📘 Salesforce Project Documentation – Deepfake CRM

🔹 Problem Statement

- Deepfake technology is advancing rapidly, enabling creation of hyper-realistic fake videos and audios.
- These synthetic media files are used for:
    - **Misinformation campaigns** (fake political speeches, propaganda).
    - **Fraud and scams** (CEO fraud, impersonation for financial gain).
    - **Reputation damage** (fake celebrity endorsements, corporate defamation).
    - **Cyber threats** (identity theft, phishing, extortion).
- Current detection solutions are:
    - Slow and resource-heavy.
    - Not user-friendly for the general public.
    - Lacking seamless **enterprise-level integration** with social platforms or CRMs.
- Need: A centralized CRM-based system to **detect, analyze, and manage deepfake cases** efficiently.

🔹 Use Cases

- **Media Companies**
    - Automate video screening before publishing.
    - Prevent circulation of misinformation on news portals.
    - Ensure trust in digital journalism.
- **Government Agencies**
    - Monitor political content and election-related campaigns.
    - Detect and block malicious propaganda videos.
    - Strengthen national security by preventing misuse of AI media.

- **Social Media Platforms**
    - Integrate API for **real-time flagging** of suspicious uploads.
    - Reduce virality by auto-detecting fake videos.
    - Ensure safer user experience and compliance with content regulations.
- **General Public**
    - Upload videos and check authenticity within seconds.
    - Protect from identity theft or personal reputation damage.
    - Generate verification certificates for proof of authenticity.
- **Enterprises / Corporates**
    - Detect manipulated content targeting CEOs, executives, or brands.
    - Track impersonation risks across social media.
    - Manage brand reputation proactively with CRM dashboards.

Phase 1: Problem Understanding & Industry Analysis

🔹 **Requirement Gathering**

- **Users (Public / Clients)**
    - Simple video upload option.
    - Instant authenticity result with confidence score.
    - Easy-to-understand report download.
- **Analysts (Internal Team)**
    - Access to detailed forensic evidence.
    - Track deepfake trends and campaigns geographically.
    - Generate reports for authorities or clients.
- **Enterprises**
    - Batch processing for multiple videos.
    - API integration with their content workflows.
    - Role-based access and secure data storage.

- **Admins (System Owners)**
    - Configure dashboards, roles, and permissions.
    - Automate workflows (case creation, alerts, escalations).
    - Ensure compliance with GDPR, CCPA, and data security policies.

◆ **Stakeholder Analysis**

- **Primary Stakeholders**
    - Media companies → protect content authenticity.
    - Social media platforms → safeguard platform integrity.
    - Government agencies → counter fake propaganda.
- **Secondary Stakeholders**
    - Fact-checking organizations.
    - Independent researchers studying misinformation trends.
- **Internal Users (Salesforce CRM side)**
    - CRM Administrator → setup, roles, permissions.
    - Detection Analysts → analyze flagged cases.
    - Enterprise Clients → manage batch uploads and monitoring.

◆ **Business Process Mapping**

- **Step 1: Video Upload** (public or enterprise users submit content).
- **Step 2: AI Detection** (Einstein AI + external ML APIs perform analysis).
- **Step 3: Report Generation** (confidence score + forensic evidence).
- **Step 4: Case Creation** (auto-generated if deepfake flagged).
- **Step 5: Alerts & Notifications** (emails, dashboard popups, SMS alerts).
- **Step 6: Dashboard & Analytics** (trend analysis, threat detection, statistics).

🔹 Industry-Specific Challenges

- **Misinformation:** Deepfakes fuel fake news faster than it can be fact-checked.
- **Fraud:** Corporate and financial scams are increasingly using manipulated videos.
- **Reputation Damage:** High-profile individuals and brands are targeted.
- **Entertainment Industry:** Movie piracy and fake celebrity content issues.
- **Global Regulation Gap:** No standard rules across countries to govern deepfake usage.

🔹 Salesforce Solution Mapping

- **Einstein AI** → Confidence scoring, anomaly detection, and explainable AI insights.
- **Case Management** → Track deepfake incidents as Salesforce cases with escalation rules.
- **Reports & Dashboards** → Monitor real-time detection stats, regional analysis, analyst productivity.
- **Flows & Automations** → Auto-create alerts, assign cases, notify stakeholders.
- **API Integrations** → Allow external platforms (e.g., social media, news portals) to auto-scan media.
- **Security & Compliance** → Salesforce's GDPR/CCPA-compliant architecture ensures safe handling of media data.

🔹 Conclusion (Phase 1)

- Deepfake CRM addresses one of the most **pressing issues in digital media security**.
- By combining **AI detection with Salesforce CRM workflows**, the system provides a **centralized, scalable, and secure solution**.
- This phase defines the **problem, requirements, and industry alignment**, laying the foundation for **Org setup, data modeling, and automation** in upcoming phases.