■ Deepfake Case Management CRM – Incident Reporting & Investigation System

■ Problem Statement

Social media platforms, governments, and organizations face increasing challenges due to deepfake content.

Victims find it hard to report incidents.

Investigations are slow and uncoordinated.

Evidence tracking and approvals are manual.

No centralized dashboards exist to monitor case progress or trends.

■ Solution: Implement Salesforce CRM to create a system for reporting, tracking, and resolving deepfake incidents through automation, integrations, and dashboards.

■ Use Cases

• Incident Reporting – Users report suspected deepfake content through a portal/web form.

• Case Assignment & Investigation – Auto-assign cases to analysts based on workload/region.

• Evidence Management – Store uploaded videos/images as evidence records.

• Integration with AI Deepfake Detection Tools – API integration with external ML models.

• Reporting & Dashboards – Track reported cases, resolution times, escalations, and analyst performance.

Phase 1: Problem Understanding & Industry Analysis

• Requirement Gathering – Collect business needs like reporting, AI verification, and evidence tracking.

• Stakeholder Analysis – Identify roles: reporters, analysts, managers, compliance officers.

• Business Process Mapping – Define flow: Report → Investigation → AI check → Closure.

• Industry-specific Use Case Analysis – Study digital forensics and media handling of deepfakes.

• AppExchange Exploration – Explore compliance/security apps for integration.

Phase 2: Org Setup & Configuration

• Salesforce Editions – Use Enterprise Edition for advanced automation.

• User Setup & Licenses – Create licenses for Analysts, Managers, and Reporters.

• Profiles & Roles – Define permissions and hierarchy (Reporter → Analyst → Manager → Compliance).

• Permission Sets – Grant extra access like running AI checks.

• OWD & Sharing Rules – Keep evidence private and controlled by hierarchy.

Phase 3: Data Modeling & Relationships

• Custom Objects – Deepfake Case, Evidence, Investigation Report.

• Fields – Capture incident details like URL, AI score, and date reported.

• Record Types – Separate Image vs Video Deepfake cases.

• Relationships – Case ↔ Evidence (One-to-Many), Case ↔ Report (One-to-One).

• Schema Builder – Visualize case management relationships.

Phase 4: Process Automation (Admin)

• Validation Rules – Case cannot close without evidence.

• Flows – Auto-assign cases and notify reporters.

• Approval Process – Manager approval required before closure.

• Email Alerts – Notify reporters of status updates.

• Custom Notifications – Push alerts for escalated cases.

Phase 5: Apex Programming (Developer)

• Triggers – Call AI detection API after case creation.

• Batch Apex – Run bulk verification jobs daily.

• Queueable Apex – Process evidence asynchronously.

• Scheduled Apex – Generate weekly compliance reports.

• Exception Handling – Log failed API responses.

Phase 6: User Interface Development

• Lightning App – ‘Deepfake Case Management’.

• Record Pages – Display AI results and case details.

• Tabs – Cases, Evidence, Reports.

• LWC – Evidence preview and Run AI Check button.

• Navigation Service – Redirect to investigation reports.

Phase 7: Integration & External Access

• REST API – Connect with AI detection service.

• Salesforce Connect – Link with law enforcement databases.

• Named Credentials – Secure storage of API keys.

• OAuth – Ensure secure API access.

• Remote Site Settings – Whitelist AI detection domain.

Phase 8: Data Management & Deployment

- Data Import Wizard – Upload sample cases.
- Data Loader – Bulk upload evidence records.
- Duplicate Rules – Prevent duplicate incident reporting.
- Change Sets – Move automation rules to production.
- VS Code & SFDX – Source control for deployments.

Phase 9: Reporting, Dashboards & Security Review

- Reports – Track cases by severity and analyst.
- Dashboards – Monitor volume, resolution time, and escalations.
- Dynamic Dashboards – Role-based insights.
- Field Level Security – Restrict evidence access.
- Audit Trail – Track case status and approvals.

Phase 10: Final Presentation & Demo Day

- Live Demo – Show complete workflow (report → assign → AI check → closure).
- Pitch Presentation – Demonstrate business impact.
- Feedback Collection – From analysts and managers.
- Documentation – Admin/user guide for handoff.
- Portfolio Showcase – Publish as an advanced Salesforce project.