**ROMÂNIA**

**MINISTERUL APĂRĂRII NAȚIONALE**

**ACADEMIA TEHNICA MILITARĂ**

**„FERDINAND I”**

**FACULTATEA DE SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ**

**Specializarea: Calculatoare și sisteme informatice pentru apărare**

**și securitate națională**



***Aplicație destinată telefoanelor mobile în vederea detecției conectării acestora la stații de***

***bază false care se interpun între terminalul mobil și stațiile de bază ale furnizorilor oficiali***

***de servicii GSM (IMSI CATCHER DETECTOR)***

CONDUCĂTOR ȘTIINȚIFIC:

**Col. conf. univ. dr. ing. BĂDOI ION**

ABSOLVENT:

**Ștefan OLTEANU**

Conţine \_\_\_\_\_\_\_\_\_\_\_ file

Inventariat sub nr\_\_\_\_\_\_\_

Poziţia din indicator: \_\_\_\_

Termen de păstrare: \_\_\_\_\_

**BUCUREȘTI**

**2020**

**ABSTRACT**

**REZUMAT**

**CUPRINS**

[1 INTRODUCERE 10](#_Toc39498573)

[1.1. Importanța temei alese 10](#_Toc39498574)

[1.2. Scopul și obiectivele lucrării 10](#_Toc39498575)

[1.3. Prezentarea metodologiei de cercetare 11](#_Toc39498576)

[1.4. Rezumatul lucrării pe capitole 11](#_Toc39498577)

[2 CLASIFICAREA STAȚIILOR DE BAZĂ ÎN FUNCȚIE DE LEGALITATE 12](#_Toc39498578)

[2.1. Reglementări cu privire la *Imsi Catcher* 12](#_Toc39498579)

[2.1.1. Utilizarea IMSI Catcher în afara legii 13](#_Toc39498582)

[2.2. Modalități prin care IMSI Catcher exploatează rețeaua 14](#_Toc39498583)

[2.2.1. Rețele de comunicații GSM 14](#_Toc39498584)

[2.2.2. Securitatea în GSM 15](#_Toc39498585)

[2.2.3. Tipuri de atacuri populare 16](#_Toc39498592)

[2.2.4. Modul de funcționare al IMSI Catcher-urilor 18](#_Toc39498593)

[3 SOLUȚII ȘI TEHNOLOGII FOLOSITE ÎN DETECTAREA UNEI STAȚII DE BAZĂ FALSE 22](#_Toc39498594)

[3.1. Soluții existente de detectare 23](#_Toc39498595)

[3.2. Prezentarea bazei de date OpenCellId 26](#_Toc39498596)

[4 DESCRIEREA APLICAȚIEI DEMONSTRATIVE 29](#_Toc39498597)

[6 BIBLIOGRAFIE 29](#_Toc39498598)

**LISTĂ DE FIGURI**

# INTRODUCERE

## Importanța temei alese

Dispozitivele de tip *Imsi Catcher* există încă din anul 1993(1)însă erau mari, greoaie și mai ales scumpe. Datorită acestui lucru și a faptului că existau puțini producători, aceste dispozitive nu au fost folosite decât de unele agenții guvernamentale. În zilele noastre, apariția SDR-urilor[[1]](#footnote-2) a permis crearea unor proiecte de acasă și astfel înmulțirea atacurilor asupra rețelelor GSM. Mai mult, dacă inițial aceste atacuri au fost dezvoltate pentru a putea captura codurile IMSI[[2]](#footnote-3) de la telefoanele din apropiere – de unde vine și numele atacului -, versiunile actuale oferă posibilitatea de a intercepta atât apeluri telefonice cât și mesaje.

Prin urmare, această temă este cu atât mai importantă, cu cât nu există modalități de detectare a acestor atacuri, disponibile publicului larg. De asemenea, intrucât numarul acestora a fost în continuă creștere, este necesară informarea persoanelor cu privire la riscurile la care se expun în momentul în care telefonul se conectează la o stație de bază ce nu aparține unui furnizor de servicii local. Un articol realizat de cei de la Washington Post arată că numărul dispozitivelor de interceptare ilegale, găsite în oraș pe parcursul a mai puțin de două zile, este de aproximativ 18 (2). Așadar, nevoia unei aplicații care să ajute la detectarea acestor atacturi ce pun în pericol drepturile societății, este mai mult decât evidentă.

## Scopul și obiectivele lucrării

Scopul acestei lucrări de licență este acela de a expune problematica atacurilor de tip *Imsi Catcher*, de a evidenția modalități de detecție și nu în ultimul rând de a crea o aplicație Android funcțională care să pună în practică modalitățile precizate mai sus.

Printre obiectivele care trebuiesc atinse pe parcursul rezolvării acestei teme se numără un număr de informații cu ajutorul cărora cititorul iși poate face o idee complexă despre modul de funcționare atât a dispozitivului cu care se realizează atacul cât și a dispozitivului de interceptare. De exemplu:

* informații despre modul în care o rețea GSM functionează și ce puncte slabe are;
* prezentarea pe larg a modalităților prin care un dispozitiv *Imsi Catcher* exploatează rețeaua și reușește să capteze atât locația utilizatorului cât și mesaje sau apeluri telefonice;
* descrierea metodelor folosite în cadrul aplicației pentru a detecta atacul;
* s.a.m.d.

Obiectivul principal este ca la finalul lucrării să se poată demonstra cum se realizează atacul și detecția prin simularea unei stații de bază GSM care să preia semnalul telefonului mobil. Acesta din urmă va trebui să detecteze că celula[[3]](#footnote-4) la care este conectat nu aparține furnizorului de telefonie mobilă la care utilizatorul este abonat.

## Prezentarea metodologiei de cercetare

## Rezumatul lucrării pe capitole

# CLASIFICAREA STAȚIILOR DE BAZĂ ÎN FUNCȚIE DE LEGALITATE

## Reglementări cu privire la *Imsi Catcher*

Aceste dispozitive folosite în mare parte de agențiile de securitate statală au ridicat probleme în legătură cu libertatea și intimitatea civilă. De aceea folosirea acestora se realizează numai conform regulilor scrise în *Codurile de Procedură Penală* (3)*.*

Orice utilizare a unui dispozitiv de tip *Imsi Catcher* se realizează sub jurisdicția *Convenției Europene a Drepturilor Omului,* care stabilește un nivel minim de protecție atât pentru viața privată a individului cât și pentru corespondența acestuia (4). Toate aceste legi ar trebui să analizeze foarte bine comportamentul dispozitivelor, întrucât acestea nu sunt folosite numai pentru monitorizarea prezenței telefoanelor mobile într-o anume zonă, având ca scop identificarea locației pe hartă a acestora, ci și pentru a aduna informații despre utilizatori sau despre dispozitivele pe care aceștia le folosesc.

Pe lânga drepturile descrise mai sus, pe care un astfel de atac ar putea să le încalce, se mai adaugă și încălcarea dreptului la libertatea întrunilor pașnice. Există numeroase modalități prin care acest lucru este posibil, cum ar fi (5):

* persoanele ce cunosc modul de operarare ale acestor tipuri de dispozitive, nu vor mai participa la întalniri, proteste sau orice altă manifestare pașnică deoarece vor ști că prin captarea comunicațiilor mobile, aceștia pot fi urmăriți;
* prin captarea, editarea și rutarea comunicațiilor, abilitatea persoanelor de a comunica între ele va fi alterată;
* în unele cazuri, este chiar posibil ca unele guverne să trimită mesaje tuturor telefoanelor mobile aflate în zona în care se desfășoară o întalnire pentru a intimida, manipula sau pentru a împrăștia utilizatorii.

Deși există o lege europeană care face referire la protejarea individului, nu există legi specifice pentru utilizarea acestor dispozitive. Guverne din Statele Unite ale Americii și Germania au stabilit legi și politici care limitează modalitățile în care agențiile statatale pot utiliza în mod legal dispozitive de tip *Imsi Catcher.* Mai mult, Judecătorii din SUA au impus restricții suplimentare. Câteva exemple referitoare la legile adoptate de Ministerul de Justiție din SUA cu privire la utilizarea *Imsi Catcher* vor fi expuse mai jos: (6)

* limitarea folorii acestor dispozitive numai pentru identificare;
* cererea supervizării interne pentru utilizarea acestora;
* nevoia unui mandat pentru utilizarea acestora în situații care nu sunt urgente sau excepționale.

În cazul Germaniei, *Imsi Catcher-urile* au fost supuse legilor federale încă din anul 2002, atunci când utilizarea acestora a fost autorizată ca urmare a atacurilor de pe 9/11 din Statele Unite ale Americii. Curtea de Justiție Germană are dreptul de a autoriza folosirea unui astfel de dispozitiv numai în cazul în care există dovezi clare că o crimă serioasă are loc. Mai mult, persoanele care sunt vizate de aceste dispozitive trebuie anunțate că au fost subiecții unui *Imsi Catcher*, fără a pune în pericol anumite aspecte ale investigației (6).



### Utilizarea IMSI Catcher în afara legii

Deși atât în Europa cât și în Statele Unite ale Americii există reglementări în legătură cu utilizarea acestui tip de dispozitive, guvernele, agențiile de securitate și anumite persoane rău intenționate le utilizează fără un mandat. Spre exemplu, în 2014, poliția din Florida a recunoscut că a folosit *Imsi Catcher-uri* de cel puțin 200 de ori fără a recunoaște acest lucru în fața judecătorilor sau a avea un mandat care să le permită folosirea acestui dispozitiv (7).

Ideea care ridică probleme în acest sens, este aceea că poliția nu folosește acest tip de dispozive numai pentru prindere criminalilor dar și pentru spionarea populației. Chiar dacă în SUA exista numeroase state care dețin astfel de dispozitive, utilizarea lor nu este una transparentă, fapt care a ridicat multe semne de întrebare, deoarece nu se știe dacă acestea au fost folosite cu un mandat sau nu (8).

Pe lângă poliție sau guverne, dispozitivele de tip *IMSI Catcher* sunt adesea folosite si de spioni statali pentru a intra în posesia unor date despre ofițerii de inteligență. Acest lucru este posibil prin identificarea codurilor IMSI ale telefoanelor acestor ofițeri, care sunt localizate 8 ore pe zi în același loc. (9)

## Modalități prin care IMSI Catcher exploatează rețeaua

Ținta unui *IMSI Catcher* este rețeaua GSM. Acest dispozitiv se infiltrează in rețeaua GSM printr-un atac de tip *man-in-the-middle[[4]](#footnote-5).* Practic, acesta reprezintă o antena falsă, ce este plasată între telefonul țintă si antena adevărată, a furnizorului de servicii. Chiar dacă standardele GSM oferă protecție împotriva riscurilor, datorită autentificării mutuale între dispozitiv și rețea, protocolul nu este sută la sută sigur, deoarece atacatorii pot declasa servicii cum ar fi 3G sau LTE în servicii de rețea non-LTE care nu au nevoie de această autentificare mutuală specificată mai sus.

În capitolele ce urmează vor fi prezentate detalii despre rețelele GSM, modul acestora de funcționare, securitatea lor cât și despre câteva tipuri de atacuri cunoscute. În final, după ce s-a descris cum funcționează rețelele GSM, se vor prezenta modalități prin care *IMSI Catcher-urile* exploatează rețeaua.

### Rețele de comunicații GSM

GSM sau *Global System for Mobile Communications,* standard folosit pentru a descrie protcoalele din a doua generație( 2G) de rețele celulare digitale, a fost pentru prima oara folosit în anul 1991 în Finlanda. În jurul anului 2010, acesta a devenit un standard global pentru comunicațiile mobile, operând în peste 193 de țări și teritorii. Pentru o bună funcționare a tuturor echipamentelor compatibile cu această rețea dar și interconectarea acestora într-un mod corespunzător, standardul pune la dispoziție 161 de recomandări. Toate aceste reguli privind sistemele și serviciile GSM sunt guvernate de ETSI( *European Telecommunications Standards Insitute)* (10)*.*

În Europa, standardul GSM folosește benzi de frecvență între 900 MHz și 1800 MHz pe când în Statele Unite ale Americii este folosită banda de 1900 MHz. Din această cauză, telefoanele mobile care pot opera pe ambele continente sunt numite *tri-band,* în timp ce acelea care operează doar în Europa sunt cunoscute sub denumirea de *dual band*. Deoarece standardul acceptă un maxim de 9,6 kbps se pot transmite doar voce sau un volum mic de date, cum ar fi mesaje text sau mesaje multimedia (11).

### Securitatea în GSM

Deși standardul GSM este considerat a fi cel mai sigur sistem de telecomunicații celulare din ziua de azi deoarece folosește autentificarea folosind o cheie pre-partajată și autentificare de tip întrebare-răspuns, acesta este vulnerabil la diferite tipuri de atacuri, fiecare din ele țintind o altă parte a rețelei.

Operatorii de telefonie mobilă sunt astfel obligați să asigure atât securitatea propriilor servicii dar și a clienților întrucât acestora le trebuie oferită garanția că nimeni nu le poate intercepta conversațiile sau să le detecteze locația. Cu toate acestea, o rețea sigură nu înseamnă o rețea care să îngreuneze apelurile telefonice sau transmisia de date. Astfel, principalele mecanisme de securitate folosite în standardul GSM sunt împărțite în 4 mari categorii (12):

**Autentificarea utilizatorului** se realizează printr-un mecanism de securitate de tipul întrebare-răspuns. Un număr random de 128 de biți este trimis către stația mobilă care la rândul ei calculează un răspuns pe 32 de biți bazat pe numărul primit dar și pe cheia de autentificare individuală. Criptarea acestui răspuns este realizată cu ajutorul algoritmului A3.

**Criptarea datelor și semnalului** se asigură că datele utilizatorilor, cum ar fi mesaje text dar și voce, sunt protejate împotriva interceptării. Procesul de criptare este îndeplinit cu ajutorul algoritmului A5. Tot procesul de comunicare începe, însă, printr-o cerere la rețeaua GSM pentru a specifica modul de criptare. Astfel, operatorul de rețea este cel care decide modul în care se va desfășura întregul proces de comunicare. Mai mult, cheia de criptare este schimbată la intervale regulate de timp pentru a face rețeaua chiar mai rezistentă la interceptări. Calculul acestei chei are loc în interiorul SIM-ului și astfel această informație nu va fi niciodată divulgată de SIM.

**Confidențialitatea identității utilizatorului** asigură securitatea IMSI[[5]](#footnote-6) prin faptul că într-o comunicație GSM, codul IMSI este comunicat rar. Este mult mai sigur să se folosească un cod TMSI[[6]](#footnote-7) pentru a evita descoperirea identității unui utilizator al rețelei. Acest lucru presupune că un atacator ce interceptează comunicația nu va putea afla dacă un anume telefon mobil se află în aria căutată.

**Cartela SIM** asigură securitatea prin simplul fapt că în cazul pierderii, aceasta va cere un cod PIN pentru a putea fi folosită. Metoda este utilă doar în cazul în care codul PIN este activat și cel implicit a fost schimbat de către deținătorul cartelei.



**Fig. 2.2.2.a: Conectarea la o stație de bază**



### Tipuri de atacuri populare

În majoritatea tipurilor de atac cunoscute, atacatorul trebuie să pretindă că este ori o stație de bază pentru terminalul mobil, ori o stașie mobilă pentru celula la care dorește a se conecta. Aceste tipuri de atac sunt cunoscute, așa cum am menționat și în capitolul anterior, sub numele de *man-in-the-middle.* Atacurile asupra unei rețele GSM pot fi atât active cât și pasive, dar un atac activ le implică pe amândouă.

Înainte de un atac activ, atacatorul trebuie să asculte și să învețe din ce este formată informația pe care stația mobilă o trimite stației de bază. În momentul în care s-a infiltrat între cele două stații, atacatorul va avea posibilitatea să controleze toate mesajele care sunt trimise către telefonul mobil. După ce a furat identitatea utilizatorului, acesta poatre trimite mesaje false în numele acestuia.



**Fig. 2.2.3.a: Mecanismul unui atac Man-in-the-Middle** (12)

Mai jos, vor fi prezentate două din cele mai populare tipuri de atac asupra rețelelor GSM, după cum urmează (12):

**Atacul asupra anonimității utilizatorilor GSM**

Pentru a putea localiza un abonat GSM, atacatorul se poate folosi de momentul în care celula inițiază procedura de identificare a utilizatorului, care se inițializează numai în cazul în care rețeaua nu poate identifica stația mobilă folosind un TMSI. Dacă atacatorul deține tehnologiile necesare pentru a se da drept o stație de bază, este suficient de ușor să ceară codul IMSI unui telefon mobil.

În momentul în care un atacatorul deține codul IMSI al victimei, acesta poate abuza de procedura de identificare prin cererea unui cod TMSI. Terminalul mobil nefiind conștient de faptul că este conectat la o stație de bază falsă, îl va comunica și astfel locația îi poate fi dezvăluită deoarece antena falsă va putea face cereri țintite către terminalul ce deține codurile IMSI/ TMSI.

**Atacul asupra algoritmului de autentificare**

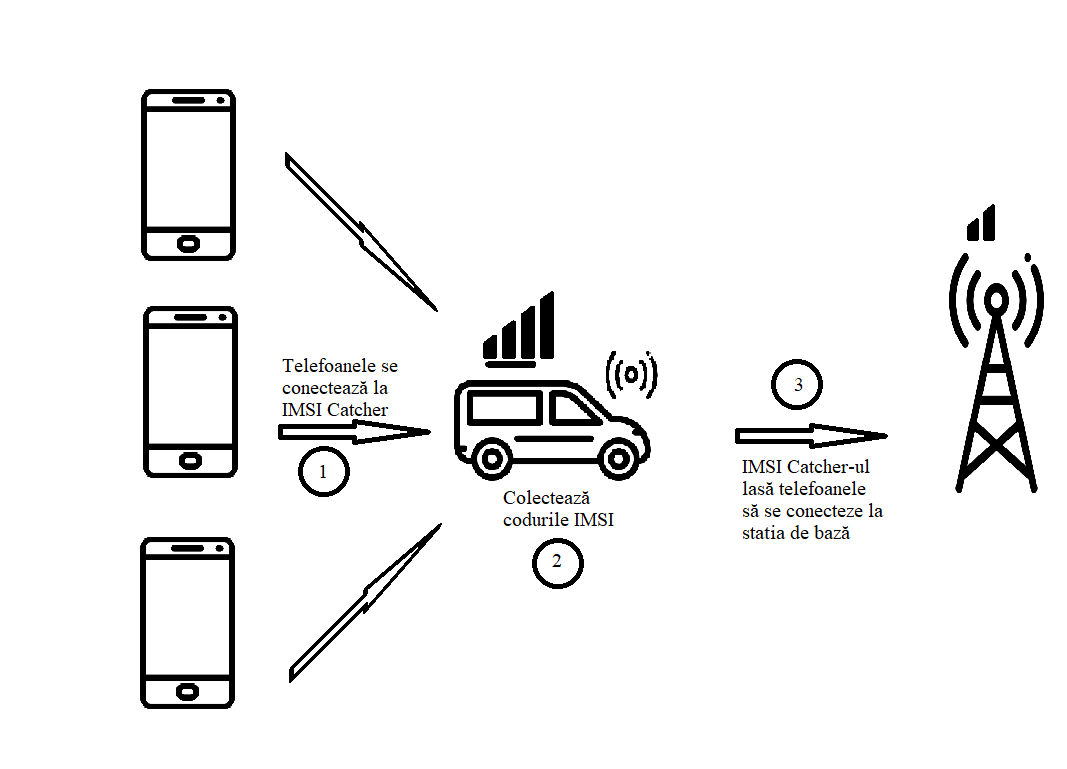
Majoritatea operatorilor GSM folosesc algoritmi de criptare ce sunt recomandați în GSM MoU[[7]](#footnote-8) în loc să își creeze algoritmi proprii pentru autentificare și generare de chei. Acest lucru se întâmplă datoriă imposibilității schimbării tuturor cartelelor SIM ce conțin algoritmii de criptare dar și a costurilor implicate de aceste schimbări.

Acest atac presupune clonarea unei cartele SIM originale, ce se poate face atât fizic cât și prin intermediul aerului. Astfel, din momentul în care atacatorul a reușit să copieze cheia secretă și codul IMSI într-o cartelă goală, se poate infiltra în rețea. În final, ținta atacului își va pierde intimitatea în rețeaua GSM întrucât îi vor fi decriptate toate apelurile.

### Modul de funcționare al IMSI Catcher-urilor

În rețelele GSM, telefoanele mobile vor încerca să se conecteze la stația de bază care oferă cel mai puternic semnal. Odată ce telefonul a identificat stația de bază cu semnalul cel mai bun, poate începe conectarea la aceasta. Cum celulele GSM au posibilitea să ceară telefoanelor să oprească criptarea datelor, la fel și un dispozitiv IMSI Catcher poate face acest lucru.

Următorul pas în conectarea la o stație de bază este identificarea terminalului mobil. Telefonul reușește să se identifice în rețea printr-un cod IMSI care se află stocat pe cartela SIM primită de la furnizorul de servicii. În momentul în care un dispozitiv malițios s-a infilitrat în rețea, acesta preia codul primit de la telefon după care se retrage pentru a permite telefonului să se întoarcă în rețea. Acesta este modul de bază în care un IMSI Catcher preia codul IMSI al telefonului dar de aici se poate continua cu diferite atacuri mai sofisticate.



**Fig. 2.2.4.a: Modul de operare al unui IMSI Catcher**

Odată obținute codurile IMSI, atacatorul poate porni un atac activ, și anume să fure identitatea în rețea a victimei. Pentru a realiza acest lucru, persoana rău intenționată trebuie să parcurgă doi pași principali (13):

**Autentificarea în rețea**

1. Atacatorul se conectează la celula de bază cu un răspuns la *Location Update Request*( cerere periodică făcută de antenă tuturor telefoanelor pentru a putea ruta apeluri și SMS-uri rapid).
2. Ca urmare a acestui răspuns, stația de bază îi cere dispozitivului malițios să se autentifice în rețea folosind o *Cerere de autentificare.* Bineînțeles, acesta va răspunde folosind codul IMSI furat anterior.
3. În acest moment, stația de bază va cere IMSI Catcher-ului să rezolve o problemă criptografică folosind o cheie privată. Cum nu are acces la cheia respectivă, ea fiind stocată pe cartela SIM a telefonului, acesta va pasa problema telefonului, care o va rezolva și va da înapoi răspunsul.
4. În final, este acceptată conexiunea între dispozitivul malițios și rețea.

Acest lucru este însă posibil numai la nivelul rețelelor 2G. Cu toate acestea, atacatorii cu experiență au posibilitatea de a degrada conexiunea telefonului de la 3G/ 4G la GSM. Posibilitatea se bazează pe faptul că stația de bază poate alege ce configurație dorește și să o impuna telefonului. Mai mult, telefonul poate decide singur să degradeze conexiunea în momentul în care benzile de conexiune 3G sau 4G sunt prea aglomerate sau există prea mult zgomot pentru a reuși să realizeaze o conectare sigură.

**Rezolvarea problemei criptării**

După cum am specificat anterior există mai mulți algoritmi folosiți în GSM, aceștia având nume precum: A5/1, A5/2 etc ... iar A5/0 înseamnă ca nu este folosită nici o modalitate de criptare.

Există două posibilități în acest caz. Rețeaua poate specifica telefonului să comunice folosind criptare, iar dispozitivul malițios să răspundă ca nu are capabilități de criptare. În al doilea rând, rețeaua poate stabili să folosească un anume algoritm dar acestea pot fi de obicei sparte în timp real. În ambele cazuri, în acest punct, atacul este complet iar atacatorul poate citi mesajele în clar dintre telefon și stația de bază.

Cele doi pași prezentați mai sus fac referire la momentul în care un dispozitiv *IMSI Catcher* este utilizat pentru a intercepta comunicarea dintre telefonul mobil și stația de bază la care s-a conectat. Deși este o problemă gravă, adevărata problemă o reprezintă urmărirea locației în timp real. Astfel, chiar și acest tip de atac se împarte în două categorii (13):

**Verificarea prezenței**

Pentru acest tip de atac nu este nevoie ca atacatorul să pretindă că este o celulă de bază ci poate folosi echipamente precum un SDR și un laptop pentru a monitoriza semnalele din zona sa.

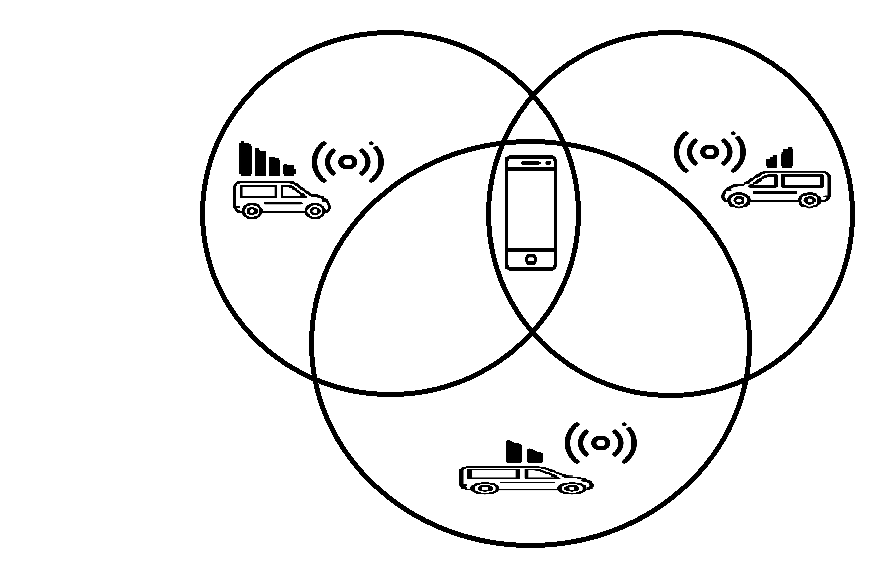
Acest lucru este posibil deoarece în cazul tehnologiilor fără fir se utilizează mesaje de tip RRC[[8]](#footnote-9). În momentul în care rețeaua are de trimis un mesaj și dorește să îl direcționeze către un telefon, trimite un mesaj RRC care este primit de toate telefoanele din zona de interes, cerându-i telefonului țintă să contacteze stația de bază pentru a realiza conexiunea și a primi apelul sau mesajul. Astfel, telefoanele monitorizează permanent aceste mesaje, le primesc și le dau la o parte pe cele care nu le sunt adresate.

În cazul în care numărul de telefon al victimei este cunoscut, acest procedeu prezentat mai sus poate fi forțat prin trimiterea unui SMS către aceasta. Rețeaua va putea fi monitorizată pentru a capta momentul de timp în care telefonul se conectează la stația de bază pentru a prelua mesajul.

**Dobândirea locației exacte( coordonate GPS)**

În acest scenariu, atacatorul a reușit să atragă telefonul să se conecteze la stația lui falsă, folosind metodele prezentate mai sus. Dispozitivul malițios are acum posibilitatea de a trimite o comandă telefonului prin care îi trimite id-urile a cel puțin 3 celule din apropiere și frecvențele acestora de conectare. Telefonul primește această comandă și îi întoarce dispozitivului malițios puterile semnalului oferit de fiecare dintre celulele cerute. Poziția dispozitivului țintă este apoi calculată prin triliterație, în cazul telefoanelor mai vechi, iar în cazul unora mai noi, răspunsul dispozitivului conține și coordonatele exacte ale acestuia.

Triliterația, diferită de triangulație, presupune calcularea intersecției cercurilor desenate în jurul fiecărei celule menționate în comanda pe care *IMSI Catcher-ul* o dă telefonului. Raza fiecărui cerc este o funție ce depinde de puterea semnalului, pe care telefonul o trimite înapoi, ca răspuns, dispozitivului malițios.



**Fig. 2.2.4.b: Triliterația folosită ca metodă de calcul ale coordonatelor GPS ale telefonului țintă**

Un ultim tip de atac pe care un dispozitiv *Imsi Catcher* îl poate realiza asupra unei rețele este un atac de tipul *Denial of Service[[9]](#footnote-10).* Deși există metode simple de a realiza un astfel de atac, precum aglomerarea rețelei cu semnal alb, sunt folosite tehnici pentru atacuri DoS care țintesc telefoane individuale.

Un atac *denial of service* asupra unui singur dispozitiv prespune exact același procedeu ca în cazul degradării protoculului, acțiune ce a fost descrisă mai sus, cu excepția faptului că *IMSI Catcher-ul* va răspunde cu mesajul „serviciile LTE și non-LTE nu sunt permise”. Telefonul va intra într-o stare în care nu va mai realiza nici o conexiune cu rețeaua și nu va reveni la starea inițială decât în momentul în care va fi repornit (13).

# SOLUȚII ȘI TEHNOLOGII FOLOSITE ÎN DETECTAREA UNEI STAȚII DE BAZĂ FALSE

Există numeroase soluții prin care se poate detecta existența unui dispozitiv malițios de tip IMSI Catcher însă nici una nu poate opri telefonul de la a se conecta la aceste antente false. Utilizatorul poate fi anunțat, poate primi rapoarte în legătură cu activitatea telefonului de la diferite aplicații dar din păcate nu poate fi ferit de atacatori. Acest tip de aplicații se bazează pe colecționarea de date de la mediul înconjurător și analizarea acestora pentru a lua o decizie în funcție de rezultatele obținute. Datele colecționate se obțin atât de la antenele ce aparțin furnizorilor de telefonie mobilă cât și de la presupuși atacator, acest lucru ajutând la compararea parametrilor între ei.

Așadar, în acest capitol se va discuta despre detectoare *IMSI Catcher*, despre tehnicile de detectare iar în final se va realiza și o evaluare a acestora pentru a stabili cât sunt de eficiente. Prima metodă, rudimentară, dar care poate fi folosită de oricine dispune de un telefon mobil pentru a detecta dacă s-a conectat sau nu la o antenă falsă este încercarea de a iniția un apel. Deoarece antena nu este înregistrată într-o rețea de telefonie mobilă, această încercare nu va a avea succes. De asemenea, telefonul respectiv nu se va putea conecta la internet și nu va putea primi sau trimite mesaje de tip SMS.

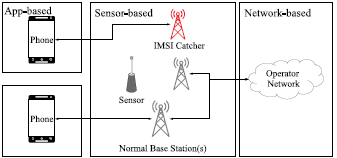
Soluția prezentată poate fi încercată dar nu garantează rezultate corecte deoarece atacul nu durează pentru o perioadă lungă de timp. În cele mai multe cazuri telefonul se conectează la dispozitivul malițios, după care este respins de acesta în momentul în care a obținut datele dorite. Acest lucru înseamnă că verificarea trebuie facută atunci când telefonul își schimbă antena curentă pentru o antenă cu semnal mai bun.

După cum a fost menționat mai sus, prima metodă nu va oferi întodeauna rezultate clare dacă este utilizată individual și mai ales dacă este utilizată de persoane fără un bagaj de cunoștințe în acest domeniu al rețelelor de telefonie. Poate fi de folos în cadrul unor aplicații care utilizează și alte modalități, iar rezultatele fiecărui test în parte sunt analizate și vor rezulta într-un răspuns mai complex. Astfel, în subcapitolul ce urmează vor fi prezentate câteva metode existente de detecție ale dispozitivelor malițioase de tip *IMSI Catcher*.

## Soluții existente de detectare

Acest subcapitol al prezentei lucrări se va axa pe diferite metode de detecție ale dispozitivelor *IMSI Catcher*, încercând să evalueze punctele tari și punctele slabe ale acestora. Astfel, detectoarele care urmează a fi descrise pot fi împărțite în trei mari categorii, după cum urmează (14):

* detectoare ce folosesc aplicații mobile
* detectoare ce folosesc senzori
* detectoare ce utilizează rețeaua de telefonie



**Fig. 3.1.a: Cele trei metode de detecție prezentate** (14)

În continuare, se va lua fiecare metodă în parte pentru a fi analizată (14).

**Detectoare ce folosesc aplicații mobile**

Acest tip de aplicații pot fi regăsite pe diferite platforme cum ar fi *Google Play[[10]](#footnote-11)* sau *AppStore[[11]](#footnote-12)* sub formă gratuită sau cu bani. Acestea utilizează și sunt limitate în acest sens de către bibliotecile, referitoare la rețeaua de telefonie mobilă, puse la dispoziție de sistemele de operare și se bazează doar pe informațiile pe care smartphone-ul le vede în rețea și le pune la dispoziția acestora. Putem afirma, de asemenea, că sunt limitate și de dispotivul fizic. Pe lângă aceste informații, pentru o detecție îmbunătățită, pot utiliza și baze de date publice ce conțin locațiile stațiilor de bază, cum ar fi *OpenCellId.*

Modul de funcționare al acestor aplicații se bazează pe faptul că deși dispozitivele *IMSI Catcher* pot fi configurate astfel încât să fie cât mai asemănătoare cu o stație de bază reală, anumiți parametri nu pot fi aceeași, tocmai pentru a induce telefonului că trebuie să se conecteze la acestea. Astfel, acest tip de detectoare salvează într-o bază de date proprie configurația fiecărei celule cu care interacționează telefonul mobil, pentru ca mai apoi să avertizeze utilizatorul dacă anumiți parametri nu se potrivesc sau dacă există prea multe diferențe între celula curentă și cele vecine. Utilizatorul dispozitivului mobil, va putea primi notificări în timp real, la scurt timp după ce telefonul acestuia s-a conectat la o stație de bază falsă.

Pentru utilizatorii ce doresc și mai multă intimitate în rețea, există un dispozitiv mobil, numit *Cryptophone*, care conform descrierii produsului garantează apeluri telefonice și mesaje securizate și mai mult, vine cu o aplicație de tip *Imsi Catcher Detector* deja instală. Potrivit unor evaluări (14), utilizarea unui astfel de telefon pentru detecție a dat aceleași rezultate, sau chiar mai bune decât în cazul utilizării unei aplicații gratuite. Acest lucru se datorează faptului că un *Cryptophone* utilizează anumiți parametri care nu sunt disponibili aplicațiilor obișnuite și mai mult în caz de detecții acesta poate trimite rezultatele către sistemul *GSKM Overwatch[[12]](#footnote-13)* pentru o analiză amănunțită.

Așadar, luând în considerare cele prezentate mai sus, se poate afirma că unul din avantajele folosirii unei astfel de aplicații este acela că poate informa utilizatorul în cel mai scurt timp că a fost victima unui atac. Pe de altă parte, dezavantajele sunt reprezentate de limitările telefonului referitoare la detaliile pe care le obține de la antena la care se conectează, cum ar fi locația exactă a acesteia, pe care o poate afla numai conectându-se la surse externe, adică baza de date publică menționată anterior. Mai mult, nu este de neglijat nici faptul că o astfel de aplicație este o mare consumatoare de baterie, lucru care nu este tocmai plăcut pentru utilizatorul obișnuit.

**Detectoare ce folosesc senzori**

Detectoarele bazate pe senzori, sunt ori dispozitive mobile pasive, ori un senzor integrat într-o stație de bază care monitorizează în continuu stațiile de bază din împrejurimi. Detecția continuă, care acoperă o zonă mare, este de dată de faptul că aceste dispozitive sunt fixe și monitorizează în același timp rețelele, urmărind diverși factori cum ar fi apariții ale unor noi stații de bază, durata de viață a acestora sau diverse anomalii de configurare.

Unii senzori funcționează activ în rețea, devenind *honeypot-uri[[13]](#footnote-14).* Astfel, modul de funcționare al acestori senzori se bazează pe o conexiune cu stația de bază, pentru ca mai apoi să poată analiza toate mesajele pe care antena le schimbă cu terminalul mobil. Acesta poate detecta lipsa serviciilor de telefonie mobilă, despre care am discutat la începutul capitolului, sau dacă schimbul de mesaje se realizează într-un mod criptat, lucru care nu se întâmplă în cazul *IMSI Catcher-urilor.* Rezultatele analizei sunt transmise mai apoi către operatorul de rețea.

Principalele avantaje ale aceste tehnici de detecție sunt:

* dimensiunea antenei, ce ajută la observarea unor zone mai largi decât în cazul telefoanelor mobile;
* se poate realiza o analiză pe o durată mai lungă de timp și astfel rezultatele vor fi mai concludente;
* se axează numai pe detecție, neavând procese ce rulează în același timp, care pot afecta capacitatea de analiză a mesajelor schimbate cu stația de bază.

Durata de timp îndelungată pe parcursul căreia se realizează analiza poate reprezenta de asemenea un dezavantaj deoarece nu poate împiedica atacurile unui *IMSI Catcher*, care își va fi terminat atacul cu mult timp înainte să fie detectat.

**Detectoare ce utilizează rețeaua de telefonie**

Acest tip de detectoare utilizează, după cum îi spune și numele, informațiile colectate de rețea, neavând nevoie să realizeze măsurători suplimentare pentru detecția *IMSI Catcher-urilor.*

Informațiile pe care rețeaua de telefonie mobilă se bazează pentru a detecta dispozitivele malițioase sunt numeroase, dar un exemplu ar fi puterea semnalului care poate fi preluată de la telefon și comparată cu cea pe care celula o emite, astfel identificând prezența și locația unui *IMSI Catcher.* Mai mult, având drepturi depline asupra rețelei, administratorii pot interzice telefoanelor să se conecteze la dispozitivele utilizate pentru atacuri.

Așadar, informațiile actualizate pe care operatorul de rețea le obține atât de la terminalele mobile , cât și de la antenele sale reprezintă un mare avantaj în detecția atacurilor. Cu toate acestea, unul dintre dezavantaje constă în faptul că identificarea dispozitivului se realizează prea tărziu, la fel ca în cazul detectoarelor ce utilizează senzori, abia după ce telefonul mobil a fost deja ținta unui atac. Mai mult, operatorul de rețea nu poate stabili nu poate stabili cât de grave au fost consecințele atacului, adică dacă atacatorul a dezactivat criptarea datelor pentru interceptarea informațiilor.

O modalitate prin care aceste metode de decție ar da rezultate mult mai concludente, ar fi utilizarea unei combinații ale acestora. Un bun exemplu ar fi utilizarea unui senzor împreună cu o aplicație deoarece primul poate da informații la care al doilea tip de detector nu are acces, cum ar fi momentul în care rețeaua de telefonie decide să declaseze nivelul rețelei. Dacă senzorul ar detecta o ca deși există o conexiune 4G într-un loc dar cu toate acestea celula la care este conectat declasează nivelul de la 4G la 2G, acesta este un semn ca un *IMSI Catcher* se află în preajmă, informație care ar putea fi trimisă catre aplicația mobilă. Problema care stă la baza acestei soluții este faptul că, momentan, senzorii utilizează rețeaua de internet pentru a putea transmite informațiile referitoare la dispozitivele malițioase. Aplicația mobilă nu poate primi nici un mesaj în timp real atunci când atacul se află în desfășurare. Soluția care poate rezolva problema este utilizarea și celei de a treia metode, cu ajutorul căreia se poate interzice telefonului să părăsească anumite celule pentru unele cu semnal mult mai puternic.

## Prezentarea bazei de date OpenCellId

Deoarece aplicația dezvoltată în cadrul acestui proiect, se bazează efectiv pe datele obținute din telefon, a fost necesară utilizarea unei baze de date publice pentru obținerea informațiilor veridice despre celule.

Acestă bază de date conținea (15) în 21 august 2017 în jur de 35.5 milioane de celule unice, ceea ce o face potrivită pentru verificarea informațiilor pe care antena la care se conectează terminalul mobil le face publice. Este de înțeles că unele celule pot lipsi și de aceea analiza realizată la nivelul aplicației nu se bazează doar pe aceste date, adică, în cazul în care datele unei stații de bază nu se găsesc, aplicația nu va eticheta acea stație ca fiind un *IMSI Catcher* ci o va cataloga ca activitate suspicioasă, până stabilirea unei decizii finale.

Conectarea și obținerea datelor necesare analizei se realizează cu ajutorul unui api pus la dispoziție de firma ce a creat baza de date. Astfel, pentru a trimite cereri se poate utiliza unul din endpointurile listate în documentația api-ului. Programatorul îl poate folosi pe oricare, însă recomandarea este să îl folosească pe acela care este cel mai apropiat din punct de vedere geografic pentru a minimiza latența. În cadrul proiectului am utilizat serverul de mai jos:

* <https://eu1.unwiredlabs.com/v2/process.php>

Tot în documentația api-ului este prezentată modalitatea în care trebuie realizată cererea și cum va arăta răspunsul primit de la server.



**Fig. 3.2.a: Cerere și răspuns api OpenCellId**

În continuare vor fi detaliați fiecare parametri pe care aplicația trebuie să îi pună la dispoziție pentru a putea primi un răspuns pozitiv înapoi.

* token – cheia pentru a putea accesa api-ul ce se poate obține de pe site-ul producătorului
* radio – tipul celulei pe care dorim să o căutam. În cazul de față nu vom utiliza decât GSM
* mcc – codul țării în care este înregistrată cartela SIM
* mnc – codul operatorului de telefonie mobilă din țara în care este înregistrată cartela SIM
* lac – codul locației în care se află celula căutată
* cid – codul de identificare a celulei

Ca răspuns api-ul întoarce statusul cerererii, *ok* însemnând că cererea a fost tratată cu succes. În caz contrar, mesajul *error* va apărea la câmpul *status*. Mai mult, răspunsul conține numărul de cereri care se mai pot trimite către api iar în cazul în care statusul este unul negativ, acestea nu se iau în considerare. În continuare, sunt furnizate clientului detalii despre locația celulei, cum ar fi latitudinea și longitudinea precum și adresa exactă.

Toate datele primite de la server sunt preluate de aplicația client și afișate utilizatorului, iar dacă celula nu există acesta va fi înștiințat de faptul că în zona sa poate exista un dispozitiv malițios de tip *IMSI Catcher*, rezultatul final urmând să fie stabilit prin efectuarea tuturor testelor din cadrul aplicației.

În cadrul aplicației dezvoltate a fost utilizat un *HttpRequest*, metoda *Post*, care a primit ca parametru un *Json* în care au fost introduse toate datele cerute de către api. Răspunsul primit, a fost tot sub forma unui obiect Json și a fost parsat tot în cadrul clasei ce realizează cererea pentru a putea salva informațiile, ce urmează a fi folosite în aplicație pentru analiză sau pentru informarea utilizatorului.



**Fig. 3.2.b: Pornirea conexiunii http și crearea obiectului Json**

Toate apelurile metodelor de mai sus se realizează în mod asincron pentru a nu interfera cu restul operațiilor ce se execută în cadrul aplicației. Pe lângă faptul că mediul de lucru nu permite executarea sarcinilor de acest tip pe firul principal de execuție, a fost nevoie de o astfel de abordare deoarece se execută un număr mare de cereri de care utilizatorul nu este conștient, fapt care ar fi însemnat blocarea aplicației.

# DESCRIEREA APLICAȚIEI DEMONSTRATIVE

Prezentul capitol al acestei lucrări își propune descrierea aplicației ce pune în practică o parte din noțiunile teoretice prezentate anterior în acest document. Astfel, se vor descrie mediul de lucru utilizat pentru dezvoltarea aplicației informatice, tehnicile de programare folosite, câteva principii care au fost respectate în ceea ce privește design-ul aplicației și pașii urmați în analiza datelor pe care celula la care telefonul se conectează le furnizează.

Capitolul se va încheia cu prezentarea modului de funcționare al aplicației, simulând detectarea unei stații de bază false. Rezultatele simulării vor fi expuse sub forma unor figuri și comentarii pe baza acestora care să ateste faptul că modul de funcționare al programului este unul corespunzător.

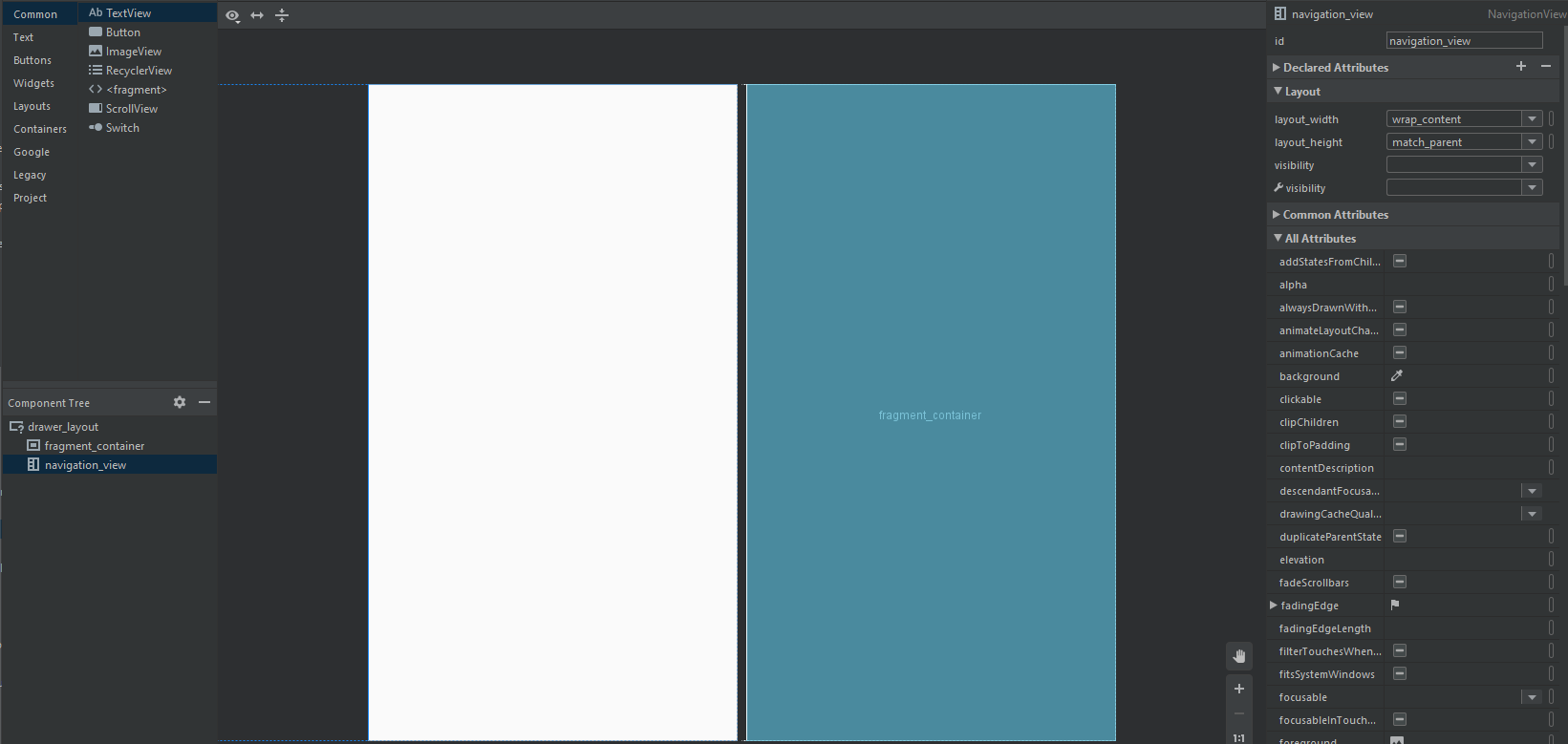
## Prezentarea arhitecturii și descrierea mediului de lucru

### Descrierea mediului de lucru

Aplicația informatică, numită sugestiv *Imsi Catcher Detector*, a fost dezvoltă cu ajutorul unui mediu de dezvoltare, numit Android Studio, pus la dispoție de Google. Acest *IDE[[14]](#footnote-15)* este specializat pe dezvoltarea de aplicații pentru sistemul de operare Android și este utilizat încă din anul 2013, atunci când a fost anunțat de Google într-o conferință (16).

Android Studio îmbină editarea vizuală bazată pe fișiere xml cu limbajele de programare Java sau Kotlin. Mai mult, acesta pune la dispoziția programatorilor un emulator pe care aceștia pot rula sau depana aplicațiile, nefiind nevoie neapărat de un dispozitiv fizic.

Astfel, interfața grafică a programului dezvoltat în cadrul acestui proiect a fost realizată folosind editorul vizual menționat anterior, cu ajutorul cărora au fost adăgate componente grafice mai mult sau mai puțin complicate cum ar fi: texte, casete de text, tabele, hărți, liste etc. Parametrii fiecărei componentă în parte au fost modificați cu ajutorul editorului vizual, a fișierelor XML aferente fiecărui ecran din aplicație sau prin limbajul Java, întrucât fiecare componentă grafică are corespondent un obiect Java. Acest obiect, permite programatorului să modifice programatic felul în care componenta vizuală arată, locația acesteia din ecran precum și să definească comportamentul acesteia în funcție de anumite acțiuni ale utilizatorului. Mai mult, editorul vizual pune la dispoziție previzualizarea interfeței grafice a aplicației dar și modificarea dimensiunilor acesteia pentru a vedea cum se comportă pe ecrane diferite.



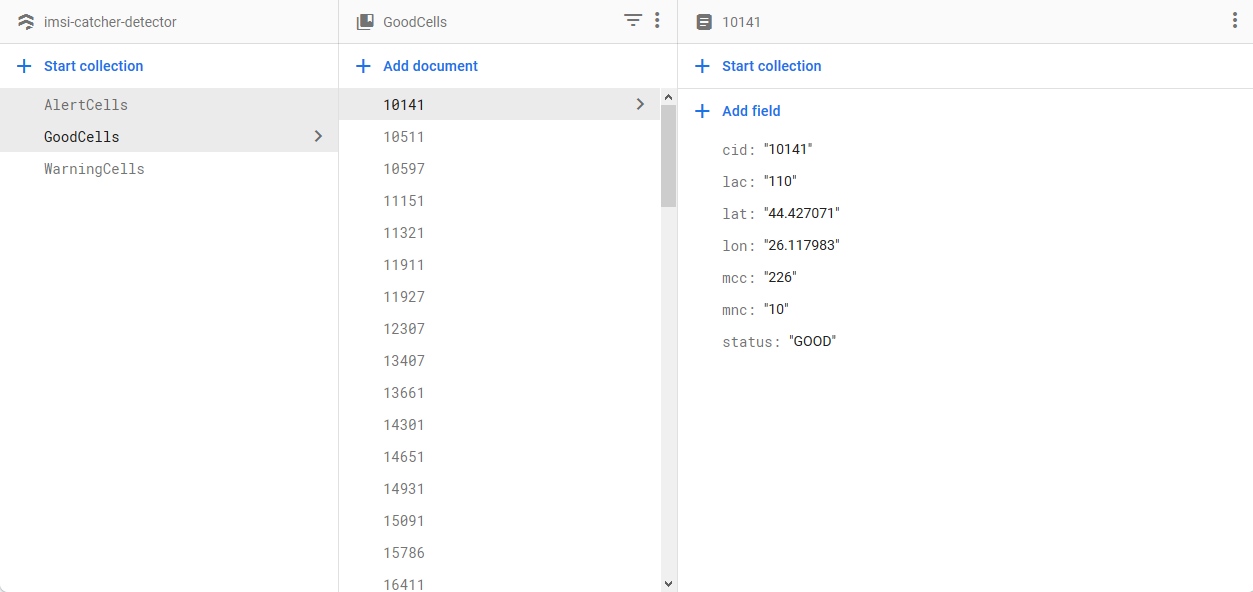
**Fig. 4.1.1.a: Editorul vizual din Android Studio**

Pe lângă dezvoltarea aplicației în Android Studio a fost nevoie de un server ce conține o bază de date care să fie accesibiliă tuturor dispozitivelor pe care aplicația rulează. Astfel, a fost utilizat serviciul celor de la Google numit Firebase ce pune la dispoziție un api cu ajutorul căruia datele pot fi sincronizate între toți utilizatorii aplicației. Modul de funcționare al acestei baze de date se bazează pe stocarea datelor sub forma unor colecții de date imbricate, pe care aplicațiile, fie ele mobile sau web, le pot accesa în mod asincron fără a bloca firul principal de execuție cât timp se realizează transferul de date.

Astfel, datele au fost organizate sub forma a 3 colecții denumite în funcție de tipul celulelor detectate:

* GoodCells – celule ce aparțin operatorilor de telefonie mobilă
* WarningCells – celule despre care încă nu se cunoaște dacă sunt stații de bază sau dispozitive malițioase
* AlertCells – dispozitive de tip *IMSI Catcher*

Fiecare intrare din colecție este denumită în funcție de id-ul celulei, asigurând așadar unicitatea intrărilor din baza de date. Fiecare document din colecție conține informații precum id, local area code, latitudine, longitudine etc.



**Fig. 4.1.1.b: Intrările din baza de date**

Baza de date este actualizată numai în cadrul aplicației în diferite momente de timp. Un prim caz în care se modifică este atunci când telefonul schimbă celula la care este conectat, moment în care stația de bază împreună cu toate celulele vecine declarate de aceasta sunt introduse în colecția corespunzătoare. Dacă aplicația are o suspiciune că antena ar putea fi un *IMSI Catcher*, datorată de faptul că nu există în baza de date publică, înainte de a face modificări în baza de date, aceasta verifică existența celulei respective în colecția *GoodCells*. Un alt caz de actualizare a datelor este atunci când după efectuarea analizei a rezultat că celula la care este conectat telefonul este un dispozitiv malițios, moment în care datele acelei celule vor fi introduse în colecția *AlertCells.*

# BIBLIOGRAFIE

1. *IMSI-Catch Me If You Can: IMSI-Catcher-Catchers.* **Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, Edgar Weippl.** 2014, ACSAC '14: Proceedings of the 30th Annual Computer Security Applications Conference, p. 10.

2. **Ashkan Soltani, Craig Timberg.** Tech firm tries to pull back curtain on surveillance efforts in Washington. *The Washington Post.* [Online] The Washington Post, 09 17, 2014. [Cited: 04 09, 2020.] https://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f\_story.html.

3. **Wikipedia.** Imsi-catcher. *Wikipedia.* [Online] 03 11, 2020. [Cited: 04 09, 2020.] https://en.wikipedia.org/wiki/IMSI-catcher.

4. **Naarttijärvi, Markus.** *Swedish police implementation of IMSI-catchers in a European law perspective.* Umeå : Computer Law & Security Review, 2016.

5. **International, Privacy.** *Privacy International’s contribution to the half-day general discussion on Article 21 of.* s.l. : Privacy International, 2019.

6. **Tamir Israel, Christopher Parsons.** *Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada.* Toronto : Telecom Transparency, 2016.

7. **Wikipedia.** Stingray phone tracker. *Wikipedia.* [Online] Wikipedia, 04 10, 202. [Cited: 04 13, 2020.] Stingray phone tracker.

8. **Lee, Timothy B.** The police are secretly using fake cellphone towers to spy on people. *Vox.* [Online] Vox, 04 22, 2015. [Cited: 04 13, 2020.] https://www.vox.com/2015/4/22/8463239/stingray-fbi-secret.

9. **Catherine Cullen, Brigitte Bureau.** Someone is spying on cellphones in the nation's capital. *CBC News.* [Online] CBC, 04 03, 2018. [Cited: 04 21, 2020.] https://www.cbc.ca/news/politics/imsi-cellphones-spying-ottawa-1.4050049.

10. **Wikipedia.** GSM. *Wikipedia.* [Interactiv] 13 09 2019. [Citat: 09 04 2020.] https://ro.wikipedia.org/wiki/GSM.

11. **xlxmarketing.** The Cell Phone Mysteries, What Are Dual Band, Tri Band And Quad Band Cell Phones And Where Will They Work? *Chinavasion.* [Online] Chinaviasion, 11 21, 2008. [Cited: 04 21, 2020.] https://blog.chinavasion.com/1099/the-cell-phone-mysteries-what-are-dual-band-tri-band-and-quad-band-cell-phones-and-where-will-they-work-part-2/.

12. **Korkusuz, Ammar Yasir.** *Security in the GSM Network.* Bogazici University, Electrical-Electronics Engineering Department : s.n., 2012.

13. **Lab, Threat.** *GottaCatch’EmAll:UnderstandingHowIMSI-CatchersExploitCellNetworks(Probably.* s.l. : Electronic Frontier Foundation, 2019.

14. **Shinjo Park, Ravishankar Borgaonkar,Altaf Shaik,Jean-Pierre Seifert.** *Anatomy of Commercial IMSI Catchers and Detectors.* London : RIGHTSLINK, 2019.

15. **Wikipedia.** OpenCellID. *Wikipedia.* [Online] Wikipedia, 04 06, 2020. [Cited: 05 04, 2020.] https://en.wikipedia.org/wiki/OpenCellID.

16. —. Android Studio. *Wikipedia.* [Online] Wikipedia, 04 27, 2020. [Cited: 05 04, 2020.] https://en.wikipedia.org/wiki/Android\_Studio.

17.

18. **GSMK.** GSMK. *NETWORK SECURITY.* [Interactiv] GSMK, 2017. https://www.gsmk.de/products/network-security/#overwatch.

1. Software Defined Radio – sistem de comunicare radio. Componente care în mod normal ar fi implementate hardware, precum amplificatoare, modulatoare sunt implementate pe partea de software. [↑](#footnote-ref-2)
2. International Mobile Subscriber Identity – cod alocat utilizatorului de către operatorii de telefonie, ce le permite să identifice abonatul in funcție de numărul de telefon. [↑](#footnote-ref-3)
3. Celulă – releu GSM ce deservește o mică suprafață, mai mult sau mai puțin rotundă si cu diametrul de aproximativ 8-10 kilometri. (10) [↑](#footnote-ref-4)
4. Atac man-in-the-middle – tip de atac în care o persoană rău intenționată se infilitrează între furnizorul de date și

   țintă. Acesta poate fi atât pasiv, doar pentru monitorizare, cât și activ prin alterarea datelor. [↑](#footnote-ref-5)
5. International Mobile Subscriber Identity – identifică în mod unic fiecare utilizator dintr-o rețea GSM [↑](#footnote-ref-6)
6. Temporary Mobile Subscriber Identity [↑](#footnote-ref-7)
7. MoU – Memorandum of Understanding, mai târziu devenit GSM Association GSMA [↑](#footnote-ref-8)
8. RRC – Radio Resource Control, protocol folosit pentru comunicarea dintre telefon și stația de bază (13) [↑](#footnote-ref-9)
9. DoS – Denial of Service, tip de atac în care ținta nu mai poate accesa serviciul dorit. De obicei acest atac se realizează prin aglomerarea rețelelor. [↑](#footnote-ref-10)
10. Google Play – magazinul de aplicații utilizat de telefoanele ce folosesc sistemul de operare Android [↑](#footnote-ref-11)
11. AppStore – magazinul de aplicații utilizat de telefoanele ce folosesc sistemul de operare iOS [↑](#footnote-ref-12)
12. GSMK Overwatch – sistem pentru detecția, localizarea și neutralizarea stațiilor mobile malițioase (18) [↑](#footnote-ref-13)
13. Honeypot – mecanism de securitate a care încearcă să detecteze atacurile asupra sistemelor informatice [↑](#footnote-ref-14)
14. IDE – integrated development environment – mediu de dezvoltare pentru diferite aplicații informatice. [↑](#footnote-ref-15)