"موقع تحليل الأدلة الجنائية الرقمية"

مقدمة:
يهدف هذا المشروع إلى تقديم موقع إلكتروني يوفر خدمات تحليل الأدلة الرقمية باستخدام أدوات تحليل متقدمة مثل Wireshark و Pyshark. المشروع يركز على تحليل ملفات PCAP التي تحتوي على بيانات الشبكة لاكتشاف أي نشاط مشبوه أو غير طبيعي يمكن أن يُستخدم في تحقيقات جنائية رقمية.

الأدوات المستخدمة في المشروع:

1. **Django**:
يتم استخدام إطار عمل Django لتطوير الموقع ككل Django .يوفر لنا إمكانيات متقدمة في إدارة المستخدمين، رفع الملفات، وتنظيم الصفحات. كما أن Django يسهل علينا تطبيق معايير الأمان والتأكد من حماية البيانات.

2. **Pyshark**:
Pyshark هو واجهة Python لأداة Wireshark. يتم استخدامه في الموقع لتحليل ملفات PCAP المرفوعة من قبل المستخدمين. يتم تحليل الحزم الشبكية لاستخراج المعلومات المتعلقة بالاتصالات مثل بروتوكول الحزمة، عنوان IP المصدر، وعنوان IP الوجهة.

3. **Wireshark**:
Wireshark هو الأداة الرئيسية لتحليل الحزم الشبكية، وهو يُستخدم لفهم وتحليل حركة المرور عبر الشبكة بشكل مفصل . Pyshark يُسهّل عملية دمج Wireshark في الموقع.

4. **نظام إدارة الملفات**:
النظام يسمح للمستخدمين برفع الملفات) مثل ملفات (PCAP التي يتم تحليلها باستخدام .Pyshark ويتم تأمين الملفات بحيث لا يستطيع المستخدمون الآخرون الوصول إلى ملفات بعضهم البعض.

5. **مصادقة المستخدمين**:
تم تطبيق نظام مصادقة يعتمد على تسجيل الدخول والخروج، مما يتيح للمستخدمين رفع ملفاتهم الخاصة وتحليلها في بيئة آمنة، حيث يستطيع كل مستخدم عرض وتحليل الملفات الخاصة به فقط.

كيف يعمل الموقع:

1. **التسجيل وتسجيل الدخول**:
يقوم المستخدم بإنشاء حساب على الموقع من خلال التسجيل، ثم يستطيع تسجيل الدخول للوصول إلى لوحة التحكم.

2. **رفع ملفات الأدلة الرقمية:(PCAP)**
بعد تسجيل الدخول، يمكن للمستخدم رفع ملفات PCAP الخاصة به من خلال صفحة "رفع الأدلة". هذه الملفات تمثل حركة مرور الشبكة التي يتم تحليلها.

3. **تحليل ملفات:PCAP**
بعد رفع الملف، يستطيع المستخدم تحليل ملف PCAP الخاص به. يتم تحليل الحزم الشبكية في الملف باستخدامPyshark ، ويتم عرض النتائج بشكل جداول تعرض الحزم الملتقطة، البروتوكولات المستخدمة، وعناوين IP الخاصة بالمرسل والمستقبل.

4. **عرض النتائج**:
في صفحة النتائج، يستطيع المستخدم مشاهدة تحليل أول 10 حزم من ملفPCAP ، ويمكن عرض البروتوكولات المستخدمة في الاتصالات، وكذلك بيانات مثل حجم الحزم والمعلومات المتعلقة بها.

5. **تأمين الملفات**:
جميع الملفات التي يتم رفعها وتحليلها على الموقع مؤمنة بحيث لا يمكن الوصول إليها إلا من قبل المستخدم الذي قام برفعها.

ماذا يمكن للمستخدم فعله في الموقع؟

1. **التسجيل وإنشاء حساب**:
يمكن للمستخدم التسجيل في الموقع لإنشاء حساب جديد.

2. **رفع وتحليل ملفات:PCAP**
بعد تسجيل الدخول، يمكن للمستخدم رفع ملفات الأدلة الرقمية مثل ملفات PCAP التي تحتوي على حركة مرور الشبكة. هذه الملفات يتم تحليلها وعرض نتائجها.

3. **عرض النتائج التفصيلية**:

4.
بعد التحليل، يتم عرض النتائج التي تشمل معلومات مثل عناوينIP ، البروتوكولات، طول الحزم، وغيرها من التفاصيل الهامة.

5. **إدارة الملفات**:
يمكن للمستخدمين إدارة ملفاتهم ورفع ملفات جديدة وتحليلها.

الخلاصة:

المشروع يقدم منصة سهلة الاستخدام للمستخدمين لتحليل الأدلة الرقمية المتعلقة بالشبكات باستخدام أدوات مفتوحة المصدر مثل Wiresharkو .Pysharkالهدف الأساسي هو توفير وسيلة لتحليل البيانات الشبكية بشكل سهل وآمن للباحثين والمحققين الجنائيين.