

# Table des matières

Introduction générale.....	8
1. Contexte du travail .....	12
1.1 Introduction.....	13
1.2 Historique .....	13
1.3 Plan hospitalier.....	13
1.3.1 Organigramme général de CHU Tlemcen .....	13
1.3.2 Présentation du Service d'Anatomie et cytologie pathologiques .....	14
1.3.3 Qu'est que le frottis cervico-vaginal (FCV).....	14
• Définition.....	14
• Réalisation de frottis cervico-vaginal .....	15
1.4 Etude de l'existant.....	15
1.5 Critique de l'existant .....	16
1.6 conclusion.....	17
2. Conception de notre système G-Anlys_distance.....	18
2.1 Introduction.....	19
2.2 Analyse des besoins.....	19
2.3 Modélisation UML du système G-Analyse_distance .....	20
2.4 Les diagrammes desystème .....	21
2.4.1 Diagramme de cas d'utilisation .....	21
➤ Identification des acteurs .....	21
➤ Identification des cas d'utilisation.....	22
2.4.2 Diagramme de séquence.....	25
2.4.3 Diagramme de classe.....	28
2.4.4 Le Modèle logique.....	29
2.5 Conclusion .....	30
3. Mise en œuvre de notre système Anlys_distance.....	31
3.1 Introduction .....	32
3.2 Architecture du Système.....	32
3.2.1.1 Architecture MVC.....	33
3.2.2.1 Remote Method Invocation (Java RMI).....	34
3.3 Logiciels et outils utilisés .....	36
3.4 Présentation de quelques interfaces.....	38

3.4.1	Application web.....	38
3.4.2	Application à distance RMI.....	45
3.4.3	Application mobile pour les patientes .....	47
3.5	Conclusion.....	50
4.	Simulation du réseau G-Anlys_distance en mode sécurité .....	51
4.1	Introduction.....	52
4.2	Problèmes lié à l'application web.....	52
4.3	Logiciels utilisé pour la simulation .....	54
4.4	Intérêt de sécuriser notre système .....	54
4.5	La sécurisation d'une application web .....	55
4.5.1	Sécurité au niveau de la couche d'application.....	55
4.5.2	Sécurité au niveau de la couche de transport.....	56
4.5.3	Sécurité au niveau de la couche réseau .....	56
4.5.4	Sécurité au niveau de la couche d'accès.....	57
4.6	Sécurisation de l'application mobile .....	57
4.7	La simulation .....	58
4.5.1	Topologie de notre réseau .....	58
4.5.2	Les équipements d'interconnexion .....	58
4.5.3	Configuration de routeur.....	59
4.5.4	Configuration de ASA (firewall) .....	60
➤	Configuration de VPN SSL sous ASA .....	60
4.5.5	Exemple d'une attaque de réseau avec le Kali Linux .....	67
4.8	Conclusion .....	70
	Conclusion générale .....	71
	Webographie.....	73
	Bibliographie.....	73

## Liste des figures

Figure 1 : L'organigramme général de CHU Tlemcen .....	14
Figure 2 : Brosse pour la réalisation de frottis .....	15
Figure 3: Feuille Excel pour un rapport médical de frottis .....	16
Figure 4 : Schéma de processus unifié UP .....	21
Figure 5: Diagramme de cas d'utilisation .....	25
Figure 6: Diagramme de séquence d'authentification.....	26
Figure 7: Diagramme de séquence d'ajouter patient et donner un code .....	26
Figure 8: Diagramme de séquence de rédiger bulletin.....	27
Figure 9: Diagramme de séquence de consulter rapport médical .....	27
Figure 10: Diagramme de séquence pour voir l'historique .....	28
Figure 11: Diagramme de classe .....	29
Figure 12: Architecture global de Système G-Analyse_distance.....	33
Figure 13: Le fonctionnement de l'architecture MVC de notre système.....	34
Figure 14: Le fonctionnement de l'architecture RMI.....	35
Figure 15: Fenêtre d'authentification .....	38
Figure 16: fenêtre de gestion de secrétaire.....	39
Figure 17: Enregistrement de patiente .....	39
Figure 18: Exemple d'un code de rendez-vous .....	40
Figure 19: Fenêtre d'affectation des frottis aux patientes .....	40
Figure 20: Fenêtre de pathologiste .....	41
Figure 21: Fenêtre de remplir le rapport médical.....	42
Figure 22: Imprimer de rapport médical .....	43
Figure 23: Fenêtre d'authentification pour la patiente ou l'agent d'un centre médical sur l'application web.....	44
Figure 24: Fenêtre de choix la méthode de confirmation de compte .....	44
Figure 25: Fenêtre de réception de code de confirmation de compte par email .....	45
Figure 26: Fenêtre d'entrée le code confirmation.....	45
Figure 27: Fenêtre d'authentification pour l'application RMI .....	46
Figure 28: Message de serveur qu'il n'a pas de résultat pour le moment.....	46
Figure 29: Fenêtre des résultats.....	47
Figure 30: Fenêtre d'authentification pour l'application android.....	48
Figure 31: Fenêtre de choisir la méthode de confirmation.....	48
Figure 32: Entrer le code confirmation .....	49
Figure 33: Consultation du résultat par smartphone .....	50
Figure 34: Topologie de notre réseau.....	58
Figure 35: Configuration de routeur R1 .....	60
Figure 36: Configuration de ASA .....	60
Figure 37: Fenêtre d'installation de ASDM.....	61
Figure 38: Fenêtre de Cisco ASDM Launcher.....	62

Figure 39: Fenêtre de Cisco ASDM pour ASA.....	62
Figure 40: Fenêtre de configuration .....	63
Figure 41: Fenêtre de Cisco ASDM Packet Tracer.....	63
Figure 42: Fenêtre de configuration de Clientless SSL VPN.....	64
Figure 43: Création réussi de SSL VPN connexion.....	65
Figure 44: Page de certificat.....	66
Figure 45: Fenêtre d'authentification de secrétaire après la sécurisation .....	66
Figure 46: Fenêtre principal d'attaque avec Owasp .....	67
Figure 47: Résultat d'attaque d'Owasp .....	68
Figure 48: le scan des paquets de notre réseau (Attaque Sniffing) .....	69
Figure 49: Fenêtre d'analyse les paquets sniffé par Wirshark .....	70

## Liste des tableaux

Tableau 1:Les rôles des acteurs de diagramme de cas d'utilisation .....	21
Tableau 2:Table d'identification de cas d'utilisation authentification .....	22
Tableau 3:Table d'identification de cas d'utilisation enregistré patiente.....	22
Tableau 4:Table d'identification de cas d'utilisation donné code.....	23
Tableau 5:Table d'identification de cas d'utilisation rédigé rapport médical.....	23
Tableau 6:Table d'identification de cas d'utilisation consulter et imprimer résultat .....	24
Tableau 7:Table d'identification de cas d'utilisation voir l'historique .....	24
Tableau 8: Outils utilisé .....	37

# Introduction générale

## **Introduction générale**

### **Contexte**

Actuellement, le monde connaît une avance technologique considérable dans tous les secteurs et cela grâce à l'informatique qui est une science qui étudie les techniques du traitement automatique de l'information. Ce qui nécessite des systèmes d'information qui garantissent une bonne gestion de ces informations.

Le domaine de la santé est l'un des secteurs critiques qui nécessite un système d'information particulier à savoir systèmes d'information hospitalier ; ce système regroupe l'ensemble d'outils de partage et d'échanges incontournables au bénéfice des patients, des professionnels et du système de santé. Il est primordial de garantir leur disponibilité, leur sécurité, et leur confidentialité pour maintenir la confiance des patients dans le système de santé et celle des professionnels dans les outils qu'ils utilisent au quotidien.

Notre travail, consiste à réaliser une solution dédiée pour le service d'anatomie et de cytologie pathologiques du laboratoire Central de CHU de Tlemcen afin d'être utilisé dans la pathologie du cancer du col utérin et dans le programme national de dépistage des lésions précancéreuses et cancéreuses du col utérin, et qui pourra par la suite étendu pour d'autres pathologies tel que (cancer mammaire, cancer cutané, cancer de la prostate, cancer de la thyroïde,...)

### **Problématique et Objectifs**

Chaque jour, le service d'anatomie pathologique reçoit pour analyse un nombre important de prélèvements de FCV émanant des secteurs public et privé. Les résultats d'analyse aident les praticiens demandeurs à poser un diagnostic précis afin de donner aux patientes le traitement adéquat. Cette collaboration pluridisciplinaire a comme objectif de mieux explorer, diagnostiquer et traiter les différentes lésions courantes et rares.

Cependant, Un rapport d'analyse doit être rempli suite à la visualisation des lames microscope. Cette opération est effectuée soit :

- **par le pathologiste** : qui va saisir en plus des résultats d'analyse, les informations personnelles de la patiente (un formulaire électronique en Microsoft Word) et le remettre sous format électronique.
- **par la secrétaire** : qui va le saisir à partir d'un formulaire imprimé qui été rempli par le pathologiste.

Ces rapports médicaux sont enregistrés sur un ordinateur, mais ils sont mal organisés et peu exploitable.

Ainsi, la gestion des dossiers des patientes sur papier est confrontée à des pertes d'informations, alors que ces données sont importantes pour faciliter les activités quotidiennes administratives et médicales.

Aussi, la patiente doit se déplacer jusqu'au laboratoire Central juste pour récupérer son rapport médical, alors qu'il peut y avoir une collaboration entre le CHU et les centres médicaux pour qu'elle puisse le récupérer du centre médical le plus proche, et encore pourquoi pas exploiter la technologie mobile.

Ce que nous visons à travers notre travail est de faciliter la tâche pour :

- Le Pathologiste : pour la rédaction du compte rendu (ou bulletin) en exploitant toute les avantages que peut offrir une application informatique (recherche rapide, réutilisation, consultation de l'historique de la patiente....) ;
- La Secrétaire : pour enregistrer et archiver tous les données et résultats des patientes.
- La Patiente : elle n'est pas obligée de se déplacer pour récupérer son rapport.

Pour cela, nous avons exploité toutes les technologies avancées pour concevoir et réaliser notre système baptisé : G-Analys\_distance qui comporte 3 applications :

1. Application Web G\_Analyse\_Labo : qui consiste à aider la secrétaire surtout pour faire la gestion des données des patientes, utilisable aussi par le pathologiste afin de rédiger les rapports médicaux, vérifier et consulter l'historique de la patiente , et même la patiente peut consulter ces résultat depuis cette application web.
2. Application à distanceG\_Cons\_Rapport: application RMI qui consiste à la consultation des résultats au niveau des centres médicaux.

3. Application Android G\_And\_Rapport: application mobile qui consiste à la consultation des résultats pour la patiente toute seule sans se déplacer.

Aussi, afin de garantir la confidentialité des rapports médicaux des patientes, nous avons simulé notre système sur un réseau réel

### **Plan du mémoire**

Le premier chapitre présente l'établissement CHU Tlemcen particulièrement le service d'anatomie et cytologie pathologique ensuite nous expliquons le rôle d'un dépistage et plus particulièrement du col utérin, depuis l'arrivée du jusqu'à l'impression des résultats.

Le deuxième chapitre présente la conception de notre système d'information que nous allons modéliser avec le langage UML et plus particulièrement avec le processus unifié.

La réalisation et l'implémentation de notre Système fera l'objet du troisième chapitre dans lequel nous illustrerons les différentes parties de notre système à savoir la base de données et les différentes requêtes qui permettent l'accès à ce lui là.

Le chapitre quatre aura comme objectif de vérifier la sécurité, et la confidentialité des rapports des patientes dans le système de santé pour cela nous allons faire une simulation de la sécurité dans un réseau réel.

Enfin, nous terminerons ce document par une conclusion générale.

# 1. Contexte du travail

## **1.1 Introduction**

Dans ce chapitre, nous allons présenter une étude en profondeur du contexte de notre travail à savoir le CHU Tlemcen puis le service d'Anatomie et cytologie pathologiques. Parmi les différents types des pathologies traitées au niveau du service d'Anatomie Pathologique, nous allons traiter le cas du col utérin via l'analyse du Frottis Cervico Vaginal (FCV). Ensuite, nous terminons ce chapitre par l'étude du système existant et ces limites.

## **1.2 Historique**

La construction de l'hôpital civil de Tlemcen a débuté en 1947 et achevée en 1954. C'était l'hôpital colonial de la ville de Tlemcen. A l'indépendance, il est devenu secteur sanitaire et universitaire de Tlemcen.

Il prend le nom du docteur TIDJANI DAMERDJI, médecin, patriote de la 1ère heure, martyr de la révolution algérienne, tombé au champ d'honneur le 17 avril 1957. [1]

## **1.3 Plan hospitalier**

La capacité technique de CHU Tlemcen de 646 lits, et il s'occupe d'une superficie de 13 hectares avec 44 services et laboratoires spécialisés.

### **1.3.1 Organigramme général de CHU Tlemcen**

L'organigramme représente graphiquement la structure de « CHU Tlemcen ».[2]

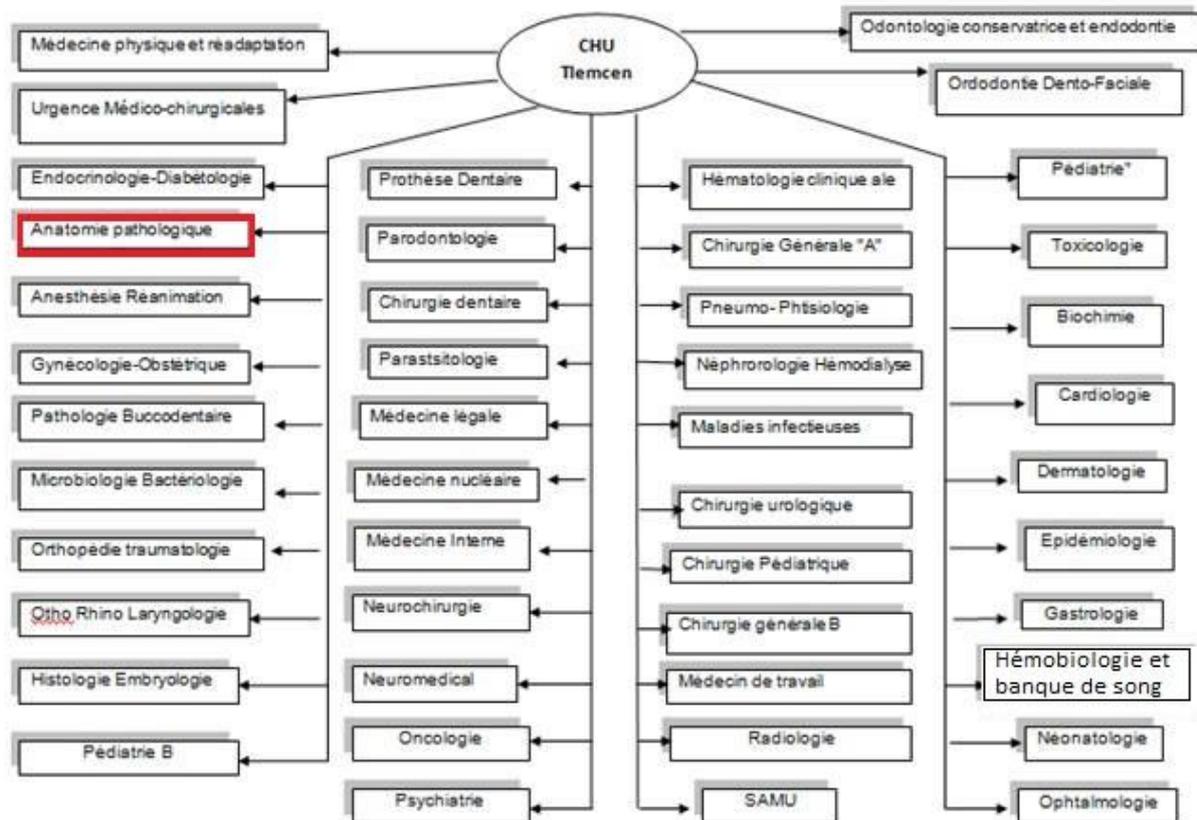


Figure 1 :L'organigramme général de CHU Tlemcen

### 1.3.2 Présentation du Service d'Anatomie et cytologie pathologiques

Ce service étudie les lésions macroscopiques et microscopiques de tissus prélevés sur des êtres vivants malades ou décédés par biopsie, frottis ou biopsie extemporanée. [3]

Notre centre d'intérêt est le prélèvement cytologique du col utérin à savoir Frottis cervico vaginal (FCV).

### 1.3.3 Qu'est que le frottis cervico-vaginal (FCV)

- **Définition**

Le frottis cervico-vaginal est un examen effectué dans le cadre du dépistage du cancer du col de l'utérus. Cet examen consiste à prélever des cellules superficielles au niveau du col de l'utérus, il est pratiqué au cours d'un examen gynécologique. Le prélèvement est ensuite examiné au microscope dans un laboratoire de cytologie. Selon l'aspect des cellules, on peut supposer que le col utérin est normal, ou bien qu'il présente une infection, une lésion précancéreuse ou un cancer. [4]

- **Réalisation de frottis cervico-vaginal**

Le prélèvement du frottis est réalisé à l'aide d'une spatule ou d'une petite brosse (voir la figure 2), par le gynécologue ou la sage femme.

Ce prélèvement est étalé sur une lame. La lame est ensuite fixée (la fixation ayant pour but de préserver l'état morphologique des cellules). [5] La lame est ensuite examinée au microscope par le pathologiste (Cytopathologiste).



Figure 2 : Brosse pour la réalisation de frottis

#### **1.4 Etude de l'existant**

L'étude de l'existant est une phase importante pour bien comprendre le système actuel. Notre but est de remédier aux problèmes et limites détectés et apporter des solutions requises ainsi que des suggestions d'améliorations. Nous résumons dans ce qui suit, les étapes que devait faire une patiente depuis le dépôt des lames à analyser jusqu'à l'obtention du résultat dans le système actuel.

**Etape dépôt et enregistrement** : La patiente (ou le conjoint) se présente au guichet pour déposer les lames de frottis à analyser, la secrétaire doit enregistrer la patiente avec ces informations dans un registre puis lui donner un code. C'est ce numéro qu'elle doit le présenter au guichet lors de la récupération de son rapport médical.

**Etape de rédaction du rapport médical** : Le pathologiste rédige le rapport médical du cas de la patiente dans un fichier Microsoft Excel, et l'imprimer. Ou il va juste remplir le formulaire sous format papier et le donner à la secrétaire pour faire la saisie.

**Etape récupération du rapport d'analyse** : La patiente **doit** revenir à l'hôpital pour récupérer son résultat.

- La figure ci-dessous présente un exemple de document Excel utilisé.

<b>C.H.U TLEMCEN</b> Laboratoire d'anatomie et cytologie pathologique		
Tél : 043 – 20 – 84 - 03    Poste : 23 - 30		
Programme national de dépistage des lésions du col uterin		
Patiente :		<b>401F12</b>
Age : 37 ans		
Médecin traitant : Pr BENHABIB R		
Service : Clinique Benhabib		
Fait le : 13/03/2012	Remis le :	
<b>Diagnostic cytopathologique</b>		
Frottis de dépistage <input checked="" type="checkbox"/>	Frottis de control <input type="checkbox"/>	
* qualité du prélèvement : satisfaisant <input checked="" type="checkbox"/>	ininterprétable <input type="checkbox"/>	
Causes .....		
Limité par :		
Inflammation <input type="checkbox"/>	Absence de cellules glandulaires <input type="checkbox"/>	Présence du mucus <input type="checkbox"/>
* cytologie normale <input checked="" type="checkbox"/>		
* absence de lesion neoplasiques : <input checked="" type="checkbox"/>		
* Cytologie inflammatoire : Trichomonas <input type="checkbox"/> Mycose <input type="checkbox"/> Bactérie <input type="checkbox"/> autres <input type="checkbox"/>		
* Modifications réactionnelles : - Secondaire à :		
Inflammation <input type="checkbox"/>	Atrophie <input type="checkbox"/>	Irradiations <input type="checkbox"/>
DIU <input type="checkbox"/>	Ectropion <input type="checkbox"/>	Autres <input type="checkbox"/>
- A type de : Métaplasie <input type="checkbox"/> Autre <input type="checkbox"/>		
* lesion intra-epitheliales ou invasives :		
* Anomalies des cellules épithéliales squameuses :		
ASC-US <input type="checkbox"/>	ASC-H <input type="checkbox"/>	Lésion de bas grade <input type="checkbox"/> Lésion de haut grade <input type="checkbox"/>
Carcinome épidermoïde <input type="checkbox"/>	HPV <input type="checkbox"/>	
* Anomalies des cellules épithéliales glandulaires :		
GUAS <input type="checkbox"/>	Adénocarcinome <input type="checkbox"/>	Autres <input type="checkbox"/>
* Autres néoplasiques :		
Malignes : .....		
<b>Conclusion :</b>		
Aspect cytopathologique d'une muqueuse cervicale d'allure sub normale.		
<b>Recommandations :</b>		
Refaire dans les meilleurs délais <input type="checkbox"/>	06 mois après traitement <input type="checkbox"/>	
Orienter vers le service de gynécologie <input type="checkbox"/>	Colposcopie <input type="checkbox"/>	Biopsie <input type="checkbox"/>
Refaire le frottis dans : 01 ans <input type="checkbox"/>	03 ans <input checked="" type="checkbox"/>	05 ans <input type="checkbox"/>
Dr BOUKLI-HACENE Z.		

Figure 3:Feuille Excel pour un rapport médical de frottis

### 1.5 Critique de l'existant

La méthode de travail actuel possède un nombre important de problèmes tels que :

- Le volume important des informations traitées manuellement, ce qui provoque parfois des erreurs dans l'établissement des documents.
- La recherche difficile sur les registres chose qui engendre une perte de temps.
- Une insécurité des informations, perte de confidentialité des données de la patiente.
- Possibilité d'erreur dans le remplissage des différents documents et registres.
- Nombre important des archives qui engendre une difficulté de stockage.

- Détérioration et risque de perte
- Mauvaise manipulation de l'outil Microsoft Word et difficulté de remplissage des rapports médicaux par les pathologistes.
- Possibilité d'erreur dans les calculs des statistiques.
- déplacement des patientes vers le laboratoire centrale et peut être à répétition pour récupérer son résultat.

### **1.6 conclusion**

Dans ce chapitre, nous avons pu donner une présentation claire du contexte de travail. En outre, nous avons projeté les limites du système actuel. Pour cela, nous avons commencé par la présentation des services. Par ailleurs, nous s'intéressons, dans le chapitre suivant, aux besoins de l'application pour répondre aux attentes du système.

## **2. Conception de notre système G- Anlys\_distance**

## **2.1 Introduction**

Pour mener à bien le projet, nous devons tout naturellement avoir recours à un formalisme de conception dont nous choisissons le langage de modélisation UML «Unified Modeling Language» qui est le langage de modélisation graphique qui va nous permettre de décrire les besoins, de spécifier et modéliser notre cas d'application ainsi que d'esquisser les architectures logicielles.

Dans ce chapitre, nous commençons par tirer les nouveaux besoins de notre système puis nous passons à la conception d'où nous allons faire appel à la boîte à outils UML tout en respectant le processus d'unification UP (Unified Processus) à savoir : le diagramme des cas d'utilisation, le diagramme de séquences et le diagramme de classes.

## **2.2 Analyse des besoins**

Dans un souci de concevoir une application avec plus de fonctionnalités possibles et dans le but d'avoir une interface plus conviviale et plus facile à utiliser tout en étant plus efficace, nous allons concevoir un système de gestion de laboratoire des analyses et plus particulièrement de Frottis au sein du CHU Tidjani Damedrji Tlemcen. concevons notre système baptisé G-Analyse\_distance qui vise à pallier les limites de l'existant.

Nous résumons dans ce qui suit, les nouveaux besoins à prendre en considération dans notre système.

### **Etape d'enregistrement**

Lorsque la patiente(ou conjoint) se présente au secrétariat pour déposer les lames de frottis ainsi le certificat médical du médecin qui a demandé l'analyse.

La secrétaire va enregistrer cette patiente dont deux cas se présentent :

1. Nouvelle patiente.
2. Sélectionner patiente (une chose qu'elle ne se faisait pas avant (pas d'historique des frottis de la patiente)).

Pour ce qui concerne la nouvelle patiente elle doit saisir :

Nom, prénom, nom de l'époux et l'âge (ou date de naissance).

Et dans les deux cas, elle va saisir :

- ➔ Le nom du médecin traitant c'est à dire qui a demandé cette analyse (d'après certificat médical).

→ Le nom du pathologiste qui va voir les lames et rédiger le rapport médical.

A la fin, un code séquentiel (année+numséquentiel), va être généré automatiquement pour impression, ce code servira à se connecter de chez soi pour récupérer son rapport sans à se déplacer.

### **Etape de rédaction du bulletin**

Une fois que le pathologiste examine les lames, il ne va plus se préoccuper à saisir les informations personnelle de la patiente (une chose faite par la secrétaire) mais plutôt sélectionner le code du frottis pour remplir les résultats directement. Afin d'aider le pathologiste, il faut mettre à sa disposition un aperçu de l'historique d'une patiente au moment de rédaction du rapport.

Il pourra vérifier s'elle a déjà des cas précédents, pour qu'il puisse prendre les meilleures décisions concernant son nouveau cas.

### **Etape de consultation à distance**

C'est l'étape la plus critique du point de vue patiente. D'un coté, la patiente ne va plus se déplacer jusqu'au laboratoire central du CHU Tlemcen pour récupérer ses résultats d'analyses, d'où lui offrir un moyen plus facile (soit exploiter la technologie mobile ou se rapprocher du centre médical le plus proche).

Et d'un autre coté, vue quel rapport est une ressource confidentielle qu'il faut bien la protéger, il faut garantir sa confidentialité et sécurité de personnes intruse.

## **2.3 Modélisation UML du système G-Analyse distance**

Pour bien décrire les différentes étapes de conception de notre système, nous avons choisi le langage de modélisation UML (Unified Modeling Language). [6] et plus exactement le Processus Unifié UP qui est un processus de développement logiciel itératif, centré sur l'architecture, piloté par des cas d'utilisation et orienté vers la diminution des risques.

UP prend de la boîte à outils appelée diagrammes d'UML le diagramme de cas d'utilisation, diagramme de séquence et diagramme de classe (voir la figure 4)



Figure 4 : Schéma de processus unifié UP

## 2.4 Les diagrammes de système

### 2.4.1 Diagramme de cas d'utilisation

Le but de ce diagramme est d'avoir une vision globale sur les interfaces du futur logiciel. Ce diagramme est constitué d'un ensemble d'acteurs qui agit sur des cas d'utilisation.

#### ➤ Identification des acteurs

Au niveau de cette section, nous présentons les différents acteurs susceptibles d'interagir avec le système, mais tout d'abord, nous donnons une définition du concept acteur.

Un acteur représente l'abstraction d'un rôle joué par des entités externes (utilisateur, dispositif matériel ou autre système) qui interagissent directement avec le système étudié. [8]

La mise en marche de notre système nécessite essentiellement quatre acteurs:

Acteur	Rôle
<b>-Secrétaire</b>	-enregistrer les patientes. -donner et imprimer rendez vous. -imprimer les bulletins.
<b>-Pathologiste</b>	-rédiger les bulletins. -imprimer les bulletins. -vérifier l'historique de patiente.
<b>-Patiente/agent d'un centre médical</b>	-voir le résultat de ces analyses. -imprimer son bulletin.

Tableau 1:Les rôles des acteurs de diagramme de cas d'utilisation

➤ Identification des cas d'utilisation

❑ **Authentification**

<b>Cas d'utilisation</b>	S'authentifier
<b>Acteurs</b>	Secrétaire, pathologiste, l'agent d'un centre.
<b>Résumé</b>	L'utilisateur doit s'authentifier pour accéder à ses services.
<b>Pré condition</b>	L'utilisateur doit être créé dans la base de données et connaître ses identifiants.
<b>Post condition</b>	L'utilisateur est authentifié.
<b>Scénario</b>	<ol style="list-style-type: none"> <li>1. le système affiche le formulaire d'authentification.</li> <li>2. l'utilisateur saisit le nom d'utilisateur et le mot de passe.</li> <li>3. l'utilisateur envoie son nom d'utilisateur et mot de passe.</li> <li>4. le système vérifie l'existence de nom d'utilisateur.</li> <li>5. Le système vérifie le mot de passe.</li> <li>6. le système ouvre la session.</li> <li>7. le système affiche la page d'accueil.</li> </ol>

**Tableau 2: Table d'identification de cas d'utilisation authentification**

❑ **Enregistrer patiente**

<b>Cas d'utilisation</b>	Enregistrer une patiente
<b>Acteurs</b>	Secrétaire.
<b>Résumé</b>	Permettre au secrétaire d'enregistrer une patiente.
<b>Pré condition</b>	Secrétaire doit être d'authentifié.
<b>Post condition</b>	une patiente enregistrée.
<b>Scénario</b>	<ol style="list-style-type: none"> <li>1. Secrétaire vérifié d'abord si le nom de patiente existe ou non.</li> <li>2. Secrétaire sélectionné l'option «Ajouter patiente».</li> <li>3. le système affiche un formulaire d'ajout.</li> <li>4. Secrétaire remplit le formulaire avec l'ensemble des informations nécessaires de la patiente.</li> <li>5. Secrétaire envoie le formulaire.</li> <li>6. le système effectue un contrôle sur les champs saisis.</li> <li>7. le système ajoute la patiente.</li> </ol>

### ❑ Donner Code

<b>Cas d'utilisation</b>	Donner Code
<b>Acteurs</b>	Secrétaire.
<b>Résumé</b>	Permettre au secrétaire de donner un code à la patiente.
<b>Pré condition</b>	Secrétaire doit être identifié.
<b>Post condition</b>	code imprimé.
<b>Scénario</b>	<ol style="list-style-type: none"> <li>1. Secrétaire vérifié d'abord la disponibilité du pathologiste responsable pour faire les analyses.</li> <li>2. Secrétaire sélectionne l'option imprimé le code (rendez-vous).</li> <li>3. le système affiche un formulaire pour entrer les informations de code.</li> <li>4. Secrétaire remplit le formulaire.</li> <li>5. Secrétaire envoie le formulaire et click à l'option imprimer.</li> <li>6. le système affiche le code avant impression.</li> <li>7. le code imprimé.</li> </ol>

**Tableau 4:Table d'identification de cas d'utilisation donné code**

### ❑ Rédiger Rapport médical

<b>Cas d'utilisation</b>	Rédiger Rapport médical
<b>Acteurs</b>	Pathologiste.
<b>Résumé</b>	Permettre au pathologiste de rédiger des Rapports médicaux
<b>Pré condition</b>	Pathologiste doit être identifié.
<b>Post condition</b>	Le Rapport médical rédigé avec succès.
<b>Scénario</b>	<ol style="list-style-type: none"> <li>1. Pathologiste cherche d'abord le non de patiente.</li> <li>2. Pathologiste sélectionne l'option «rédiger Rapport médical».</li> <li>3. le système affiche un formulaire de rédigé le Rapport médical.</li> <li>4. Pathologiste remplit le formulaire avec l'ensemble des informations nécessaires de la patiente pour le Rapport médical.</li> <li>5. Pathologiste envoie le formulaire.</li> <li>6. le système effectue un contrôle sur les champs saisis.</li> <li>7. le système affiche Rapport médical rédigé.</li> </ol>

**Tableau 5:Table d'identification de cas d'utilisation rédigé rapport médical**

❑ **Consulter résultat et imprimer Rapport médical**

<b>Cas d'utilisation</b>	Consulter résultat et Imprimer Rapport médical
<b>Acteurs</b>	Secrétaire, Patiente, Agent.
<b>Résumé</b>	Permettre à l'utilisateur d'imprimer Rapport médical
<b>Pré condition</b>	L'utilisateur doit être identifié.
<b>Post condition</b>	Rapport médical imprimé avec succès.
<b>Scénario</b>	<ol style="list-style-type: none"> <li>1. l'utilisateur saisi le code séquentiel de patiente.</li> <li>2. Le système envoi un SMS de confirmation au numéro de téléphone de patiente.</li> <li>3. l'utilisateur entre le code de confirmation.</li> <li>4. le système affiche les résultats des analyses avec un bouton d'imprimer le Rapport médical.</li> <li>5. le système affiche un formulaire d'avant impression de Rapport médical.</li> <li>5. l'utilisateur click au bouton imprimer</li> <li>6. Rapport médical imprimé</li> </ol>

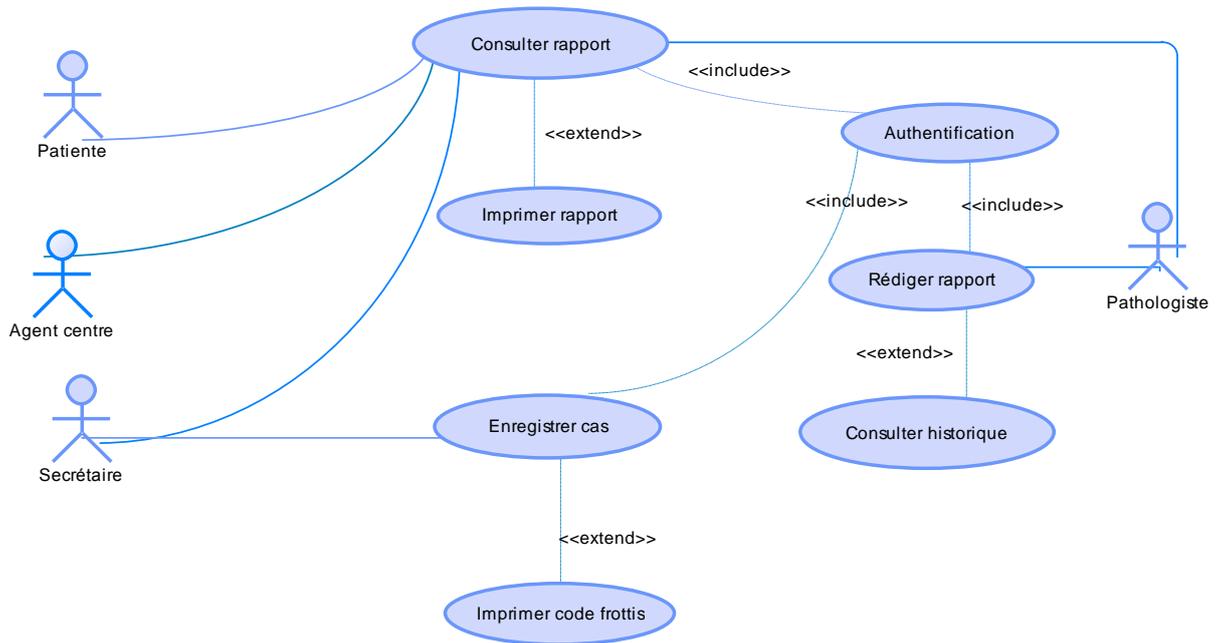
**Tableau 6:Table d'identification de cas d'utilisation consulter et imprimer résultat**

❑ **Voir historique**

<b>Cas d'utilisation</b>	Voir l'historique
<b>Acteurs</b>	Pathologiste, patiente, secrétaire.
<b>Résumé</b>	Permette au utilisateur de voir l'historique de patiente si elle a déjà fais un frottis.
<b>Pré condition</b>	L'utilisateur doit être identifié.
<b>Post condition</b>	Vérification d'historique terminé.
<b>Scénario</b>	<ol style="list-style-type: none"> <li>1. l'utilisateur saisi le code séquentiel de patiente.</li> <li>2. l'utilisateur sélectionne l'option «voir historique».</li> <li>3. si la patiente a déjà fait un frottis le système affiche tout l'historique de patiente.</li> </ol>

**Tableau 7:Table d'identification de cas d'utilisation voir l'historique**

La figure ci-dessous présente le digramme de cas d'utilisation :



**Figure 5:Diagramme de cas d'utilisation**

#### 2.4.2 Diagramme de séquence

Les cas d'utilisations. Avec ses multiples relations (**extend**, **include**, etc.), nous donne une vue presque réelle de l'application. Cette richesse nous montre une vue globale de l'application mais pour voir réellement la succession des actions des acteurs il nous faut un autre modèle qui nous détaille le séquençage des opérations ce diagramme s'agit du diagramme des séquences. Ce dernier comme son nom l'indique il développe un cas d'utilisation en montrant les différentes opérations permettant de réaliser l'action du cas en question.

❑ **Diagramme de séquence d'authentification**

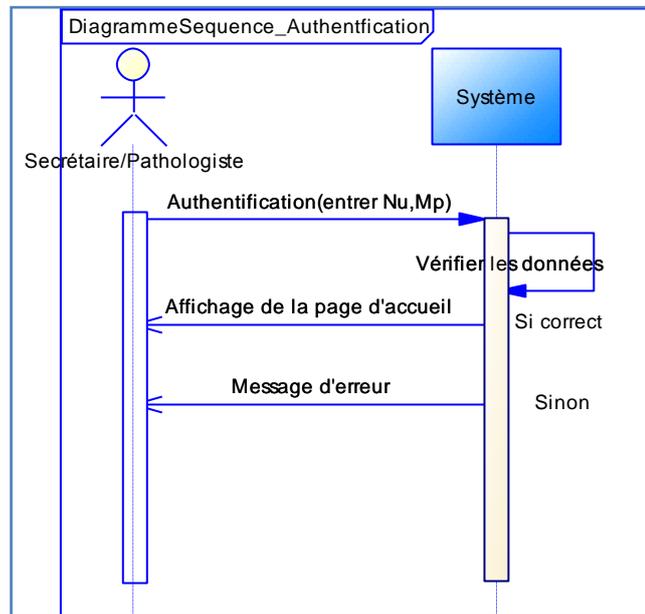


Figure 6:Diagramme de séquence d'authentification

❑ **Diagramme de séquence d'ajouter un cas**

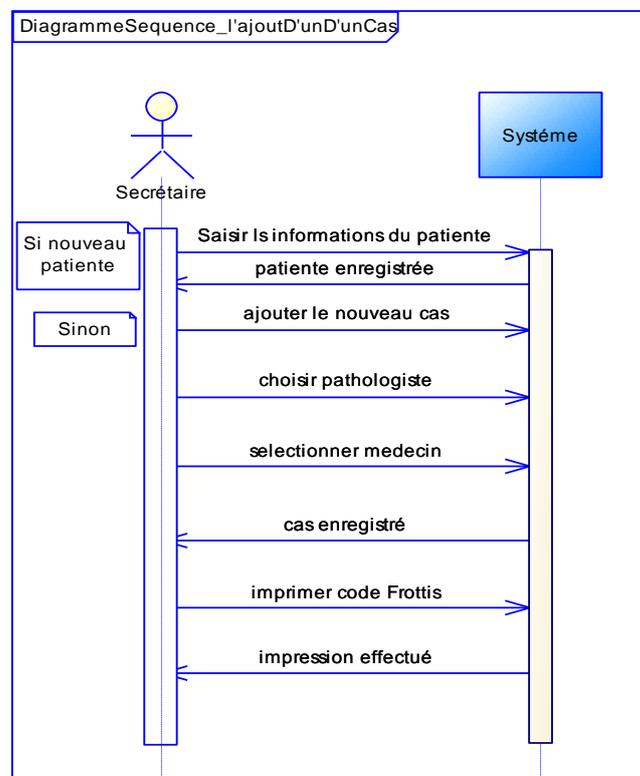


Figure 7:Diagramme de séquence d'ajouter patient et donner un code

❑ **Diagramme de séquence de rédiger Rapport médical**

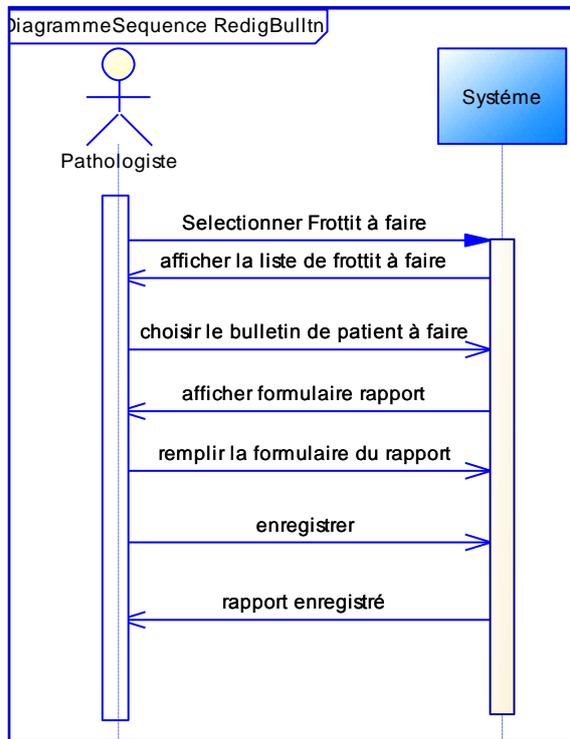


Figure 8: Diagramme de séquence de rédiger bulletin

❑ **Diagramme de séquence de consulter le Rapport médical**

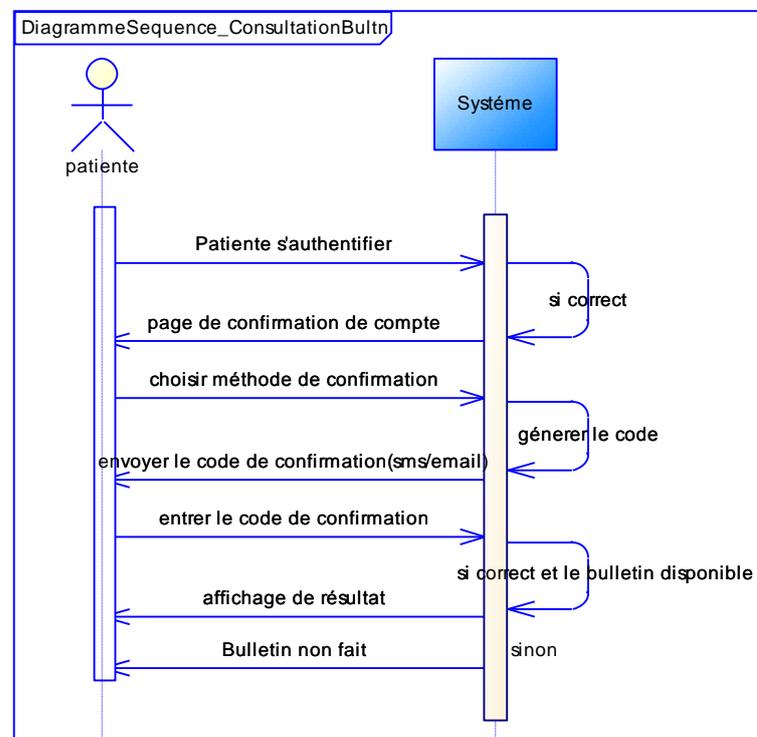


Figure 9: Diagramme de séquence de consulter rapport médical

### ❑ Diagramme de séquence pour voir l'historique

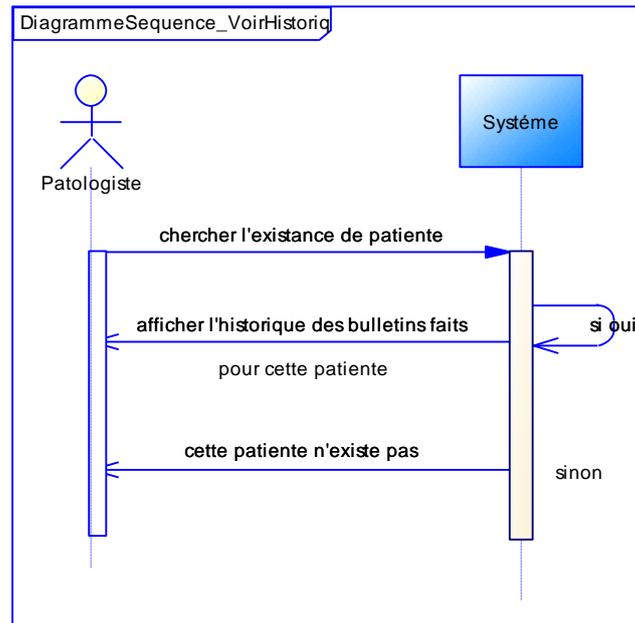


Figure 10:Diagramme de séquence pour voir l'historique

#### 2.4.3 Diagramme de classe

Le diagramme de classe permet de représenter l'ensemble des informations finalisées qui sont gérées par le domaine. Ces informations sont structurées, c'est-à-dire qu'elles ont regroupées dans des classes. Le diagramme met en évidence d'éventuelles relations entre ces classes.

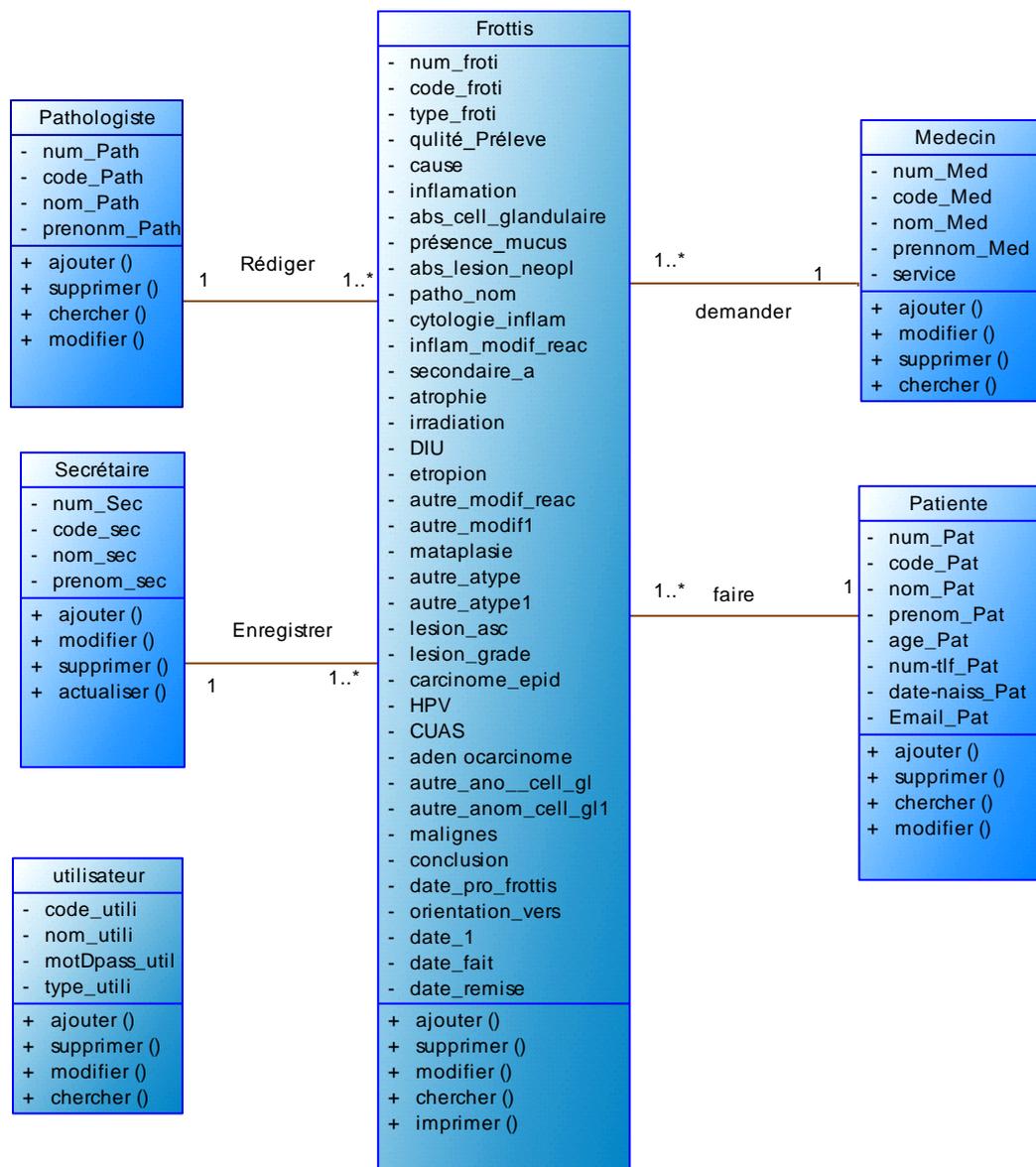


Figure 11:Diagramme de classe

#### 2.4.4 Le Modèle logique

A partir du diagramme de classe que nous avons effectué, on peut réaliser le modèle logique, vu que le système d'information ne peut pas le manipulé directement et cela en utilisant les règles de passage suivantes :

- Affecter une table à chaque classe.
- Une association « un à plusieurs » engendre la migration de la clé primaire de la table mère à la table fille.
- Une association « plusieurs à plusieurs » est représentée par une table ayant pour clé primaire la concaténation des clés primaires des deux tables associées.

En appliquant les règles de transformation d'un diagramme de classe vers un modèle relationnel, nous avons abouti au schéma logique suivant :

- Patiente (num\_pat, code\_pat, nom\_pat, prénom\_pat, age\_pat, num-tlf\_pat, date-nais\_pat, email\_pat).
- Secrétaire (num\_secr, code\_secr, nom\_secr, prénom\_secr).
- Pathologiste (num\_cyt, code\_cyt, nom\_cyt, prénom\_cyt).
- Médecin traitant (num\_Med, code\_Med, nom\_Med, prénom\_Med, spécialité, service).
- Frottis (num\_frotti, code\_frotti, type\_frotti, qualité\_prelev, Causes, inflammation, abs\_cell\_gland, presence\_mucus, pathlo\_norm, abs\_lesion\_neopl, cytologie\_inflam, secondaire\_a, inflam\_modif\_reac, atrophie, irradiation, DIU, ectropion, autre\_modif\_reac, autre\_modif1, metaplasie, autre\_atype, autre\_atype1, lesion\_ASC, lesion\_GRADE, carcinome\_epid, HPV, GUAS, adenocarcinome, autre\_anom\_cell\_gl, autre\_anom\_cell\_gll, malignes, conclusion, date\_pro\_frottis, orientation\_vers, date\_1, frottis\_fait, date\_fait, date\_remise, #num\_pat, #num\_Path, #num\_secr, #num\_Med, #code\_util).
- Utilisateur (code\_util, nom\_util, motDpass\_util, type\_util) .

## **2.5 Conclusion**

L'étape de l'analyse et de conception est l'étape la plus importante dans le cycle de développement, Car c'est le résultat de cette étape qui sera nous guidé dans l'étape d'implémentation. Dans le chapitre suivant on va montrer comment nous avons implémenté le résultat de ce chapitre pour réaliser notre application.

### **3. Mise en œuvre de notre système**

#### **Anlys\_distance**

### **3.1 Introduction**

Après avoir analysé les besoins et défini la méthodologie de conception, nous allons implémenter notre système via un environnement adéquat.

Ce chapitre aborde l'implémentation de notre système, nous allons présenter notre choix de technologie d'implémentation, les outils, les techniques et les langages de programmation que nous allons utiliser. Nous terminons avec quelques interfaces utilisateurs.

### **3.2 Architecture du Système**

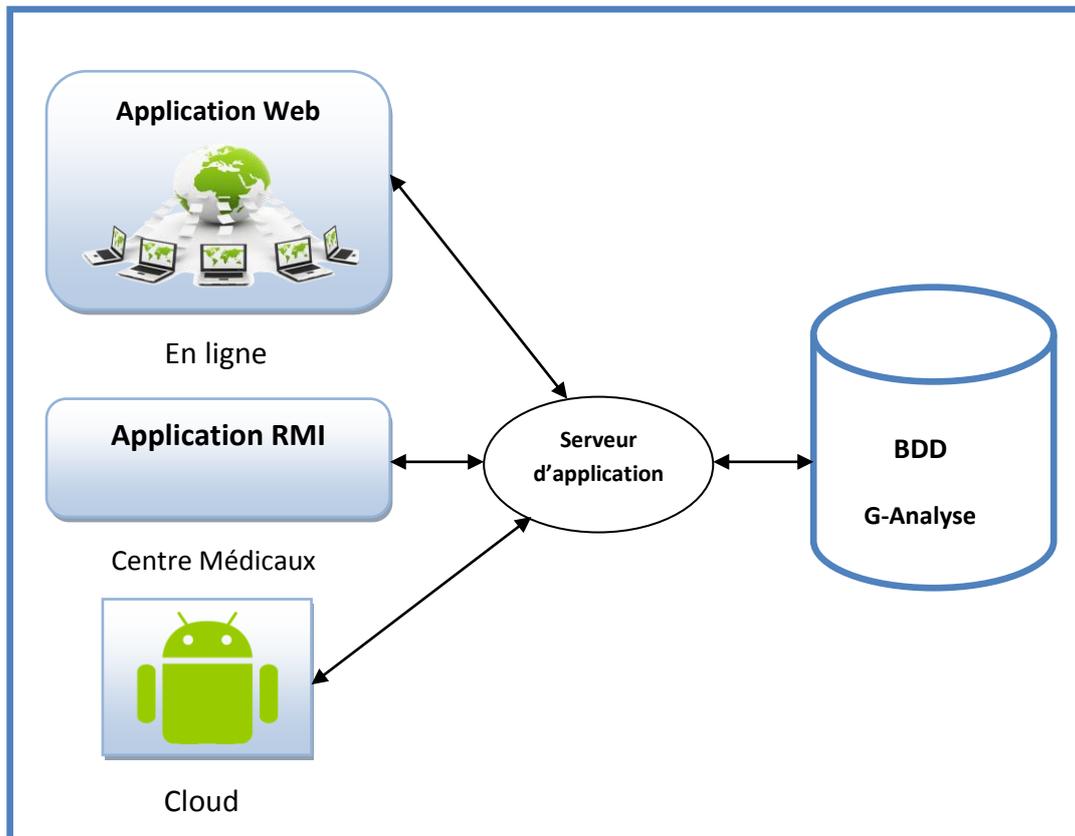
Afin de mener à bien la mise en œuvre de notre système, nous nous sommes basés sur différente architecture qui nécessite un grand nombre de technologies. Pour faciliter l'intégration de ces technologies et le développement d'applications, les éditeurs offrent des Frameworks globaux comme J2EE de Sun. [9] Parmi ces technologies :

- **Présentation** : HTML, PHP, JSP, ...
- **Applicatif** : objets, composants, scripts exécutables, services ...
- **BDD** : fichiers XML, SGBDR, ...
- **Protocoles de communication** : RPC / RMI, HTTPS, ...

Pour réaliser notre travail, nous avons implémenté 3 applications (voir figure suivante) partageant le même serveur d'application (serveur BDD, serveur web, serveur RMI) qui est hébergé au niveau du réseau du laboratoire central du CHU Tlemcen

1. **Application web en ligne** dont les utilisateurs de cette application sont la secrétaire, le pathologiste, et même la patiente peut l'utiliser pour la consultation.
2. **Application RMI à distance** installé au niveau des centres médicaux, dont l'utilisateur de cette application est l'agent du centre médicale.
3. **Application mobile sous Android** téléchargeable et utilisable par les patientes

La figure (12) présente l'architecture globale de notre système



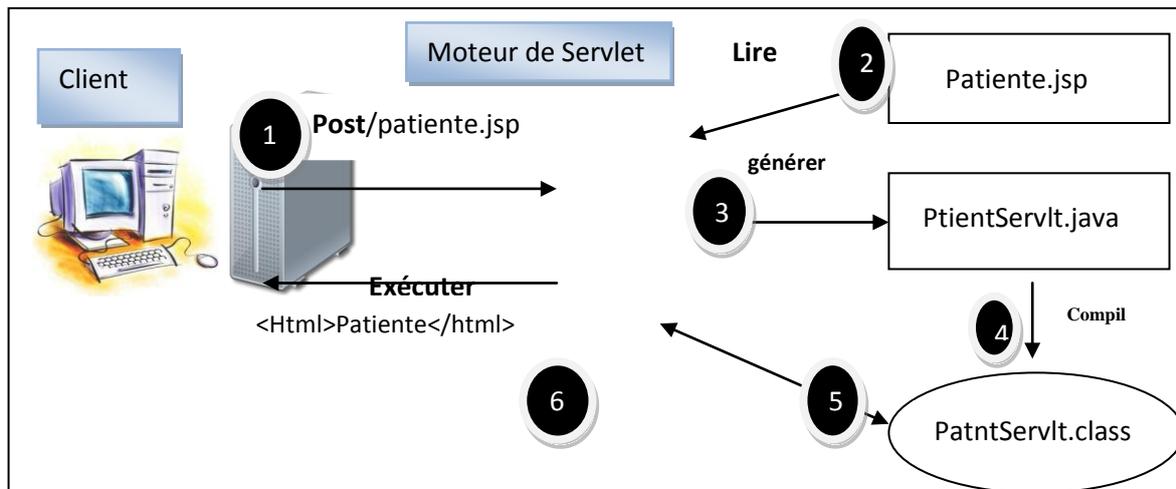
**Figure 12: Architecture global de Système G-Analyse\_distance**

Principalement, nous avons utilisé l'architecture MVC, RMI, dont l'architecture détaillé de notre système est la suivante :

### 3.2.1.1 Architecture MVC

L'objectif d'utilisation d'une telle architecture est la séparation des différentes *couches* constituant une application interactive, de manière à simplifier la gestion de chacune.

La figure suivante explique le fonctionnement pratique de l'architecture MVC dans notre système, nous prenons le cas d'enregistrement patiente.



**Figure 13:Le fonctionnement de l'architecture MVC de notre système**

1. le client débute avec une requête qui demande une page ou une ressource de notre application, cette requête destinée au contrôleur pour la traitée.
2. et 3. Une fois que la requête arrive au contrôleur (moteur de servlet), celui-ci va lire cette jsp et génère sa servlet correspondante, puis la servlet fait appel au Bean.
4. et 5. Après la compilation et l'exécution des traitements, cette communication terminés par une sortie.
6. Finalement, quand la sortie est générée, elle est immédiatement rendue au client.

### 3.2.2.1 Remote Method Invocation (Java RMI)

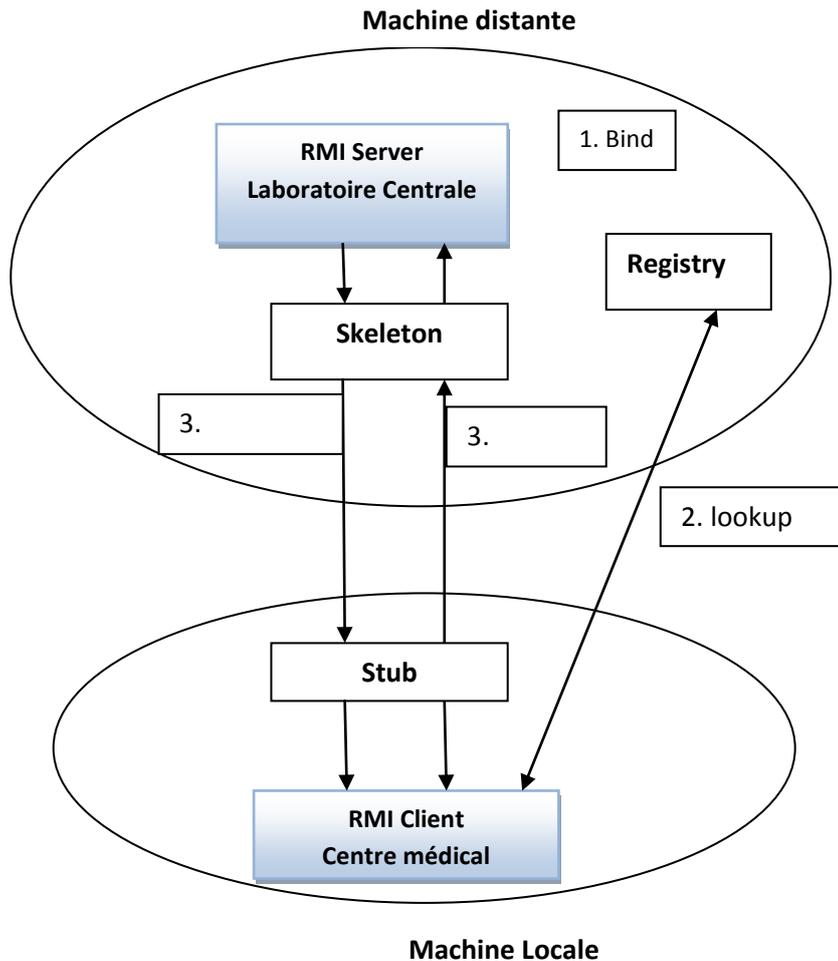
Est une interface de programmation (API) pour le langage Java qui permet d'appeler des méthodes distantes. [11]

#### ➤ Architecture RMI

Mécanisme qui permet à des objets localisés sur des machines distantes de s'échanger des messages (invoquer des méthodes).

L'architecture RMI définit la manière dont se comportent les objets, comment et quand des exceptions peuvent se produit, comment gérer la mémoire et comment les méthodes appelées passent et reçoivent les paramètres.

La figure(14) présente le déroulement de l'architecture RMI Général



**Figure 14: Le fonctionnement de l'architecture RMI**

1. Le serveur doit d'abord enregistrer (bind) son nom dans l'annuaire (Registry).
2. Le client récupère les références du serveur à partir de son nom auprès de l'annuaire (lookup).
3. Le stub sérialise les paramètres, l'envoie au squelette (skeleton) qui invoque la méthode sur serveur et retourne les résultats auprès de stub.

L'architecture interne de RMI : le système RMI contient 3 couches qui sont :

- .\_La couche des amorces (stub/Skelton).
- .\_La couche des références (RRL).
- .\_La couche de transport.

Chacun de ses couches est indépendante de l'autre et utilise un protocole spécifique, la transmission des objets utilise deux technique :

1. La sérialisation.

2. Le chargement dynamique du stub, permet au client de charger dynamiquement le stub quand il a seulement l'interface. [12]

### **3.3 Logiciels et outils utilisés**

#### *3.1.1. Java*

Nous avons exploité le langage java dans notre travail. Java est un langage de programmation et une plate-forme informatique créée par Sun Microsystems en 1995. Beaucoup d'applications et de sites Web ne fonctionnent pas si Java n'est pas installé et leur nombre ne cesse de croître chaque jour. Java est rapide, sécurisé et fiable. [13].

#### *3.1.2. Servlet*

Programme Java qui s'exécute dynamiquement sur le serveur Web et permet l'extension des fonctions de ce dernier, typiquement : accès à des bases de données, etc. Un Servlet peut être chargé automatiquement lors du démarrage du serveur Web ou lors de la première requête du client. Une fois chargés, les servlets restent actifs dans l'attente d'autres [14]

#### *3.1.3. JSP (Java Server Page)*

Extension de la technologie Java Servlet de Sun qui permet de programmer simplement l'affichage de contenus dynamiques sur le Web. JSP consiste en une page HTML incluant du code Java qui s'exécutera soit sur le serveur Web, soit sur le serveur d'application. Un exemple d'utilisation de JSP dans notre application web Java et à certaines actions prédéfinies d'être ajoutés dans un contenu statique. [14]

#### *3.1.4. Java Script*

Langage de rédaction de scripts, destiné aux utilisateurs non spécialistes, qui permet d'intégrer des instructions Java préprogrammées dans la construction d'un document Web. Alors que le langage Java permet aux programmeurs de créer de nouveaux objets et des mini-applications, le langage JavaScript permet aux concepteurs de pages Web de fusionner des applets ou de les programmer de façon personnalisée, sans avoir à manipuler de code Java. [15]

#### *3.1.5. HTML (HyperText Mark-Up Language)*

Est un langage dit de « marquage » de « structuration » ou de « balisage » dont le rôle est de formaliser l'écriture d'un document avec des balises de formatage. [16]

### 3.1.6. *Css*

Est un langage informatique utilisé sur l'internet pour mettre en forme les fichiers HTML ou XML. Ainsi, les feuilles de style, aussi appelé les fichiers CSS, comprennent du code qui permet de gérer le design d'une page en HTML. [17]

### 3.1.7. *MYSQL*

MySQL est un système de gestion de base de données relationnelle libre très employée sur le Web, souvent en association avec Apache (serveur web). MySQL fonctionne indifféremment sur tous les systèmes d'exploitation. Le langage SQL (Structured Query Language) est un langage universellement reconnu par MySQL et les autres bases de données et permettant d'interroger et de modifier le contenu d'une base de données. [18]

### 3.1.8. *JQuery*

JQuery est une bibliothèque JavaScript gratuite et multiplateforme. Compatible avec l'ensemble des navigateurs Web (Internet Explorer, Chrome, etc.), elle a été conçue et développée pour faciliter l'écriture de scripts. Elle ne nécessite aucune installation particulière et peut être téléchargée directement depuis le site officiel de la bibliothèque. [19]

### 3.1.9. *Plateforme logicielles*

Notre travail a été réalisé en utilisant plusieurs outils en peut citer les exemples suivants :

Logo	Nom de logiciel	Description
	Netbeans	est un environnement de développement intégré (EDI), permet la prise en charge native de divers langages tels le C, le C++, le JavaScript, java...ect
	XAMPP	XAMPP est une distribution Apache entièrement gratuite et facile à installer contenant MySQL, PHP et Perl. Le paquetage open source XAMPP a été mis au point pour être incroyablement facile à installer et à utiliser.
	Les navigateurs	Des navigateurs Pour tester et exécuter l'application. (Mozilla Firefox, Google Chrome ...ect).
	PowerAMC	est un logiciel de modélisation. Il permet de modéliser les traitements informatiques et leurs bases de données associées.

**Tableau 8: Outils utilisé**

### **3.4 Présentation de quelques interfaces**

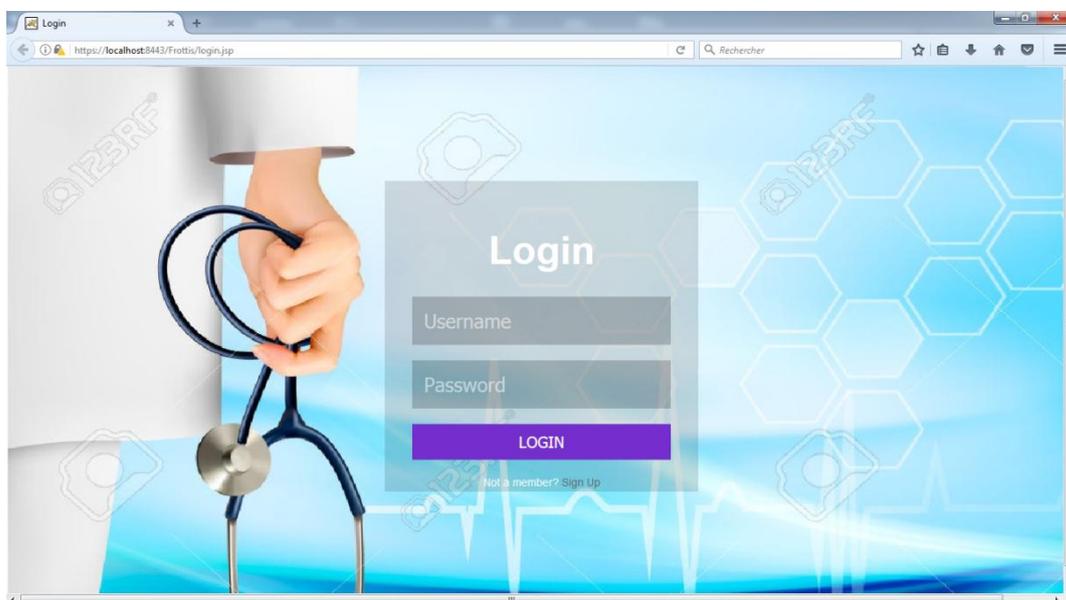
Dans la conception des interfaces de notre système nous avons respecté un ensemble des choix ergonomiques comme la lisibilité, la compréhension, etc. Dans ce qui suit une présentation des captures écrans des plus importantes tâches de l'application.

#### **3.4.1 Application web**

Cette application est dédiée pour le service d'anatomie et cytologie pathologiques du laboratoire central du CHU Tlemcen, elle sera utilisée par soit la secrétaire pour l'enregistrement des cas pathologiques ou par le pathologiste pour remplir le rapport médical qui sera mis à la disposition de la patiente ou l'agent du centre médical une fois fait.

##### 3.4.1.1 Fenêtre authentification

Cette fenêtre permet aux utilisateurs de notre application à savoir la secrétaire, le pathologiste, la patiente, et l'agent de centre de saisir le nom d'utilisateur et le mot de passe pour commencer à utiliser notre application. Cette interface constitue la fenêtre d'accueil de notre application. Cette étape met en valeur l'aspect sécurité : nous vérifions la disponibilité du compte utilisateur et nous lui attribuons les droits et privilèges nécessaires.



**Figure 15: Fenêtre d'authentification**

##### 3.4.1.2 La gestion des rôles

A l'aide d'un contrôleur « UsersController », des Sessions et des deux tables « USERS & PROFILS » dans la base de donnée ; notre application gère 4 profils :

## 1. Fenêtre de la secrétaire

C'est une fenêtre spécifique au profil de secrétaire, nous trouvons dans cette fenêtre les différentes activités que doit faire une secrétaire, la figure suivante illustre ces activités.



Figure 16:fenêtre de gestion de secrétaire

Par exemple le sous menu patiente sert à ajouter les informations personnelles de la patiente (figure 17), cette tâche ne s'effectuera plus par le pathologiste et case fait une seule fois. Une fois que la patiente est enregistrée, un nouveau cas doit être ajouté c'est-à-dire un nouveau frottis (voir figure 19) pour attribuer à la patiente un numéro qui lui servira pour récupérer son résultat d'analyse : soit à distance, soit au niveau du laboratoire central (voir figure 18)

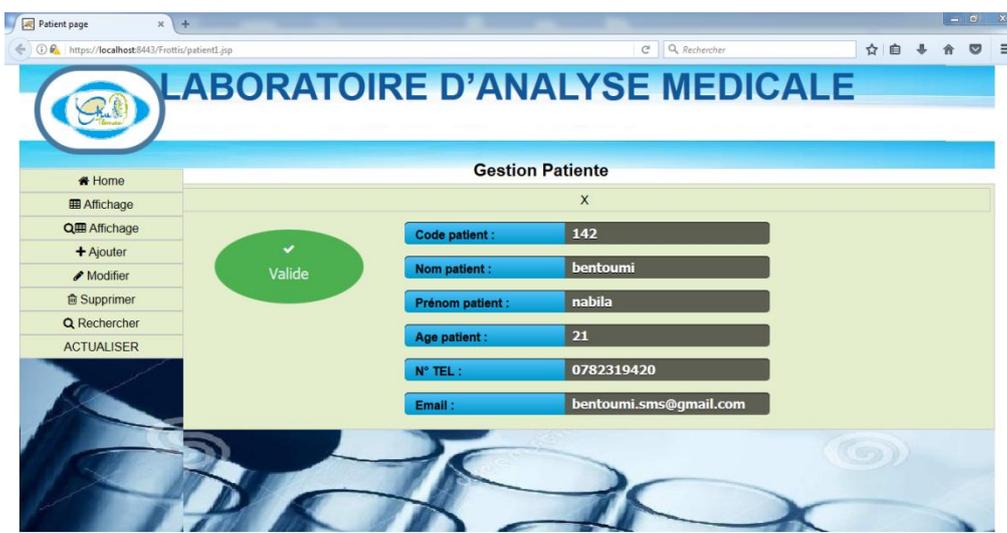


Figure 17: Enregistrement de patiente

Exemple de donner un code pour une patiente :



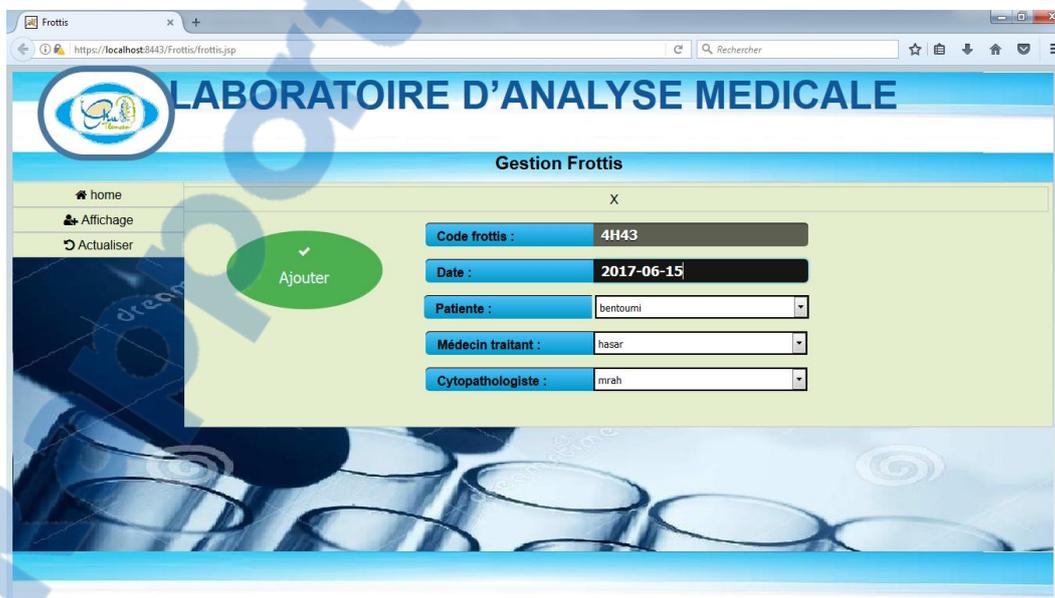
## CHU Tlemcen

<p><b><u>Patient</u></b></p> <p><u>Code</u> : 1314</p> <p><u>Nom</u> : bouakaz</p> <p><u>Prénom</u> : nassima</p> <p><u>Age</u> : 24</p> <p><u>Medecin traitant</u> : bjai</p> <p><u>Service</u> : Chirurgie</p>	<p><b><u>cytopathologiste</u></b></p> <p><u>Nom</u> : Zerga</p> <p><u>Prénom</u> : Mustapha</p> <p><b><u>Frottis</u></b> :</p> <p><u>Code</u> : 4423</p> <p><u>Fait le</u> : 2017-06-17</p>
--	---

Figure 18:Exemple d'un code de rendez-vous

À la prochaine arrivée de patiente elle doit présentée son code pour passer.

La secrétaire est responsable aussi à l'enregistrement des frottis



The screenshot shows a web browser window with the URL `https://localhost:8443/Frottis/frottis.jsp`. The page title is "LABORATOIRE D'ANALYSE MEDICALE". The main content area is titled "Gestion Frottis" and contains a form with the following fields:

- Code frottis : 4H43
- Date : 2017-06-15
- Patiente : bentoumi
- Médecin traitant : hasar
- Cytopathologiste : mrah

A green "Ajouter" button with a checkmark icon is positioned to the left of the form fields. The background of the page features a blue and white image of laboratory glassware.

Figure 19:Fenêtre d'affectation des frottis aux patientes

## 2. Fenêtre pathologiste

Dans cette interface qu'elle spécifié au pathologiste, nous trouvons les différentes rôles du pathologiste, nous avons deux menus : Menu et Recherche (voir figure 20)



Figure 20:Fenêtre de pathologiste

Pour le premier Menu, nous avons deux sous menu : Frottis fait et Frottis non fait.

Frottis non fait par exemple, une fois que le pathologiste examine les lames, il n'a qu'à sélectionner le numéro de frottis de la patiente pour remplir les résultats d'analyse (voir figure 21).

**LABORATOIRE D'ANALYSE MEDICALE**

home  
Affichage  
Actualiser

Numéro : 486  
 Nom : bentoumi  
 Prénom : zohlr  
 Age : 24  
 Medecin traitant : hasar  
 Service : Chirurgie

CODE\* frotis : 4422  
 Type frotis : Depistage  
 Qualité de prélèvement : Satisfaisant  
 Fait le : 2017-06-15  
 Remise le : 2017-06-20

Limité par : Inflammation   
 Absence de cellules glandulaires   
 Présence du mucus

Cytologie normale   
 Absence de lésions néoplasiques   
 Cytologie inflammatoire : chronique  
 secondaire à : Mycose

Modifications réactionnelles :  
 Inflammation  Ectropion   
 DIU  Irradiations   
 Atrophie  Autres

A type de :  
 Métablasie  Autres

Lésions intra-épithéliales ou invasives :  
 Anomalie des cellules épithéliales squameuses  
 ASC- : US  
 Lésion de : Base grande  
 Carcinome épidermoïde   
 HPV

Anomalie des cellules épithéliales glandulaires :  
 GUAS  Adénocarcinome

\* Autres néoplasiques  
 Malignes

Conclusion :

Recommandations :  
 Refaire dans : Dans les meilleurs delais  
 Orienter vers le service de : Gynécologie  
 Refaire le frottis dans : 01 ans

Valider

Figure 21: Fenêtre de remplir le rapport médical

La figure suivante un aperçu du rapport médical qui peut être imprimé

## Résultat d'Anatomie Pathologique

Patient		Frottis :	
Code :	1313	Code :	4422
Nom :	bentoumi	Type :	Deplstage
Prénom :	nabila	Qualité :	Satisfaisant
Age :	21	Fait le :	2017-06-15
Medecin traitant :	hasar	Remise le :	2017-06-20
Service :	Chirurgie		

**Limité par :**

Inflammation : oui | Absence de cellules glandulaires : non | Présence du mucus : oui  
 Cytologie normale : non

Absence de lésions néoplasiques : oui  
 Cytologie inflammatoire : chronique  
 Secondaire à : Mycose

**Modifications réactionnelles :**

Inflammation : non | Ectropion : oui | Atrophie : non  
 DIU : oui | Irradiations : non | Autres : non

**A type de :**

Métablasie : oui | Autres : non

**Lésions intra-épithéliales ou invasives :**

\* Anomalie des cellules épithéliales squameuses :  
 ASC- US | Lésion de | Base grande  
 Carcinome épidermoïde : non | HPV : oui

\* Anomalie des cellules épithéliales glandulaires :  
 GUAS : oui  
 Adénocarcinome : non

\* Autres néoplasiques :

Malignes :

Conclusion : Aspecte cytopathologique d'une muqueuse d'allure sub normale.

**Recommandations :**

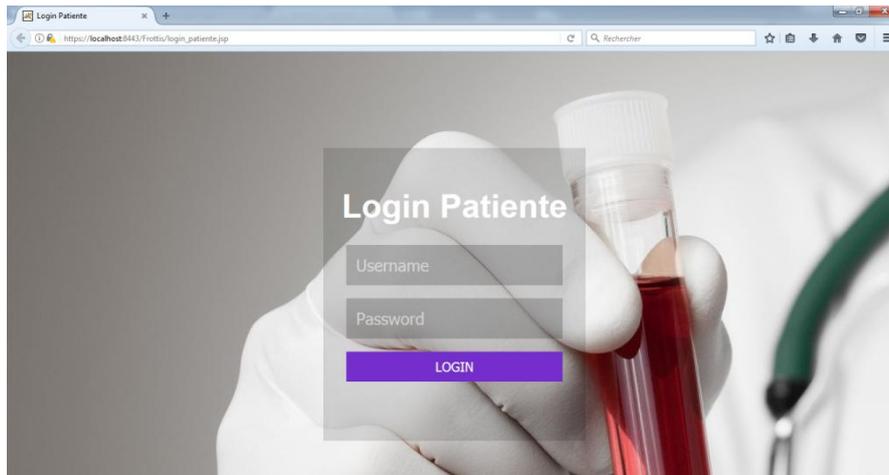
Refaire dans : Dans les meilleurs delais  
 Orienté vers le service : Gynécologie  
 Refaire le frottis dans : 01 ans

dimanche 18 juin

Figure 22:Imprimer de rapport médical

3. **Fenêtre patiente ou d'agent d'un centre médicale** (ils ont les mêmes rôles) :

Ils doivent s'authentifier pour accéder à l'application :



**Figure 23:Fenêtre d'authentification pour la patiente ou l'agent d'un centre médical sur l'application web**

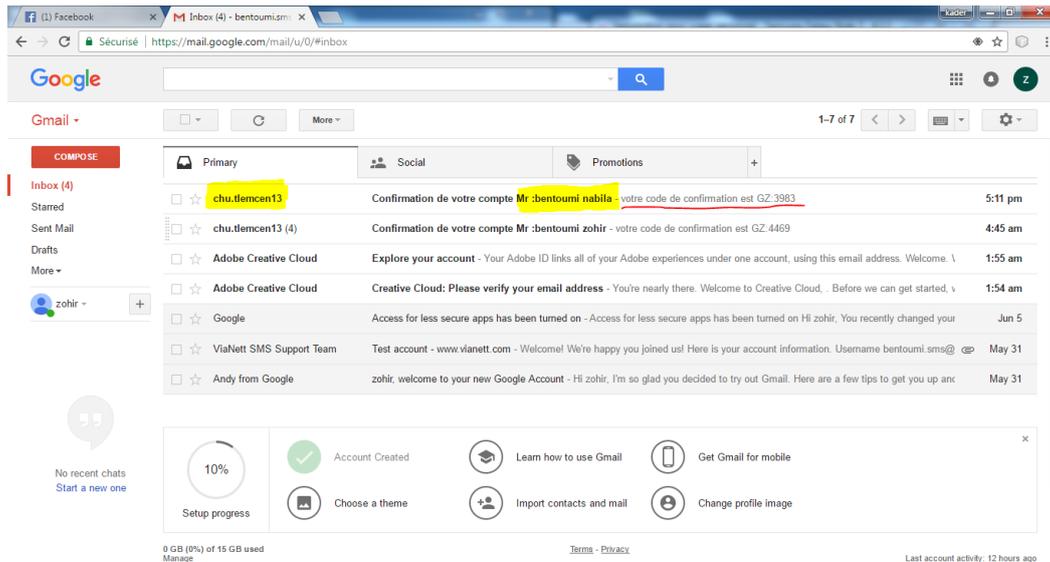
Une fois la patiente/agent du centre se connecte, il peut passer à la consultation et l'impression de résultat, pour cela il faut saisir le code séquentiel de la patiente, après il faut passer par la confirmation du compte par email ou par message (SMS) sur le numéro de téléphone comme suit :

C'est une partie importante de la sécurité de notre application web.



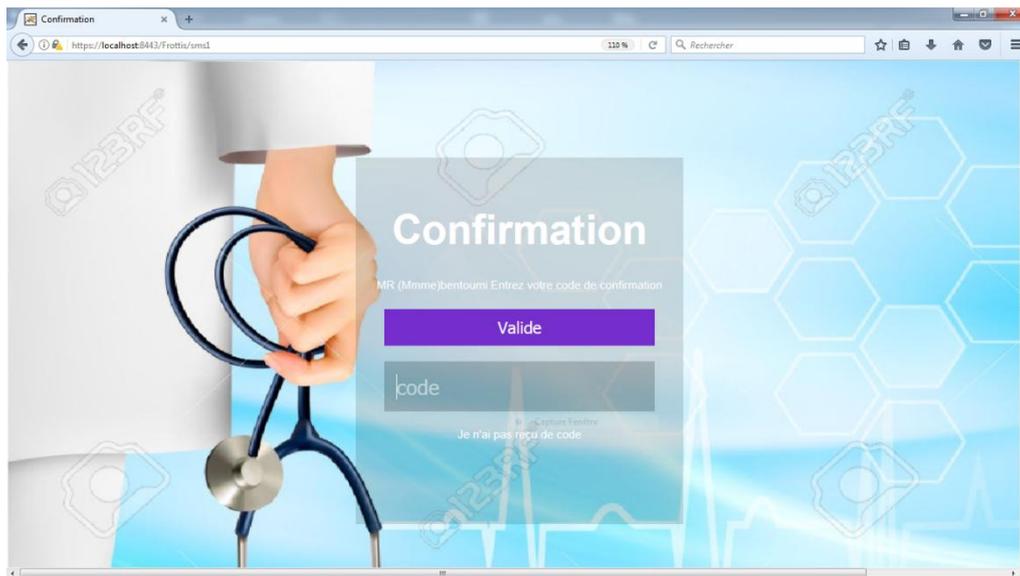
**Figure 24:Fenêtre de choix la méthode de confirmation de compte**

Après il reçoit son code de confirmation sur son email par exemple :



**Figure 25:**Fenêtre de réception de code de confirmation de compte par email

Et après viens l'étape pour entrer le code pour accéder au résultat :



**Figure 26:**Fenêtre d'entrée le code confirmation

En fin ils peuvent consulter le résultat et l'imprimé que ça soit la patiente toute seule ou l'agent d'un centre médical.

### 3.4.2 Application à distance RMI

Cette application est spécifiée pour l'agent d'un centre médical, elle est installée sur un pc pour que la patiente peut consulter ces résultat à partir du centre médicale le plus proche (dans le cas où elle n'a pas des moyens pour consulter toute seule).voici quelque interface.

### 3.4.2.1 Fenêtre authentification

L'agent d'un centre médical à un nom d'utilisateur et un mot de passe qu'il a eu avec l'application pour qu'il puisse accéder au résultat ;



Figure 27:Fenêtre d'authentification pour l'application RMI

### 3.4.2.2 Fenêtre consulter les résultats

Si le rapport médical n'est pas fait cava afficher :

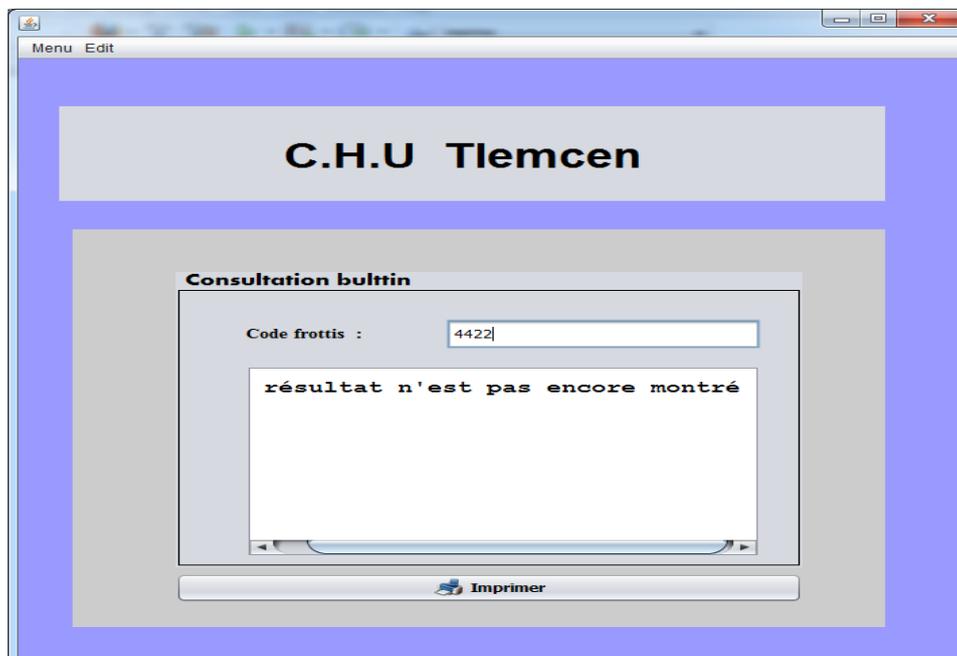


Figure 28:Message de serveur qu'il n'a pas de résultat pour le moment

Sinon il va se transmettre à la fenêtre suivante :

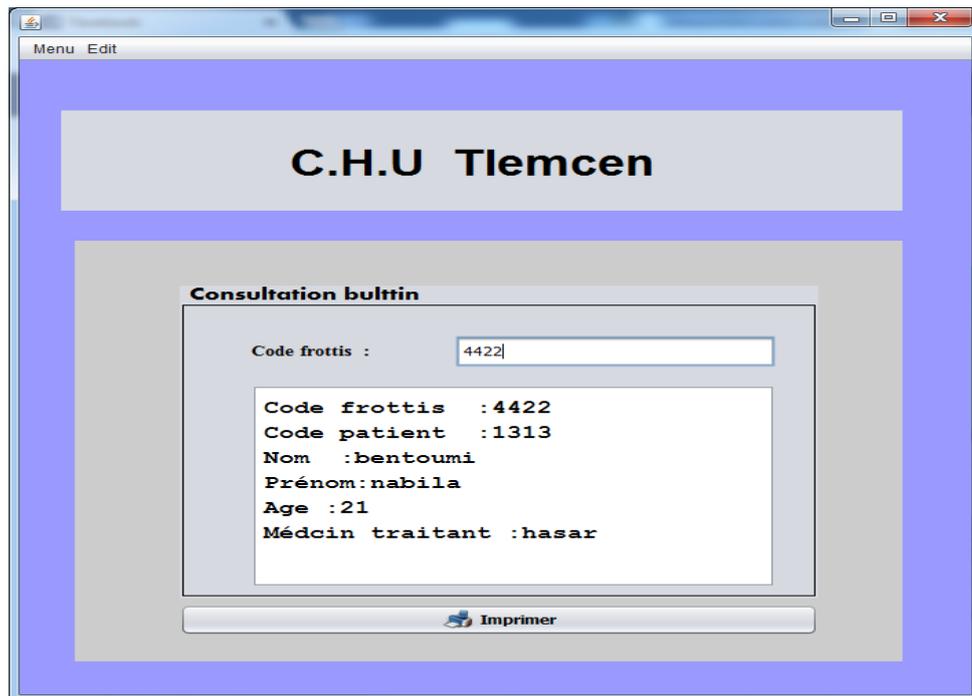


Figure 29:Fenêtre des résultats

Après il peut imprimer le résultat déjà démontré dans la figure (22).

### 3.4.3 Application mobile pour les patientes

Cette application Android est spécialement pour la patiente pour qu'elle puisse consulter ses analyses toute seule sans se déplacer.

Voici quelques interfaces :

#### 3.4.3.1 Fenêtre authentification

Elle doit avoir un nom utilisateur et mot de passe qu'elle a eu avec l'application :

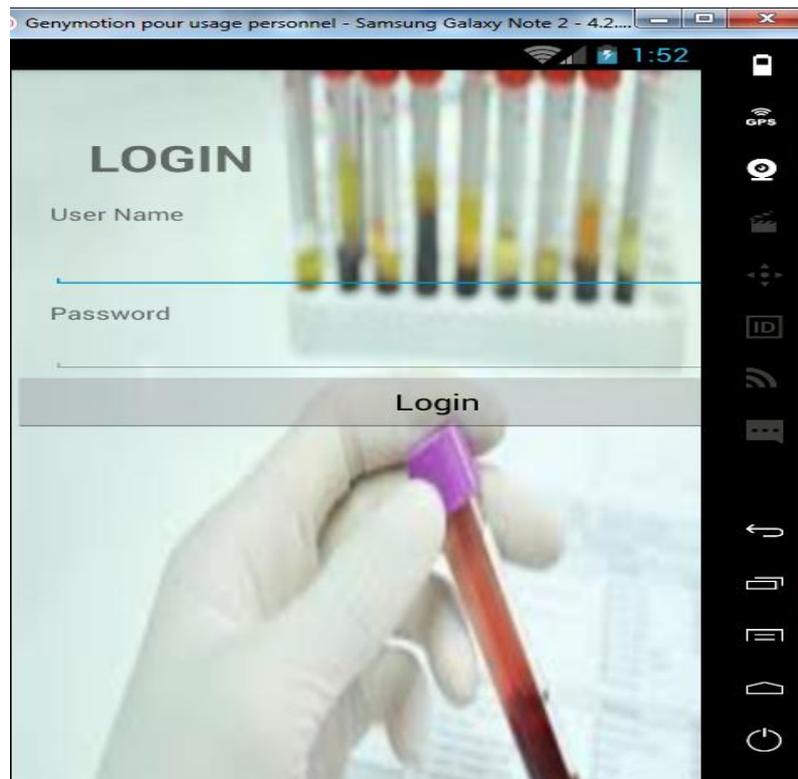


Figure 30:Fenêtre d'authentification pour l'application android

#### 3.4.3.2 Fenêtre consulter les résultats

D'abord elle doit choisir la méthode de confirmation :

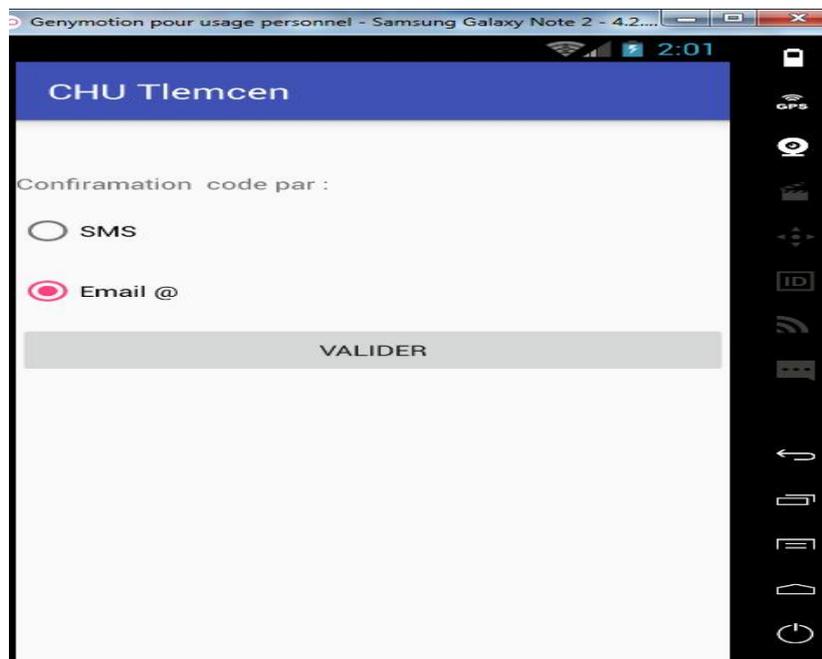
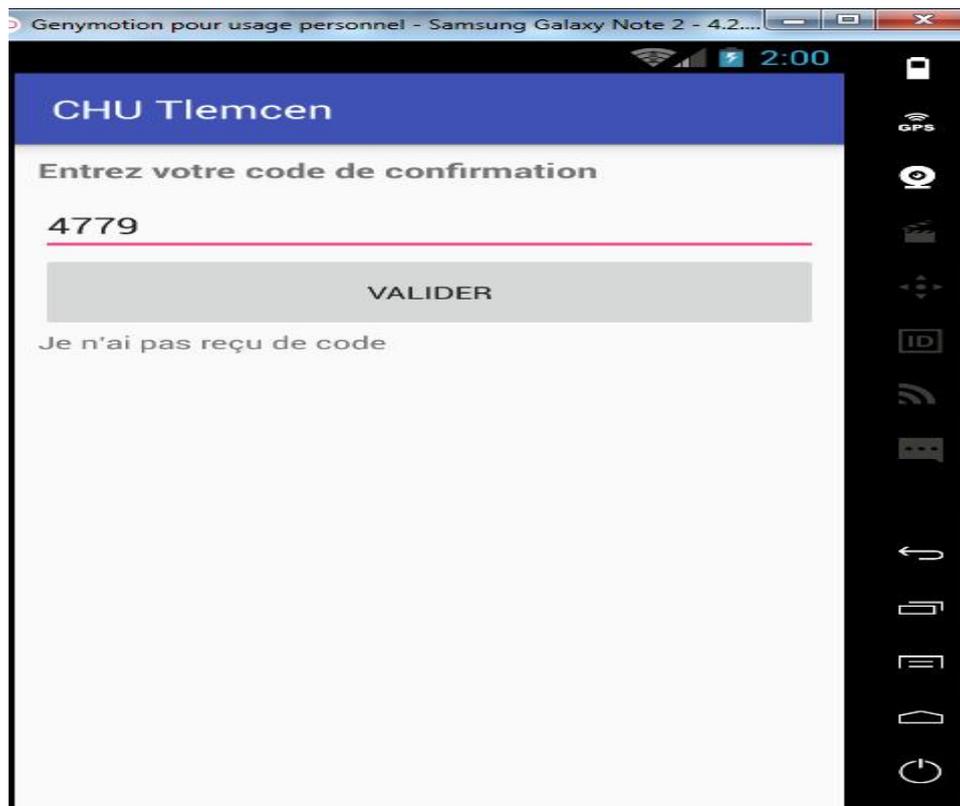


Figure 31:Fenêtre de choisir la méthode de confirmation

Après elle doit entrer son code de confirmation pour accéder au résultat



**Figure 32: Entrer le code confirmation**

En fin elle peut consulter son résultat :

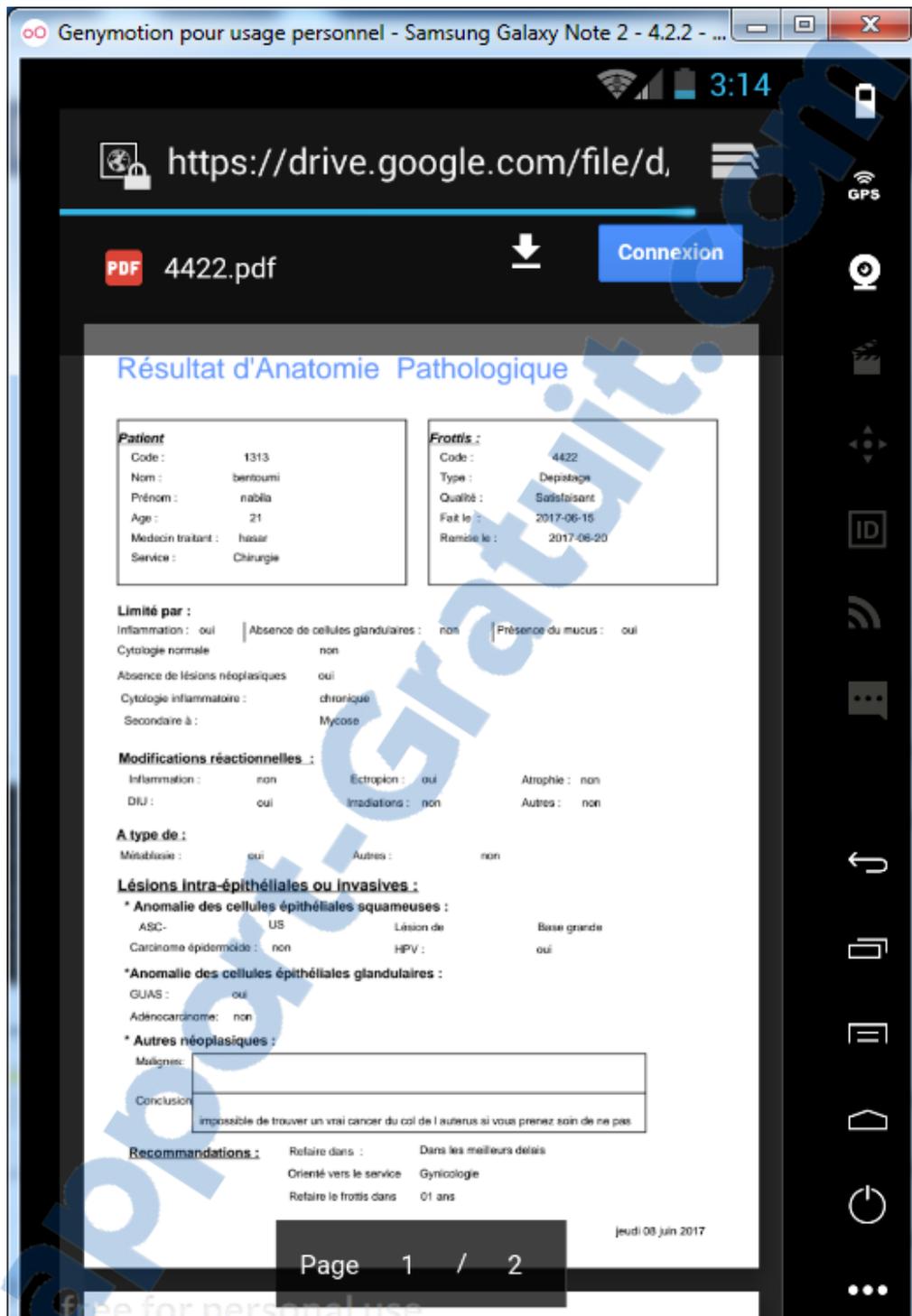


Figure 33: Consultation du résultat par Smartphone

### 3.5 Conclusion

Dans cette partie de notre projet, nous avons présentés les différents outils du développement de notre application ainsi que ses interfaces essentielles réalisé dans notre application web pour clarifier les étapes d'utilisation de notre application.

## **4. Simulation du réseau G- Anlys\_distance en mode sécurité**

## **4.1 Introduction**

Le réseau informatique est une interconnexion des équipements informatiques et de télécommunication en vue de se communiquer et de s'échanger des ressources tant matérielles que logicielles. Pour que ces équipements forment un réseau, ils doivent être mis ensemble et configurés. Cependant, l'implantation d'un réseau informatique, quelle que soit sa taille et son importance, augmente le risque d'altération, de suppression et de piratage de données. Ce risque devient encore plus grand si ce réseau est connecté sur Internet.

Au regard de ce qui précède, nous disons que l'interconnexion, la configuration du réseau et la mise en place d'une politique sécuritaire définitive et adéquate vont occuper le centre de ce chapitre.

## **4.2 Problèmes lié à l'application web**

Nous présentons quelque type d'attaques : [20]

### **A. Buffer overflow**

Une attaque par buffer overflow (dépassement de capacité mémoire) consiste à envoyer en paramètre (dans l'URL ou en POST d'un formulaire) une données dont la longueur excède la taille attendue ou autorisée par le serveur d'application ou l'application en elle-même et remplace la valeur d'autres variables. Cette attaque peut avoir plusieurs types de conséquences.

- obtention de privilèges supplémentaires
- instabilité de l'application ou du serveur
- injection de code malveillant

L'objectif du pirate est alors de mettre en panne le serveur ou l'application, ou plus généralement, d'obtenir des droits d'accès supplémentaires à des fins d'intrusion permettant le vol de données, la destruction du SI où l'attaque d'autres cibles.

### **B. SQL injection**

L'attaque par SQL injection, ou plus généralement par *command injection* consiste à injecter du code malveillant, en l'occurrence une requête SQL dans un paramètre. Si ce

paramètre est insuffisamment contrôlé par l'application et est utilisé au sein d'une commande système, où d'une requête de base de données, alors cette dernière va voir son comportement modifié : des actions non prévues vont être pilotées à distance par un pirate.

Les conséquences d'une telle attaque peuvent être la corruption de données et la prise d'accès frauduleux sur le serveur.

### C. Cookie poisoning

Une session est identifiée par un identifiant stocké chez le client sous la forme d'un cookie conservé par le navigateur web. Le serveur va rattacher un internaute à sa session via l'identifiant fourni par le client. Il est donc naturel que les pirates cherchent à pirater les cookies.

### D. Session hijacking

L'attaque par *session hijacking* est une spécialisation de *cookie poisoning* destinée à prendre le contrôle d'une session utilisateur. Il existe plusieurs types de session hijacking :

L'**interception** consiste à intercepter un cookie par écoute du réseau entre le serveur et le client. Une sonde réseau permet au pirate d'écouter le trafic et d'intercepter les informations échangées.

La **prédiction** est l'art de deviner un identifiant de session valide. Cette attaque concerne les serveurs dont l'algorithme de génération de cet identifiant permet sa prédictibilité. Ainsi, avec un peu d'analyse, en fonction de certaines informations connues (un login courant ou obtenu de façon légitime, la date, et autres informations que l'on peut obtenir facilement...), le pirate peut forger un identifiant rattaché à une session en cours.

La **force brute** permet de trouver un identifiant valide par des tentatives massives en générant un grand nombre d'identifiants et en exploitant sa prédictibilité.

La **fixation** cherche à imposer un identifiant arbitraire à un utilisateur donné. Pour réaliser cette attaque, le pirate doit créer cette session sur l'application, pousser un utilisateur à se connecter à l'application (souvent par phishing), puis se connecter lui-même à la session

lorsque l'utilisateur se sera connecté. Le pirate va typiquement utiliser un outil requêtant l'application régulièrement jusqu'à ce que le formulaire d'authentification disparaisse.

### **4.3 Logiciels utilisés pour la simulation**

Pour la simulation du réseau de notre système nous avons utilisé les logiciels suivants :

#### **4.3.1 GNS3**

Est un **simulateur** d'équipements Cisco. Cet outil permet de charger de véritable IOS Cisco et de les utiliser en simulation complète sur un simple ordinateur. [21]

#### **4.3.2 Kali linux**

Pour **tester la sécurité** de notre application nous avons utilisé le logiciel Kali Linux comme un hacker. Kali Linux est une distribution Linux dérivée de Debian et un membre de la famille d'OS UNIX. Il est un analyseur de paquets libre utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, ...ect, il peut fonctionner même dans une machine virtuelle, donc il flexible. [22]

#### **4.3.3 VirtuelBox**

Pour pouvoir connecter plusieurs machines au gns3 nous avons utilisé. VirtuelBox qui est une application de virtualisation de plateformes croisées. D'une part, il s'installe sur les ordinateurs existant basés sur Intel ou AMD, qu'ils soient sous les systèmes d'exploitation Windows, Mac, Linux ou Solaris. D'autre part, il augmente la capacité de l'ordinateur existant pour qu'il puisse lancer plusieurs systèmes d'exploitation en même temps (dans plusieurs machines virtuelles). VirtualBox est résolument simple bien que très puissant. Il peut se lancer partout, depuis de petits systèmes embarqués jusqu'aux machines de bureau en passant par des déploiements en Datacenter ou même des environnements en nuages. [23]

### **4.4 Intérêt de sécuriser notre système**

Lorsque des analyses sont pratiquées, il existe toujours un certain degré d'inexactitude. Le défi est de réduire autant que possible le niveau d'inexactitude, en tenant compte des limites de nos systèmes d'analyse.

- **Les conséquences négatives d'une erreur de laboratoire**

Les laboratoires produisent des résultats d'analyses qui sont largement utilisés à des fins cliniques ou de santé publique, et les bénéfices pour la santé dépendent de la justesse de ces analyses et du rendu des résultats. Si des résultats inexacts sont rendus, les conséquences peuvent être très graves :

- Traitements inutiles ; complications du traitement.
- Traitement inapproprié.
- Retard dans l'établissement d'un diagnostic correct.
- Analyses supplémentaires et inutiles.

Ces conséquences entraînent une augmentation en coût, en temps, en ressources humaines et n'apportent aucun bénéfice au patient. [24]

#### **4.5 La sécurisation d'une application web**

La sécurité des applications Web est devenue un enjeu stratégique aussi important que les fonctionnalités ou l'ergonomie, d'ailleurs les utilisateurs y attachent de plus en plus d'importance. Pour cela la protection d'échange ou la protection du réseau par rapport aux couches OSI, les protocoles et services de sécurité sont insérés à divers emplacements de la pile de communication. Le choix de l'emplacement dépend des exigences en matière de sécurité, c'est-à-dire les menaces qui peuvent être rencontrées. Chaque emplacement offre des avantages et des inconvénients. [25]

##### *4.5.1 Sécurité au niveau de la couche d'application*

Un mécanisme de sécurité au niveau de la couche d'application procure une sécurité point à point entre une application s'exécutant sur un hôte via le réseau jusqu'à l'application sur un autre hôte. Il existe plusieurs mécanismes de sécurité. Citons-en le protocole que nous avons utilisé dans notre projet.

–**HTTPS** (Hypertext Transfer Protocol Secure ou protocole de transfert hypertexte sécurisé) est un protocole de communication Internet qui protège l'intégrité ainsi que la confidentialité des données lors du transfert d'informations entre l'ordinateur de l'internaute et le site. Les internautes s'attendent à bénéficier d'une expérience en ligne sécurisée et confidentielle lorsqu'ils consultent un site Web.

### 4.5.2 Sécurité au niveau de la couche de transport

De nombreux mécanismes de sécurité au niveau de la couche de transport demandent la modification des applications afin d'obtenir les avantages de la sécurité. Les applications sécurisées interviennent en remplacement des applications non sécurisées par le fait que les serveurs utilisent des ports différents. Il existe plusieurs essais de tels mécanismes de sécurité. Citons-en les deux que nous avons utilisés dans notre configuration de réseau.

– **SSL** (Secure Sockets Layer) a été conçu à l'époque où son navigateur web était largement prédominant) et est largement utilisé sur Internet pour des transactions web telles que l'envoi de données de carte de crédit, avec HTTPS. C'est un protocole de sécurisation de toute sorte de trafic de données sur un réseau. SSL fonctionne suivant un mode client-serveur. Il fournit quatre objectifs de sécurité importants :

- L'authentification du serveur.
- La confidentialité des données échangées (session chiffrée).
- L'intégrité des données échangées.
- De manière optionnelle, l'authentification du client avec un certificat numérique.

En fait SSL est plus général et peut également être utilisé pour d'autres protocoles d'application comme Telnet, FTP, LDAP, IMAP et SMTP.

– **TLS** (Transport Layer Security) est un standard ouvert fondé sur SSL 3.0. SSL et TLS ne procurent la sécurité qu'à une session TCP à la fois, sur laquelle n'importe quelle quantité de données peut être envoyée en toute sécurité. Le serveur et le navigateur doivent être activés SSL ou TLS pour qu'une connexion web sécurisée puisse être établie.

### 4.5.3 Sécurité au niveau de la couche réseau

Les mécanismes de sécurité au niveau de cette couche sécurisent le trafic pour toutes les applications et protocoles de transport des couches supérieures pour que les applications n'aient pas à être modifiées. On va citer deux mécanismes que nous avons étudiés.

– **Les protocoles IP Sec** (IP Security, peuvent fournir le contrôle d'accès, l'authentification, l'intégrité des données et la confidentialité pour chaque paquet IP entre deux nœuds réseau (hôte ou passerelle). Aucune modification du matériel ou du logiciel réseau n'est nécessaire pour router IPSec. Les applications et les protocoles de niveau supérieur peuvent rester

inchangés. IPSec est à la base des réseaux virtuels (VPN pour Virtual Private Net) qui permettent d'accéder à l'intranet de son université ou de son entreprise sur un site délocalisé.

– **Le filtrage** permet de bloquer certains paquets au niveau des routeurs ou autres appareils de couche réseau. Les décisions de routage ou d'abandon sont fondées sur les règles d'une liste de contrôle d'accès proprement dites. Les listes d'accès standard effectuent un filtrage d'après l'adresse source.

#### *4.5.4 Sécurité au niveau de la couche d'accès*

La sécurité pour la couche d'accès est effectuée entre deux points, par exemple sur une ligne louée ou un circuit virtuel permanent. Des périphériques matériels dédiés sont situés à chaque extrémité du lien pour effectuer le chiffrement et le déchiffrement. Ces mécanismes sont surtout susceptibles d'être utilisés par les militaires et les organisations financières comme les banques. Nous avons cité précédemment quelques mécanismes de sécurité des réseaux informatique (PGP, SSL, filtrage, IPSec,...).

#### **4.6 Sécurisation de l'application mobile**

Pour sécuriser l'accès des patientes a leurs comptes, contre le vol de code séquentiel et ses risques : comme l'usurpation d'identité ou le vol de données nous avons utilisé l'authentification à deux facteurs (l'authentification forte).

**L'authentification forte:** l'authentification à deux facteurs est un procédé faisant appel à deux étapes de vérification pour sécuriser l'accès à un profil personnel rattaché à un service de type messagerie, espace de stockage, réseau social, etc. Après une première étape d'identification (couple identifiant/mot de passe), vient une étape d'authentification qui conditionne l'accès au compte d'utilisateur. Elle nécessite de renseigner dans un formulaire un mot de passe de confirmation à usage unique envoyé par SMS sur téléphone ou sur email, et cette technique utilise besoin des deux facteurs suivants:[26]

**Simple Mail Transfer Protocol(SMTP) :** Protocole standard de transfert de courrier entre deux serveurs de messagerie. Avant chaque envoi de message, SMTP vérifie auprès des différents FAI que l'adresse du destinataire existe réellement. Si ce n'est pas le cas, le message revient automatiquement dans la boîte aux lettres de l'expéditeur. [27]

➔ Utilise le port 25 via Telnet.

- ➔ Utilise le port 587 par authentification
- ➔ SMTP utilise TCP pour le transfert des données

**SMS gateway** : Une passerelle SMS permet à un ordinateur pour envoyer ou recevoir Short Message Service transmissions (SMS) ou d'un réseau de télécommunications. La plupart des messages sont finalement acheminés vers les réseaux de téléphonie mobile . De nombreuses passerelles SMS supportent la conversion des médias à partir du courrière électronique et d'autres formats. [28]

## 4.7 La simulation

### 4.5.1 Topologie de notre réseau

La topologie est une représentation d'un réseau. Cette représentation peut être considérée du point de vue de l'emplacement des matériels, se représente souvent par un schéma qui réunit l'ensemble des postes, des périphériques, du câblage, des routeurs, des systèmes d'exploitation réseaux, des protocoles, ect...

La figure 34 présente notre topologie

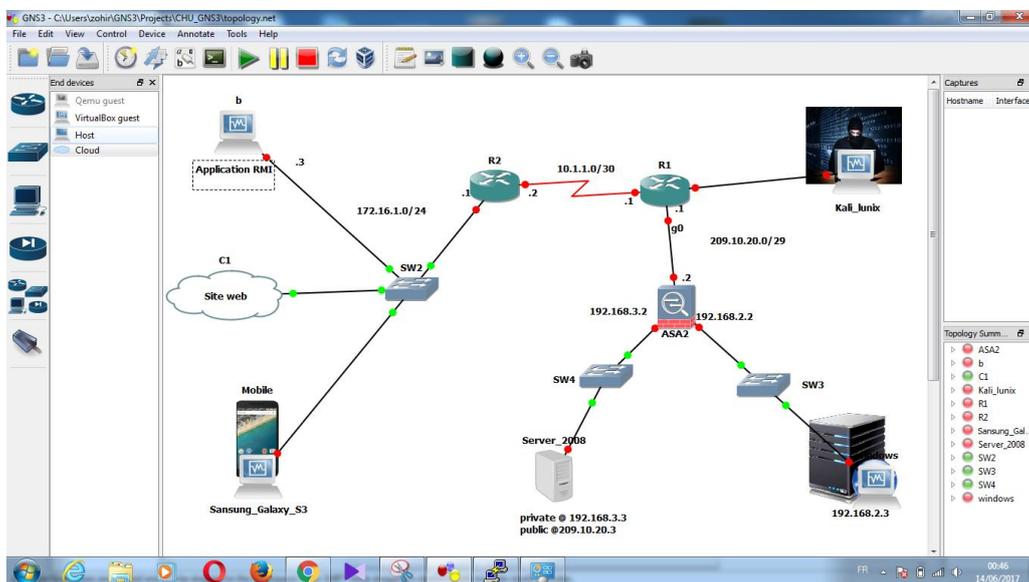


Figure 34:Topologie de notre réseau

### 4.5.2 Les équipements d'interconnexion

Les équipements à utiliser dépendent comme pour les constituants du réseau, de la taille et de l'importance de ce réseau. Plus généralement, nous avons utilisé :

- **Commutateur** : le commutateur (Switch) est intelligent. Le Switch est à mesure de diriger une requête vers le port de sortie approprié grâce à sa table d'adresse.

- **Routeur** : le routeur est un équipement qui peut jouer trois rôles : interconnecter les réseaux de nature (technologie) différente ; assurer le routage des paquets entre ces réseaux ; déterminer le chemin qu'un paquet peut emprunter (grâce à sa table de routage).

- **Firewall** : est un système de sécurité. L'objectif principal d'un pare-feu est de contrôler le trafic entrant et sortant d'un réseau en analysant les paquets de données et en déterminant si le trafic est autorisé à transiter, en fonction des règles prédéterminées. Un pare-feu réseau crée un pont entre un réseau interne considéré comme sécurisé et un autre réseau, généralement un (inter-) réseau externe, comme l'Internet, qui n'est pas considéré comme sécurisé. [29]

-**les machines virtuelles** : nous avons 5 machines virtuelles

1. Une machine pour l'application RMI.
2. Une pour l'application web.
3. Une pour l'application mobile.
4. Une pour le serveur d'application.
5. Une pour le hacker.

-**le câblage**

### 4.5.3 Configuration de routeur

La configuration de routeur R1 et R2 presque la même, pour entrer les adresses IP de chaque interface.

```

R1
description link to asa firewall
ip address 209.10.20.1 255.255.255.248
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial1/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/1
description link to R2
ip address 10.1.1.1 255.255.255.252
serial restart-delay 0
clock rate 64000
!
interface Serial1/2
--More--

```

Figure 35: Configuration de routeur R1

#### 4.5.4 Configuration de ASA (firewall)

Premièrement configuré les interfaces de asa outside et inside comme le montre la figure (36)

```

ASA2
ASA Version 8.4(2)
!
hostname ASA
domain-name asa.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0
description link to R1
nameif outside
security-level 0
ip address 209.10.20.2 255.255.255.248
!
interface GigabitEthernet1
description link to windows server
nameif inside
security-level 100
ip address 192.168.2.2 255.255.255.0
!
interface GigabitEthernet2
nameif DMZ
security-level 70
<--- More --->

```

Figure 36: Configuration de ASA

#### ➤ Configuration de VPN SSL sous ASA

Les commandes générales de pare-feu gèrent les fonctions généralement utilisées par les navigateurs et les applications Internet ; parmi ces fonctions le VPN SSL.

**Définition VPN :** Un réseau VPN (réseau privé virtuel) est une connexion entre deux points de terminaison situés dans différents réseaux, qui permet l'envoi sécurisé de données privées sur un réseau partagé ou public, comme Internet. Ce tunnel permet de créer un réseau privé capable d'envoyer des données cryptées de manière sécurisée. [30]

Pour effectuer la configuration de VPN SSL nous avons besoin de deux éléments essentiels :

- **Le serveur TFTP :** Le serveur TFTP : (**T**rivial **F**ile **T**ransfert **P**rotocol) est un protocole simplifié de transfert de fichiers, il est très utilisé pour la mise à jour des logiciels embarqués sur les équipements réseaux (routeurs, pare-feux, ...ect). [31]. Il est installé dans la machine virtuelle de serveur d'application.
- **Le Cisco ASDM Launcher pour ASA :** ASDM (Adaptive Security Device Manager) est un outil de configuration basé sur l'application conçu pour vous aider à installer, configurer et contrôler votre pare-feu avec une interface graphique. [32]

Le serveur TFTP va **transférer** le fichier bin de ASDM depuis notre serveur d'application vers le ASA, ensuite on effectua la configuration de ce fichier avec les règles qui correspond à notre réseau. Au final le ASA va générer le Cisco ASDM Launcher, et au lancement d'un navigateur avec https : 192.168.2.2 (adresse de serveur) on obtient la fenêtre d'authentification pour effectuer l'installation de ASDM Launcher.



**Figure 37:Fenêtre d'installation de ASDM**

Ensuite on peut connecter à Cisco ASDM Launcher



Figure 38:Fenêtre de Cisco ASDM Launcher

Puis nous avons l'interface de travail Cisco ASDM pour notre ASA suivante :

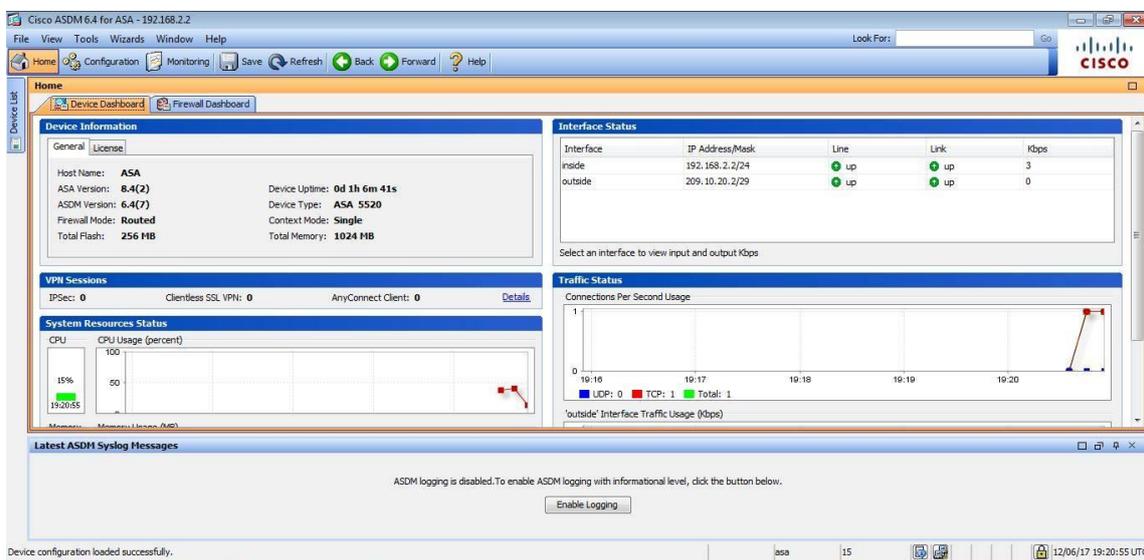


Figure 39:Fenêtre de Cisco ASDM pour ASA

Nous commençons par la configuration des serveurs depuis notre espace de travail de ASDM Launcher:

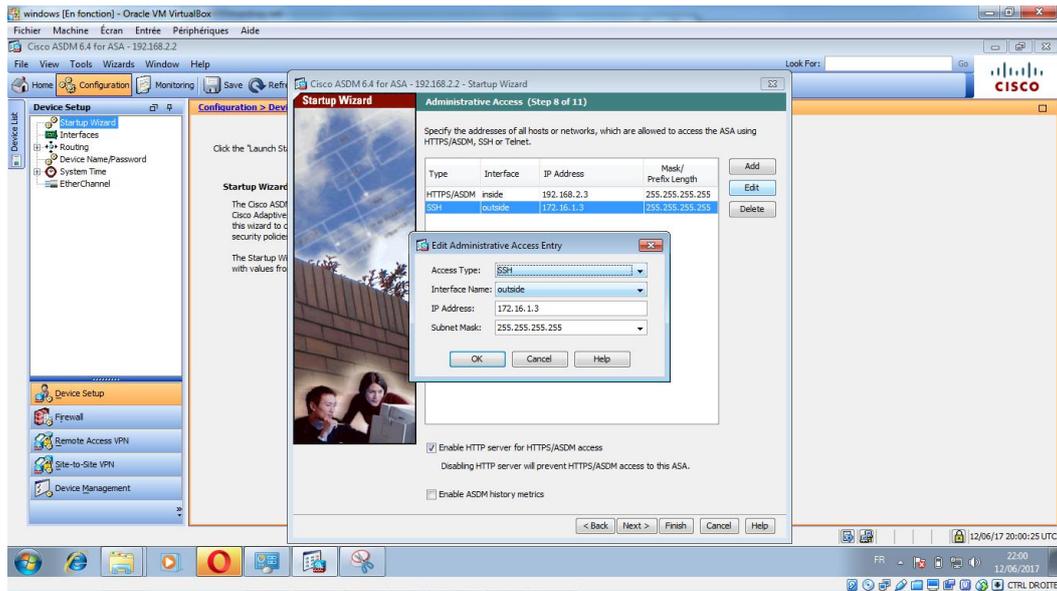


Figure 40: Fenêtre de configuration

Le Cisco ASDM Launcher contient même le Cisco ASDM Packet Tracer pour vérifier comment les paquets passent de la source vers la destination.

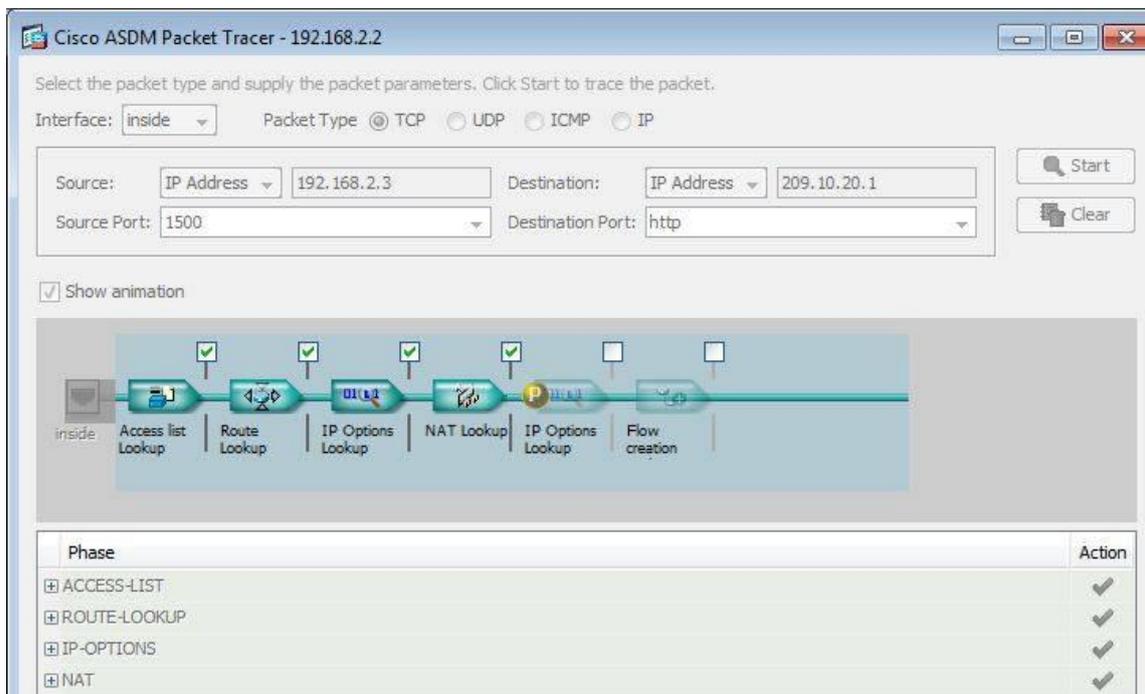


Figure 41: Fenêtre de Cisco ASDM Packet Tracer

Après la configuration des serveurs, nous devons créer les clients SSL VPN. Le mode Clientless SSL a pour but de permettre un accès à distance sécurisé grâce à un simple navigateur internet.

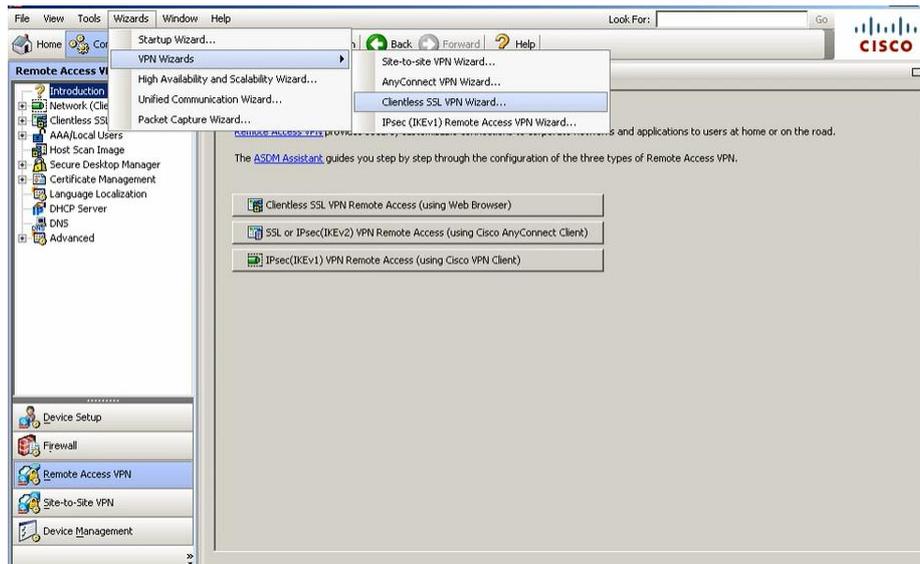


Figure 42:Fenêtre de configuration de Clientless SSL VPN

On obtient la création réussie.

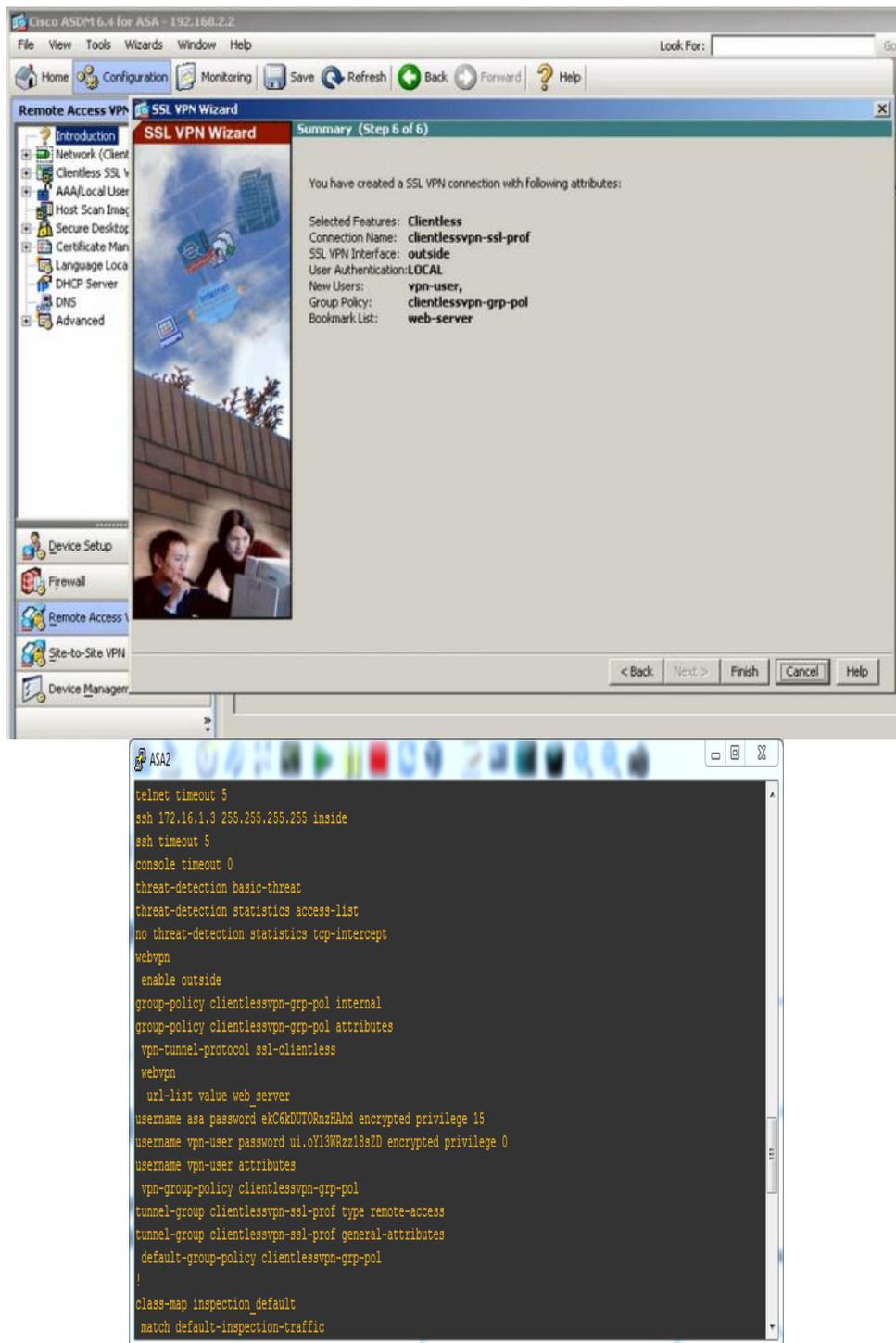


Figure 43: Création réussie de SSL VPN connexion

Finalement notre réseau sécurisé avec un certificat SSL.

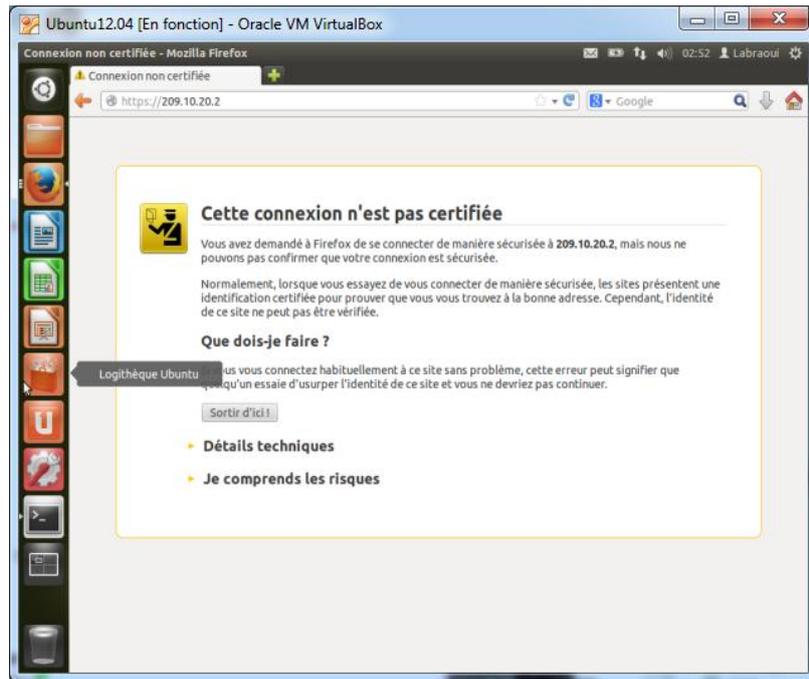


Figure 44: Page de certificat

Lorsque la secrétaire veut accéder à une ressource interne, les données sont sécurisées avec le protocole HTTPS et transmises cryptées par SSL à travers le tunnel créé entre l'interface physique du secrétaire et l'interface de l'ASA reliée vers l'extérieur, comme le montre la figure suivante :

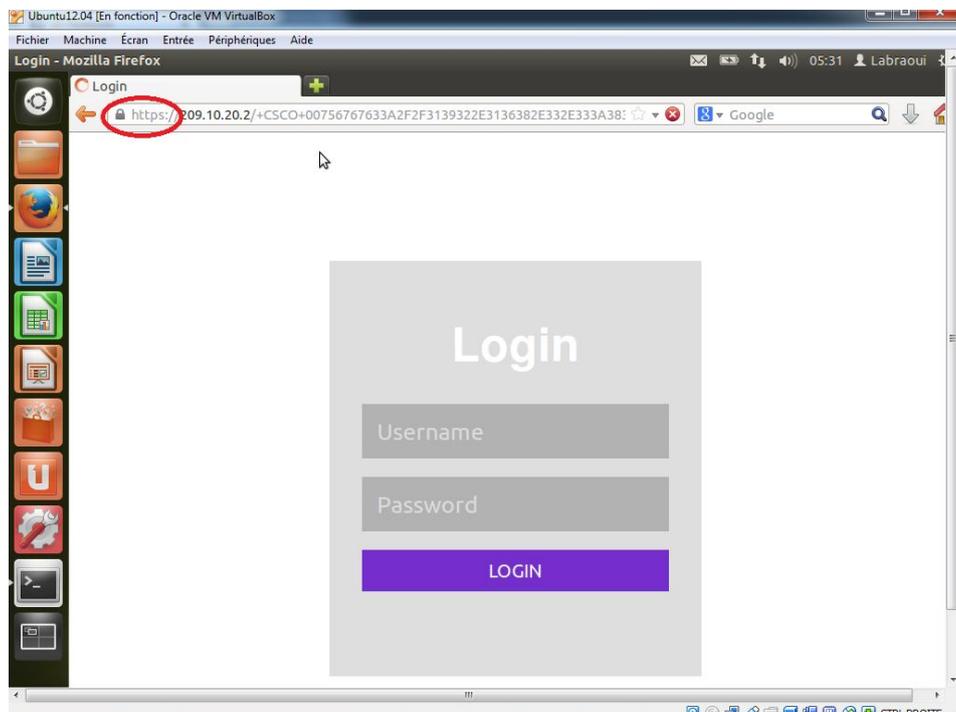


Figure 45: Fenêtre d'authentification de secrétaire après la sécurisation

### 4.5.5 Exemple d'une attaque de réseau avec le Kali Linux

Après la configuration des protocoles, on va tester la sécurité de notre réseau, nous avons organisé deux attaques par l'Owasp et le wearchark qui sont des outils de Kali Linux.

→ le **Owasp** (Open Web Application Security Project) qui permet de scanner notre application web. On met comme URL d'attaque le lien de notre application web, et on commence l'attaque, suivant la figure 46

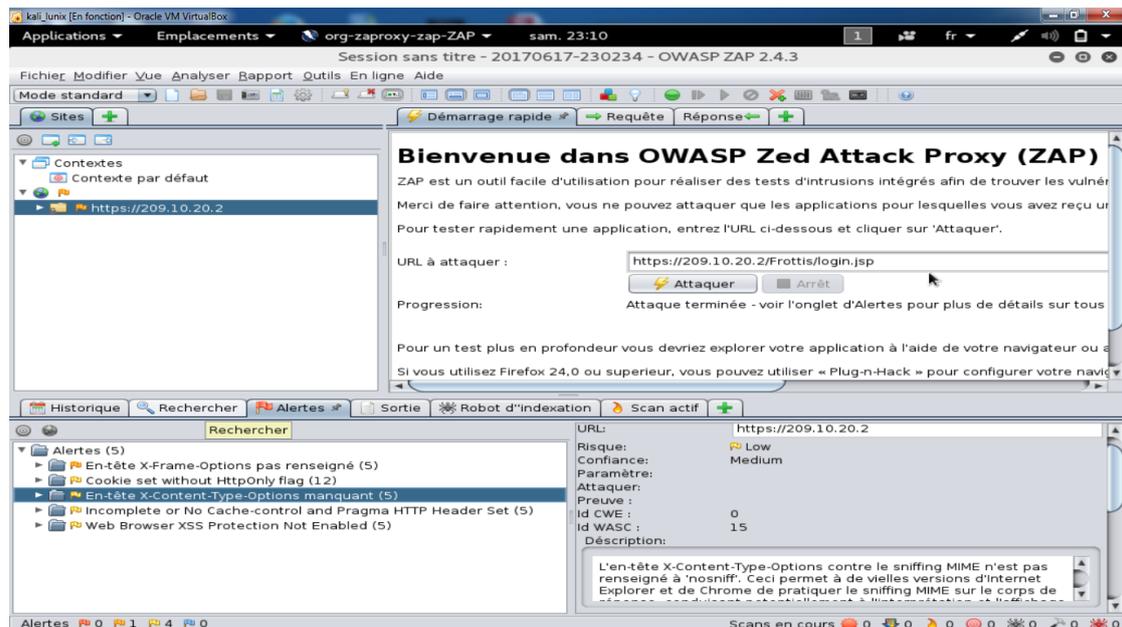


Figure 46:Fenêtre principal d'attaque avec Owasp

Après le scan on obtient comme résultat la fenêtre suivante :

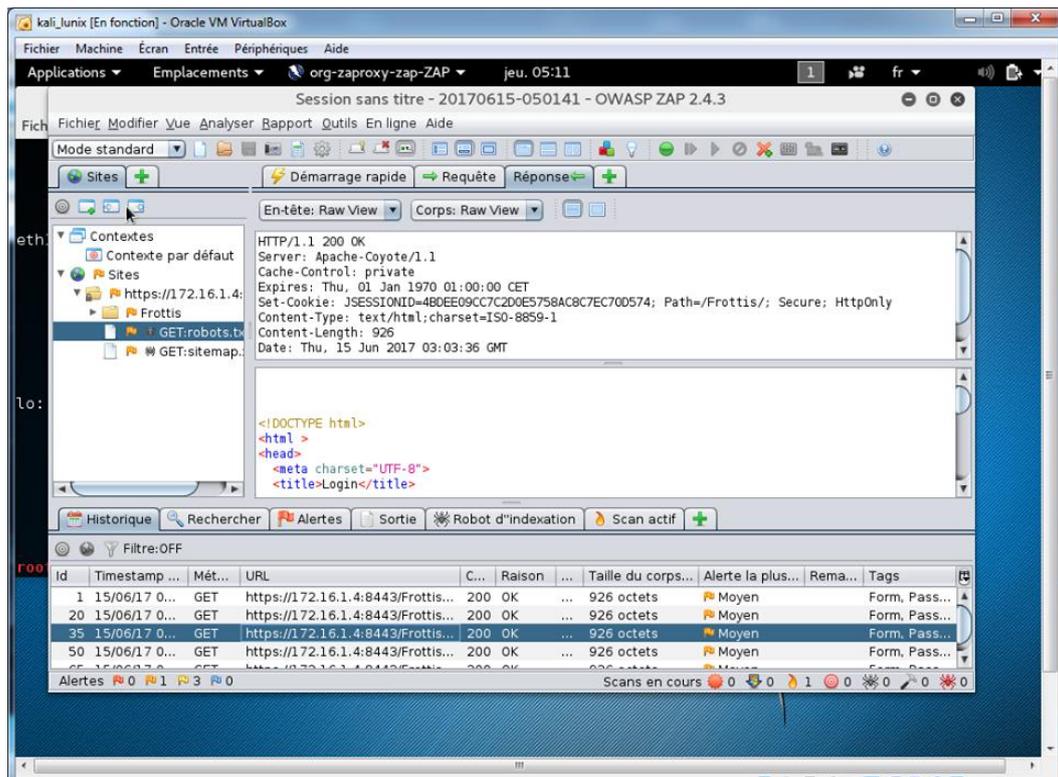


Figure 47: Résultat d'attaque d'Owasp

Remarque au dessous dans la fenêtre en trouve les alertes de sécurité, ya pas d'alerte rouge qui est le plus danger ; ya que le drapeau orange et jaune. Donc notre application n'est pas sécurisée 100% car on n'avait pas le temps pour éliminer tous les failles, mais nous avons sécurisé la partie la plus importante de transfert des fichiers.

➔ **Wirshark** : est très pratique pour monitorer un réseau et regarder ce qui s'y passe, ce qui y transite.

Nous jouons le rôle d'un Sniffer pour intercepter les paquets qui circulent sur notre réseau. cela nous donne donc la possibilité d'intercepter tout type d'informations émises à travers le réseau. Par conséquent afficher à la fois l'identité des utilisateurs au même titre que leurs mots de passe, surtout lorsque ces informations sont transférées par des protocoles qui ne sont pas suffisamment sécurisés comme : la DNS (Domain Name System) ou encore le HTTP (Protocole de transfert hypertexte), mais dans notre cas nous avons utilisé le HTTPS et le protocole SSL pour assurer la sécurité de notre réseau

1. Après choisir l'interface de réseau intercepté, le sniffer se présente comme le montre la figure suivante :

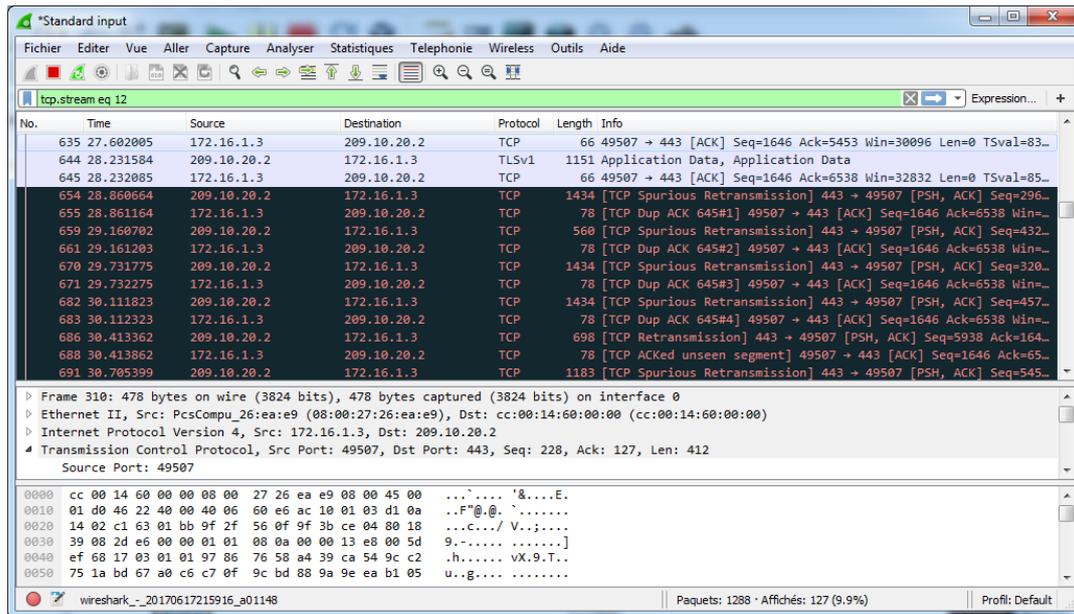


Figure 48:le scan des paquets de notre réseau (Attaque Sniffing)

On peut voir que la fenêtre de Wireshark est, par défaut, divisée en 3 sections:

- la première affiche une liste des paquets IP capturés
  - la seconde donne le détail du paquet IP sélectionné dans la première section
  - la troisième affiche le contenu (en hexadécimal) du paquet IP sélectionné dans la première section
2. Après on fait notre analyse dans la barre d’outils avec le follow TCP Stream on obtient les résultats suivants :

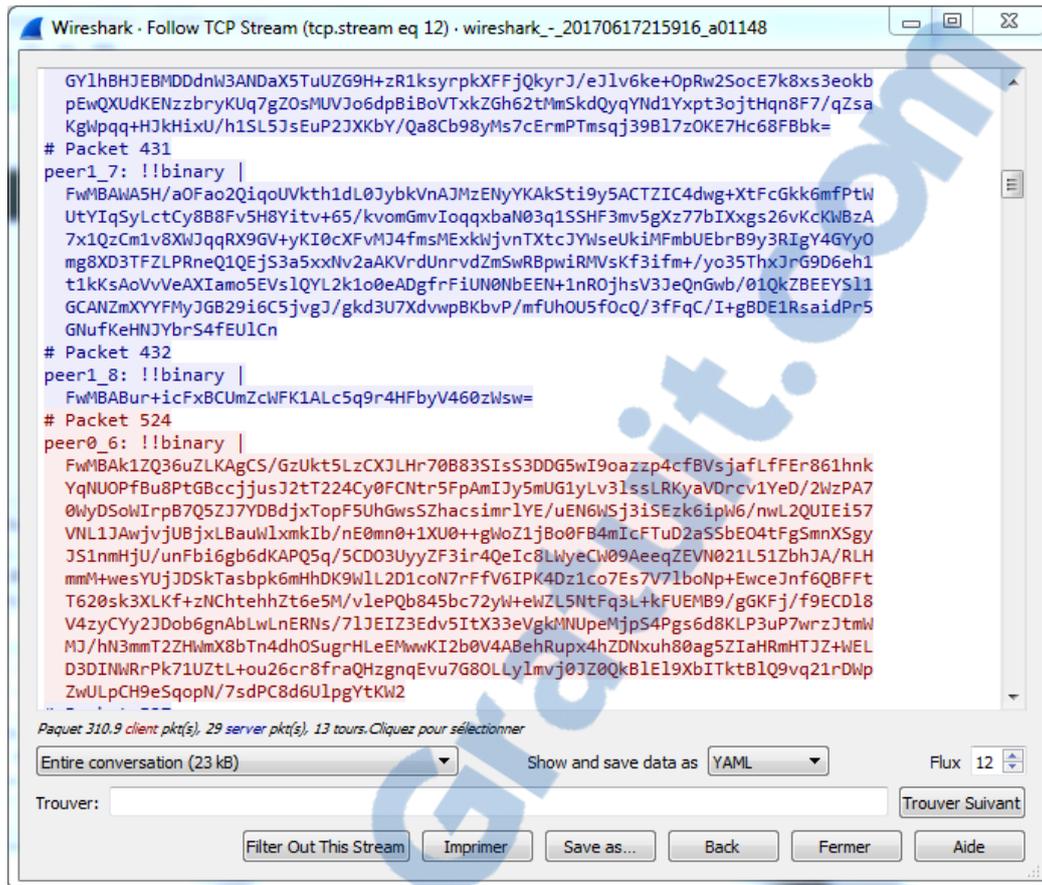


Figure 49: Fenêtre d'analyse les paquets sniffé par Wirshark

On remarque que toutes les données sont cryptées, on ne peut obtenir aucune information.

Donc notre réseau est sécurisé.

#### 4.8 Conclusion

Dans ce dernier chapitre nous sommes intéressé pour travailler dans la sécurité réseau de notre projet, nous a permis d'avoir un premier aperçu du domaine et d'acquérir des compétences qui nous seront utiles pour passer la certification CISCO sécurité.

# Conclusion générale

## Conclusion générale

« G-Anlys\_distance ». Ce dernier comporte trois applications une application web pour laboratoire d'hôpital CHU Tlemcen sous le framework J2EE, afin de pallier les limites du déroulement du travail existant au service d'anatomie et de cytologie pathologiques

Conformément à ce que nous avons spécifié, nous sommes parvenus à mettre en œuvre un système sous le nom de G-analys\_distance. Ce travail était l'occasion d'appliquer dans un cadre professionnel les connaissances acquises durant nos années d'étude. En effet il mêlait plusieurs disciplines.

Enfin les fonctionnalités offertes par cette application sont immenses, il nous a permis de bien familiariser à programmer en J2EE , utilisant aussi des architectures MVC et RMI.

Mais pour conclure, il existe toujours des améliorations à envisager pour rendre une application encore performante par exemple :

- Rendre les rapports accessible à d'autres services concerné tel que service d'oncologie, de gynécologie, de radio-thérapie,
- Construire un entrepôt de données de données qui permet l'analyse des données à des fins de prise de décision, statistiques...
- Aussi de réaliser un site Web consacré à l'application à fin de pouvoir la commercialiser.

# Webographie

- [1] : CHU Tlemcen. (s.d.). Consulté le 03 25, 2017, sur Centre Hospitalo-Universitaire Dr Tidjani Damerdji de Tlemcen: <http://www.chu-tlemcen.dz>
- [2] : CHU Tlemcen. Consulté le 04 14, 2017, sur CHU Tlemcen: <https://www.facebook.com/ChuTlemcen-1179379938767431/>
- [3] : Anatomopathologie, consulter le 01/04/2017 , sur <http://fr.wikipedia.org/w/index.php?title=Anatomopathologie&oldid=135353723>
- [4] : Benchimol, D . Consulté le 04 17, 2017, sur Docteur Benchimol : <https://docteur-benchimol.com/gynecologie/22-frottis-cervico-vaginal.html> .
- [5] : Baillet, P. Cancérologie. Consulté le 04 1, 2017, sur FACULTÉ DE MÉDECINE Pierre et Marie curie: <http://www.chups.jussieu.fr/polys/cancero/POLY.Chp.9.4.html> .
- [6] : UML. Consulté le 04 15, 2017, sur Wikipedia: [https://fr.wikipedia.org/wiki/UML\\_\(informatique\)](https://fr.wikipedia.org/wiki/UML_(informatique)) .
- [7] : Sophnouille. Consulté le 04 25, 2017, sur developpez.com: <http://sabricole.developpez.com/uml/tutoriel/unifiedProcess> .
- [11] : Java RMI . Consulté le 05 2, 2017, sur laboratoire d'informatique fondamentale de marseille : <http://pageperso.lif.univ-mrs.fr/~arnaud.labourel/PPD/cours6.pdf>
- [13] : Oracle. (s.d.). Java. Consulté le 05 11, 2017, sur Oracle: [https://java.com/fr/download/faq/whatis\\_java.xml](https://java.com/fr/download/faq/whatis_java.xml) .
- [14] : Définition . (s.d.). Consulté le 05 15, 2017, sur journalDuNet: [http://www.journaldunet.com/encyclopedie/php/commun/imprimer\\_definition.php?f\\_id\\_definition=313](http://www.journaldunet.com/encyclopedie/php/commun/imprimer_definition.php?f_id_definition=313) .
- [15] : bibliothèque virtuelle. Consulté le 05 8, 2017, sur Québec: <http://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/internet/fiches/8353961.html>
- [16] : HTML. Consulté le 06 5, 2017, sur wikipedia: [https://fr.wikipedia.org/wiki/Hypertext\\_Markup\\_Language](https://fr.wikipedia.org/wiki/Hypertext_Markup_Language)
- [17] : WebMaster Consulté le 06 2, 2017, sur infoWebMaster: <http://glossaire.infowebmaster.fr/css/>
- [18] : MySQL. Consulté le 06 2017, 5, sur Mosaique informatique: <http://www.mosaique-info.fr/glossaire-web-referencement-infographie-multimedia-informatique/m-glossaire-informatique-et-multimedia/448-mysql-definition.html>

- [19] : JQuery. Consulté le 06 05, 2017, sur JournalDuNet:  
<http://www.journaldunet.com/solutions/pratique/dictionnaire-du-webmastering/technologies-langages/19497/jquery-definition.html> .
- [20] : Etiévant, H. Sécurisé l'application web. Consulté le 06 7, 2017, sur developpez:  
<http://cyberzoide.developpez.com/securite/session/> .
- [21] : Fred. (2007, 11 26). GNS3. Consulté le 05 22, 2017, sur Réseaux et Sécurité :  
<http://www.nemako.net/dc2/?post/GNS3> .
- [22] : Kali Linux. (2017, 05 17). Consulté le 05 25, 2017, sur wikipedia:  
[https://fr.wikipedia.org/wiki/Kali\\_Linux](https://fr.wikipedia.org/wiki/Kali_Linux) .
- [23] : Corporation, O. (2013). Oracle VM VirtuelBox. Consulté le 05 11, 2017, sur Manuel de l'utilisateur: [https://www.virtualbox.org/download/testcase/manual/UserManual\\_fr\\_FR.pdf](https://www.virtualbox.org/download/testcase/manual/UserManual_fr_FR.pdf) .
- [24] : L'importance de la qualité au laboratoire . (s.d.). Consulté le 05 28, 2017, sur World Health Organization:  
[http://www.who.int/ihr/training/laboratory\\_quality/1\\_b\\_content\\_introduction\\_fr.pdf?ua=1](http://www.who.int/ihr/training/laboratory_quality/1_b_content_introduction_fr.pdf?ua=1) .
- [25] : Vue d'ensemble sur la sécurité des réseau informatique, consulté le 05/05/2017; sur :  
<http://lacl.u-pec.fr/cegielski/sec/ch3.pdf>.
- [26] : Authentification forte . Consulté le 06 1, 2017, sur Comment ça marche:  
<http://www.commentcamarche.net/faq/36542-authentification-forte-protoger-l-acces-a-ses-services-en-ligne> .
- [27] : Simple Mail Transfer Protocol. Consulté le 06 5, 2017, sur wikipedia:  
[https://fr.wikipedia.org/wiki/Simple\\_Mail\\_Transfer\\_Protocol](https://fr.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) .
- [29] : Guide d'administration . (s.d.). Consulté le 06 10, 2017, sur cisco:  
[http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv320/administration/guide/fr/rv32x\\_ag\\_fr.pdf](http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv320/administration/guide/fr/rv32x_ag_fr.pdf) .
- [30] : Réseaux privés virtuels-VPN. Consulter le 06 2017, 02, sur FrameIP:  
<http://www.frameip.com/vpn/> .
- [31] : TFTP. (s.d.). Consulté le 06 8, 2017, sur techno-science.net: <http://www.techno-science.net/?onglet=glossaire&definition=3884> .
- [32] : Exemple de configuration. . Consulté le 06 08, 2017, sur Cisco:  
[http://www.cisco.com/c/fr\\_ca/support/docs/security/pix-500-series-security-appliances/67912-pix2pix-vpn-pix70-asdm.html](http://www.cisco.com/c/fr_ca/support/docs/security/pix-500-series-security-appliances/67912-pix2pix-vpn-pix70-asdm.html) .

# Bibliographie

[8] : Lahraichi, S. Consulter le 05/04/2017, Mémoire fin d'études, Monitoring et gestion des dossiers médicaux des patients .

[9 ] : Badr, B. Architecture n – tiers et Frameworks globaux (J2EE vs .Net). Construction d'applications réparties , consulter 2017. p. 64 ; Cours Master 2.

[10] : Raphaël Fournier-S'niehotta, P. R. (s.d.). Consulter le 19/05/2017, Mémoire fin d'études ; Applications orientées données (NSY135) . Paris, France, informatique.

[12] : Ghefir Mohamed El Amine, B. S. Consulter le 05/06/2017, Mémoire de fin d'études Développement d'une application distribuée par la méthode Java RMI.

[28] : Amraoui, M. A. Simple Mail Transfer Protocol. Serveurs de messagerie, consulter 2016. p.14 , cours Master 1.

# Résumé

Dans le cadre du programme national de dépistage des lésions précancéreuses et cancéreuses du col utérin, nous avons conçu et réalisé notre système baptisé G-analyse\_distance qui permet la gestion des rapports médicaux des Frottis Cervico vaginal (FCV) du Service d'Anatomie et Cytologie Pathologique du CHU de Tlemcen.

Pour cela, nous avons réalisé 3 applications (application web, application à distance RMI, application mobile) leur objectif principal est de faciliter les tâches du secrétaire, du pathologiste, et de la patiente pour qu'elle consulte ces résultats à distance.

Aussi, la peur de se faire détériorer ou espionner les données des rapports médicaux, nous nous sommes préoccupés à intégrer la sécurité en utilisant quelques protocoles. Pour cela, nous avons effectué deux attaques sur notre système à savoir: une avec Wirshark et une avec Owasp pour s'assurer que nos données restent confidentielles.

**Mot clés:** Frottis, Web application, ASDM, ASA, RMI, VPN SSL.

## Abstract

As part of the national program for screening for precancerous and cancerous cervical lesions, we designed and realized our system called G-analysis\_distance, which allows the management of the medical reports of the Cervico Vaginal Smear (FCV) (belonging) of the Anatomy Department And Pathological Cytology of the Tlemcen University Hospital.

For this, we have realized 3 applications (web application, remote application, mobile application) their main objective is to facilitate the tasks of the secretary, pathologist, and above all of patient to consult these results from a distance.

Also, fear of getting spoiled or spying on data from medical reports, we worried about integrating security into our application using some protocols of security. For this we tested two attacks on our system namely: one with Wirshark and one with Owasp to ensure that our data remain confidential.

**Keywords :** Frottis, Web application, ASDM, ASA, RMI, VPN SSL.

## ملخص:

في إطار البرنامج الوطني المتخصص في الكشف عن سرطان عنق الرحم، قمنا بإنجاز نظام يسمح بإنجاز التقارير الطبية لخدمة تخصص تشخيص الأمراض بالنسبة للمستشفى الجامعي لولاية تلمسان. من أجل هذا لقد حققنا ثلاث تطبيقات لتسهيل عمل كل من السكرتيرة، أخصائي الباثولوجية الخلوية، و للمريضة حيث يمكنها أن تتعرف على نتائجها عن بعد.

ومن أجل حماية هذا النظام من الضرر أو التجسس على البيانات من التقارير الطبية في نظامنا، قمنا أيضا بإدراج بعض البروتوكولات الأمنية لضمان الحفاظ على المعطيات، لتأكيد ذلك قمنا بمحاولة اختراق النظام.

**الكلمات المفتاحية:** عينة، تطبيق ويب، ASDM، ASA، RMI، VPN، SSI.