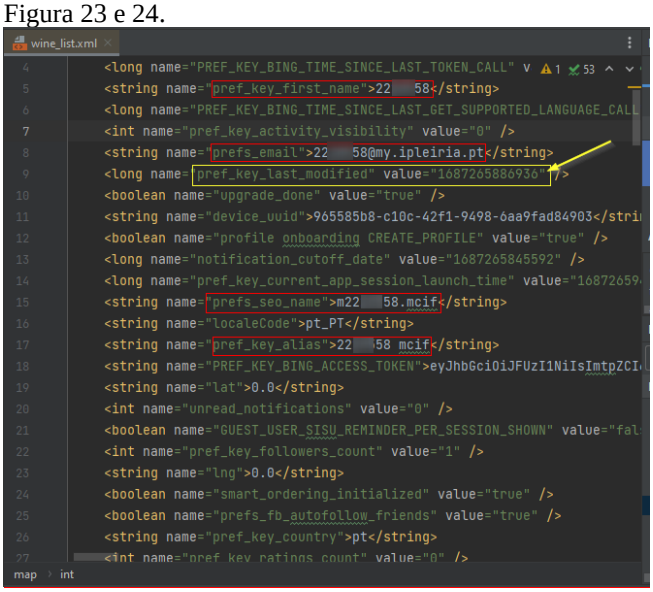

Figura 23 - - Login com sucesso do utilizador 1

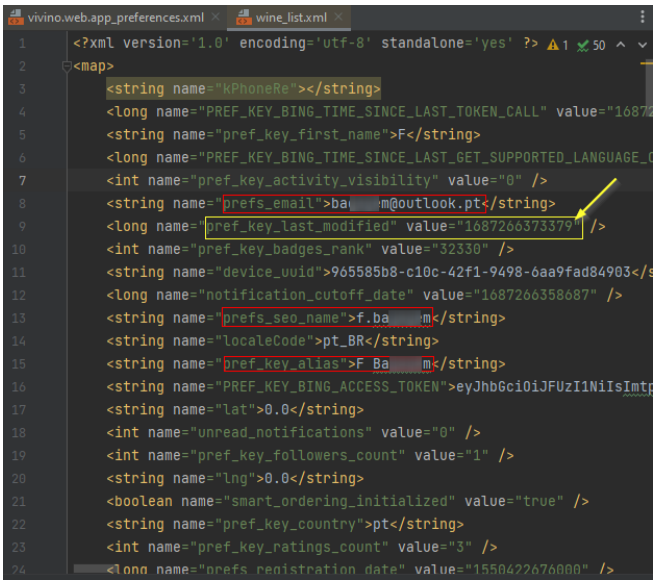

Figura 24 - Login com sucesso do utilizador 2

Analisando o ficheiro apenas se consegue identificar o último utilizador que se autenticou na aplicação, bem como timestamp em que foi gerada a *key* de ligação ao webservice do Vivino. Caso o utilizador faça "Sign Out" na aplicação Vivino a informação é removida do ficheiro "vivino.web.wine_list.xml", conforme é possível comprovar pelas figuras abaixo (25 e 26).

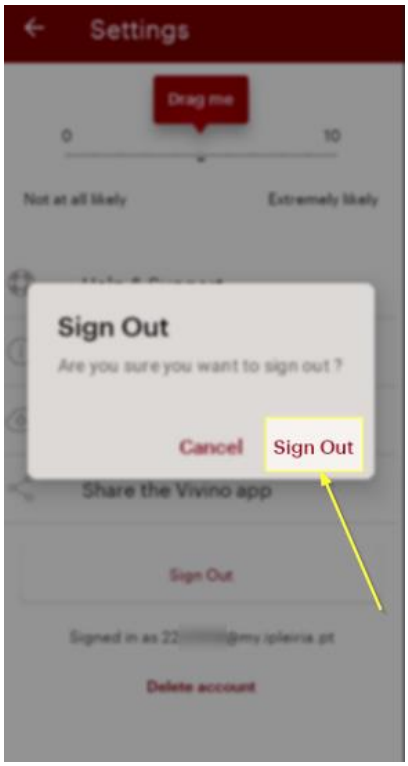

Figura 25 - Sign Out

Figura 26 - Sem informação relevante

B. Análise Dinâmica

A análise dinâmica foi realizada com recurso a várias ferramentas. Um dos relatórios da análise dinâmica consta no anexo [6] . Os factos relevantes foram anteriormente mencionados na exposição das ferramentas utilizadas e são também detalhados nas subseções seguintes.

1) Trackers

A aplicação apresenta um conjunto de *trackers* conhecidos e identificados, com servidores dentro e fora da União Europeia (27).

Figura 27 - Localização dos servidores com os quais a aplicação comunica

Os *trackers* detetados pelo MobSF podem ser agrupados nas seguintes categorias: a) analítica (Adjust, Facebook Analytics, Google Firebase Analytics, Split Analytics, MixPanel); b) identificação (Facebook Login); c) reporte de erros (Google CrashLytics); d) publicidade (MixPanel).

No *website* "exodus-Privacy.eu.org" os vários *trackers* são caracterizados. Não existe relato de infração da legislação de privacidade e proteção de dados pessoais por parte destes serviços.

2) Metadados

A aplicação permite tirar fotografias ou submeter fotografias já existentes no dispositivo. Concluímos que os metadados das imagens submetidas são eliminados conforme é possível verificar nas imagens abaixo. Os metadados da imagem obtida pelo dispositivo, antes de a submeter para o servidor do Vivino, são apresentados na Figura 28.

A análise está documentada em anexo [7], bem como as fotografias ondem foram retiradas as evidências.

- Foto submetida para o webservice da aplicação Vivino - 20230525_222325.jpg.
- Foto devolvida pelo webservice da aplicação Vivino - 20230525_222325_foto_descarregadaVivino.jpg.

[6] anexo_dinamico_MobSF_vivino.pdf

[7] anexo_metadados_foto_20230525_222325.pdf

```
C:\tools\exiftool>exiftool.exe 20230525_222325.jpg
ExifTool Version Number         : 12.50
File Name                       : 20230525_222325.jpg
Directory                       : .
File Size                       : 3.2 MB
Zone Identifier                 : Exists
File Modification Date/Time     : 2023:06:03 11:46:03+01:00
File Access Date/Time           : 2023:06:03 11:48:16+01:00
File Creation Date/Time         : 2023:05:25 22:27:23+01:00
File Permissions                : -rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Little-endian (Intel, II)
Image Description               :
Make                            : samsung
Camera Model Name               : SM-M225FV
Orientation                     : Rotate 90 CW
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : MediaTek Camera Application
Modify Date                     : 2023:05:25 22:23:27
Y Cb Cr Positioning             : Co-sited
Exposure Time                   : 1/20
F Number                        : 2.0
Exposure Program                : Program AE
ISO                             : 640
Sensitivity Type                : Unknown
Recommended Exposure Index      : 0
Exif Version                    : 0220
Date/Time Original              : 2023:05:25 22:23:27
Create Date                     : 2023:05:25 22:23:27
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/20
Aperture Value                  : 2.0
Brightness Value                : 0
Exposure Compensation           : 0
Max Aperture Value              : 2.0
Metering Mode                   : Center-weighted average
Light Source                    : Other
Flash                           : Off, Did not fire
Focal Length                    : 4.6 mm
Sub Sec Time                    : 031
Sub Sec Time Original           : 031
Sub Sec Time Digitized          : 031
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 4000
Exif Image Height               : 3000
Interoperability Index          : R98 - DCF basic file (sRGB)
Interoperability Version        : 0100
Exposure Mode                   : Auto
White Balance                   : Auto
Digital Zoom Ratio              : 1
Focal Length In 35mm Format     : 25 mm
Scene Capture Type              : Standard
Compression                     : JPEG (old-style)
Thumbnail Offset                : 1408
Thumbnail Length                : 64000
Image Width                     : 4000
Image Height                    : 3000
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Time Stamp                      : 2023:05:25 22:23:25.733+01:00
MCC Data                        : Portugal
Aperture                        : 2.0
Image Size                      : 4000x3000
Megapixels                      : 12.0
Scale Factor To 35 mm Equivalent: 5.4
Shutter Speed                   : 1/20
Create Date                     : 2023:05:25 22:23:27.031
Date/Time Original              : 2023:05:25 22:23:27.031
Modify Date                     : 2023:05:25 22:23:27.031
Thumbnail Image                 : (Binary data 64000 bytes, use -b
option to extract)
Circle Of Confusion             : 0.006 mm
Field Of View                   : 71.5 deg
Focal Length                    : 4.6 mm (35 mm equivalent: 25.0 mm
)
Hyperfocal Distance             : 1.91 m
Light Value                     : 3.6
```

Figura 28 - Metadados da imagem (POST)

Os metadados da imagem, depois de submetida (POST) para o servidor do Vivino (Figura 28) e recolhida pelo dispositivo móvel (GET), são apresentados na Figura 29.

```
C:\tools\exiftool>exiftool.exe 20230525_222325_foto_descarregadaViv
ino.jpg
ExifTool Version Number         : 12.50
File Name                       : 20230525_222325_foto_descarregada
Vivino.jpg
Directory                       : .
File Size                       : 24 kB
Zone Identifier                 : Exists
File Modification Date/Time     : 2023:06:03 11:46:06+01:00
File Access Date/Time           : 2023:06:03 11:48:18+01:00
File Creation Date/Time         : 2023:06:03 11:46:06+01:00
File Permissions                : -rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Profile CMM Type                :
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 0000:00:00 00:00:00
Profile File Signature          : acsp
Primary Platform                : Unknown ()
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             :
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Col
Rendering Intent                : Media-Relative Colorimetric
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 :
Profile ID                      : 0
Profile Description             : sRGB
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
Red Tone Reproduction Curve     : (Binary data 40 bytes, use -b opt
ion to extract)
Green Tone Reproduction Curve   : (Binary data 40 bytes, use -b opt
ion to extract)
Blue Tone Reproduction Curve    : (Binary data 40 bytes, use -b opt
ion to extract)
Media White Point               : 0.9642 1 0.82491
Profile Copyright               : Google Inc. 2016
Image Width                     : 480
Image Height                    : 640
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 480x640
Megapixels                      : 0.307
```

Figura 29 - Metadados da imagem (GET)

3) Análise de comunicações em tempo real (HTTP toolkit)

Ao submeter imagens para o servidor do Vivino, esta é codificada em trânsito, conforme é possível verificar na Figura 30.

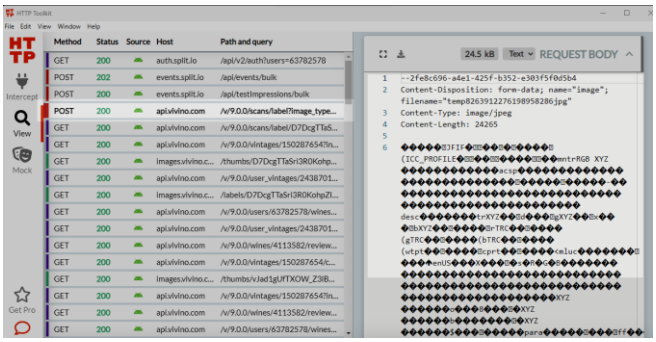

Figura 30 - Submissão de uma imagem

Observando o relatório do MobSF (Figura 31), é possível verificar que as comunicações com os vários servidores externos podem ser feitas por HTTP (comunicação não segura) e HTTPS (comunicações seguras).

Figura 31 - Tipos de comunicação permitidas com servidores remotos

4)Base de dados vivino.sqlite

Na estrutura de ficheiros da aplicação foram identificadas várias bases de dados em SQLite.

Todas as bases de dados encontradas são constituídas por três ficheiros: 1) nome da base de dados; 2) ficheiro com sufixo "-wal", que contém os dados temporários que serão eliminados após o encerramento da conexão; 3) ficheiro com sufixo "-shm", que contém os index da informação presente no ficheiro temporário "-wal".

As bases de dados presentes na pasta "databases" da pasta principal "vivino.web.app" são:

- c2jnhvf8 – base de dados criada com nome aleatório, com dados de execução da aplicação;
- com.google.android.datatransport.events – base de dados associada à interação com a instância remota de Firebase;
- db_default_job_manager – não foi possível identificar a funcionalidade concreta desta base de dados;
- mixpanel – base de dados relacionada com informações de análise, referente a serviço externo à *Vivino* para recolha de dados estatísticos sobre a utilização da aplicação;
- vivino-db – base de dados principal da aplicação.
- google_app_measurement – dados de metadata da aplicação

As mesmas contêm diversos tipos de informação, sendo que considerámos apenas relevantes as que contivessem informação com relevo forense, nomeadamente as que pudessem conter dados temporais, geográficos ou dados pessoais. Seguem-se a estrutura e descrição das tabelas recolhidas.

5) Estrutura da tabela events, base de dados google_app_measurement.db

Colunas	Descrição / tipos de dados
app_id	Id da aplicação
name	Nome do parâmetro
lifetime_count	Contador (talvez de modificações)
Current_bundle_count	Contador (talvez seja utilizado como agregador)
Last_fire_timestamp	última alteração de evento (datetime Unix epoch)
last_bundled_timestamp	Idêntico ao anterior (sem dados preenchidos)
last_bundled_day	(sem dados preenchidos)
last_sampled_complex_event_id	(sem dados preenchidos)
last_sampling_rate	(sem dados preenchidos)
last_exempt_from_sampling	(sem dados preenchidos)
current_session_count	(sem dados preenchidos)

Nesta tabela constam dados estatísticos (login, primeira foto, acesso e utilização de funcionalidades)

events

app_id	name	lifetime_count	current_bundle_count	last_fire_timestamp
vivino.web.app	_f	1	1	1683993615206
vivino.web.app	Authorisation__Launch	1	1	1683994176682
vivino.web.app	First_launch	1	1	1683994177749
vivino.web.app	SISU__Start_screen__Show	1	1	1683994182944
vivino.web.app	SISU__Start_screen__Email	1	1	1683994203533
vivino.web.app	SISU__Email_screen__Show	1	1	1683994203834
vivino.web.app	SISU__Email_screen__Continue	1	1	1683994267992
vivino.web.app	SISU__Email_validation__Request_Sent	1	1	1683994268023
vivino.web.app	SISU__Log_in_screen__Show	1	1	1683994269011
vivino.web.app	SISU__Log_in_screen__Log_in	1	1	1683994279244
vivino.web.app	Sign_in__Success	1	1	1683994280421
vivino.web.app	login	1	1	1683994280430
vivino.web.app	Settings__Button__NPS	2	2	1685120620360
vivino.web.app	First_photo	1	1	1685127457938

Figura 32 – Amostra dos dados presentes na tabela Events

6) Estrutura da tabela user_attributes, base de dados google_app_measurement.db

Colunas	Descrição / tipos de dados
app_id	Identificador da aplicação
name	Tipo de registo

set_timestamp	Datetime (Unix epoch)
value	Valor (referente ao tipo de registo)
origin	Origem (app/auto)

vivino.web.app	_id	1685791187717	63889273	app
vivino.web.app	vivino_user_id	1685791187717	63889273	app
vivino.web.app	vivino_email	1685791187717	ruilcsper@gmail.com	app
vivino.web.app	vivino_app_country	1685791187717	pt	app
vivino.web.app	database_size	1685791187718	2895872	app

Figura 33 – Amostra dos dados presentes na tabela user_attributes, onde está guardado o utilizador da App

X. Relevância forense dos dados recolhidos

Da análise efetuada podemos concluir que a aplicação recolhe um conjunto de dados limitado, fruto do cuidado em não perturbar no modelo de negócio assente na criação de uma comunidade que visa a troca de informações sobre vinho, produtores, regiões de origem e locais de compra e de consumo.

Do ponto de vista da segurança dos dados do utilizador, a aplicação apenas apresenta uma falha relacionada com a privacidade dos dados pessoais, não garantindo a cifragem da password associada à conta de utilizador, que é transmitida no momento da autenticação, antes da primeira utilização efetiva da aplicação.

A análise efetuada às fotografias também não permitiu detetar qualquer indício que as mesmas fossem enviadas para vários servidores contendo informação EXIF com PII.

No entanto, o campo de "dados biográficos" presente na caracterização do utilizador, que podem ser preenchidos por este com informação pessoal, por estarem a ser enviados para fora da EU, pode ser considerado exportação de dados pessoais.

A interligação a API de redes sociais para envio e receção de notificações de utilização, bem como notificar os contactos presentes nas listas do smartphone e redes sociais também é outro aspeto que foi identificado na análise, e que podem incorrer em violações dos direitos consagrados pelo Regulamento Geral de Proteção de Dados vigente na União Europeia.

XI. Conclusões

No decurso da realização deste trabalho de investigação sobre análise forense digital a dispositivos móveis, foi possível conhecer um conjunto de conceitos, técnicas e tecnologias que podem ser úteis não só para a análise forense, como também para robustecer a segurança das aplicações que venhamos a desenvolver, ou conhecer um pouco melhor as aplicações que utilizamos.

O recurso a ferramentas *open-source* demonstra que é possível efetuar um trabalho com algum grau de detalhe, embora se desconheça o que se poderia fazer com ferramentas utilizadas pelos profissionais de investigação criminal.

Não é possível dar resposta a quase todas as perguntas de âmbito forense ("o quê", "quem", "quando", "como", "onde" e "porquê"). Para a pergunta "quem", é possível identificar o utilizador de conta registado inicialmente, mas não podemos assegurar que seja esse o utilizador durante toda a utilização da aplicação. Para a pergunta "onde", apenas existe interação com funcionalidades de localização em partes específicas da aplicação (quando se pretende obter dados da compra para um determinado vinho), ou através de GeoIP, para os *trackers* de estatísticas (MixPanel).

Por último, consideramos que a aplicação escolhida continha poucos elementos relevantes em termos forenses e que coloquem em causa a proteção de dados pessoais que pudessem ser explorados, o que podemos considerar como um aspeto positivo de uma aplicação com bastantes utilizadores. Deste modo, podemos afirmar que o uso da aplicação não traz qualquer tipo de ameaça para os dados do utilizador, considerando que todos os dados comunicados com terceiras partes requerem consentimento explícito por parte do utilizador (por exemplo, na integração com as redes sociais e utilização dos contactos para promoção da aplicação).

XII. Bibliografia

[1] Vivino, "Vivino," [Online]. Available: https://www.vivino.com.

[2] V. Hendelmann, "The Vivino Business Model – How Does Vivino Make Money?," [Online]. Available: https://productmint.com/vivino-business-model-how-does-vivino-make-money/.

[3] B. Marr, "Vivino: Choose Your Next Great Wine With Big Data And Artificial Intelligence," [Online]. Available: https://www.forbes.com/sites/bernardmarr/2021/05/07/vivino-choose-your-next-great-wine-with-big-data-and-artificial-intelligence/?sh=64b3faac6b94.

[4] S. Damas, "Case Study: Vivino," [Online]. Available: https://www.adjust.com/resources/case-studies/vivino/.

[5] IPLeiria, LabCIF, "AndroidStudioEmulator-GUIconfig," [Online]. Available: https://github.com/LabCIF-Tutorials/AndroidStudioEmulator-GUIconfig.

[6] A. Pandey, "SSL Pinning in Android," [Online]. Available: https://mailapurvpandey.medium.com/ssl-pinning-in-android-90dddfa3e051.

[7] IPLeiria, LabCIF, "Tutorial: Android Network Traffic Interception," [Online]. Available: https://github.com/LabCIF-Tutorials/Tutorial-AndroidNetworkInterception.

[8] IPLeiria LabCIF, "ADB-Extractor," [Online]. Available: https://github.com/labcif/ADB-Extractor.

[9] Stripe, "Stribe Docs - Keys," [Online]. Available: https://stripe.com/docs/keys.

[10] Google, "Maps API Documentation," [Online]. Available:

https://developers.google.com/maps/documentation/javascript/get-api-key?hl=pt-br.

[11] Google, "Developers - API Explorer," [Online]. Available: https://developers.google.com/apis-explorer?hl=pt-br.

[12] "https://stripe.com/docs/keys," [Online].

[13] IPLeiria, LabCIF, "AndroidStudioEmulator-acquireAppsData," [Online]. Available: https://github.com/LabCIF-Tutorials/AndroidStudioEmulator-acquireAppsData.