

Digital Proof الإثبات الرقمي

مدرس المادة
د. أشرف الراعي

LAW637

الماجستير في القانون الرقمي

Lecture 2



Digital Proof

Lecture 2

LAW637

Master of Digital law



Prepared by
Dr. Ashraf Alrai

بداية، اسمحوا لي أن أشير إلى المواضيع التي ناقشناها في المحاضرة السابقة، وهي كما يلي:

- طبيعة أدلة الإثبات الرقمية وأنظمتها.
- تعريف الإثبات.
- أهمية أدلة الإثبات.
- نظم الأدلة الجنائية الرقمية وتطورها.
- نظام الأدلة الرقمية.
- نظام الأدلة الرقمية العلمية.



القواعد العامة في الإثبات الجنائي



هناك عدة مبادئ عامة ينبغي أن تؤخذ في الاعتبار، ويشار إلى هذا المجال أيضًا باسم "علم الطب الشرعي الرقمي" أو "علم الجريمة الرقمية".

وقد تختلف المبادئ العامة بين بلد وآخر ووقت وآخر على التشريعات والأنظمة القانونية في مختلف البلدان، ولكن يمكن تسليط الضوء على بعض النقاط المشتركة:



الفصل
02

تشير صحة الأدلة الرقمية إلى قدرتها على تأكيد الوقائع أو الأحداث المستخدمة كدليل في سياق قانوني.

تشمل الأدلة الرقمية جميع البيانات الإلكترونية التي يمكن استخدامها لدعم الحقائق أو المطالبات في المحكمة أو أي إطار قانوني آخر.





الفصل 02

تتحقق الحجية من خلال عدد من الضوابط :

- سلامة البيانات: يجب حماية البيانات المستخدمة في الأدلة الرقمية من التلاعب والتغيير غير المصرح به.
- التوقيع الرقمي: التحقق من صحة التوقيعات الرقمية والتأكد من هوية الشخص الذي قام بالتوقيع.
- جودة الأدلة: يجب أن تكون الأدلة الرقمية ذات جودة عالية ويمكن التحقق منها بدقة.
- سلسلة الحراسة: يجب توثيق تاريخ ومصدر الحصول على الأدلة الرقمية، ويجب الحفاظ على سلسلة الحراسة بعناية.



الفصل

02

تتحقق الحجية من خلال عدد من الضوابط :

- التحليل الرقمي: يتضمن التحليل الرقمي استخدام أساليب وأدوات متقدمة لفحص البيانات الرقمية.
- الشهادات الرقمية: تحتاج الشهادات الرقمية إلى التحقق والثقة ويجب استخدامها لتأكيد هوية الأفراد أو الكيانات الرقمية.



الفصل

2

تتحقق الحجية من خلال عدد من الضوابط :

- ❑ اللوائح القانونية: يعد الالتزام بالقوانين واللوائح المحلية والدولية المتعلقة بجمع الأدلة الرقمية واستخدامها أمراً بالغ الأهمية.
- ❑ الحفاظ على الخصوصية: يجب أن يتم التعامل مع البيانات الشخصية بعناية لضمان الحفاظ على الخصوصية والامتثال للقوانين ذات الصلة.
- ❑ توثيق العمليات: يجب توثيق كافة العمليات والخطوات التي تم اتخاذها أثناء جمع الأدلة الرقمية وتحليلها.
- ❑ التدريب والكفاءة: يجب أن يكون الأفراد المشاركون في عمليات الأدلة الرقمية مدربين تدريباً جيداً وأكفاء في مجال الطب الشرعي الرقمي.



يشير مصطلح "قرينة البراءة" في السياق القانوني إلى الأدلة التي قد تؤدي إلى إثبات براءة المتهم في قضية جنائية في إطار القانون الجنائي.

في نظام العدالة الجنائية، يُطلب من النيابة إثبات الجريمة بناءً على الأدلة المتوفرة، بينما يقوم المتهم بتقديم أدلة أو قرائن تشير إلى براءته.



يمكن أن تكون أدلة البراءة متنوعة وتختلف حسب ظروف كل قضية.

ومن أمثلة أدلة البراءة ما يلي :

- الأدلة المادية: الأدلة العلمية مثل الآثار الجينية أو بصمات الأصابع أو تحليل الدم التي قد تثبت براءة المتهم .
- شهادات الشهود: إذا كان هناك شهود يمكنهم تقديم شهادة تثبت براءة المتهم، فيمكن اعتبار أقوالهم دليل تبرئة .
- التسجيلات والتسجيلات: سجلات الهاتف أو لقطات الفيديو أو التسجيلات الصوتية التي تبين عدم تواجد المتهم في مسرح الجريمة أو وجود ظروف مخففة .



- الأدلة الظرفية: العوامل الخارجة عن إرادة المتهم والتي قد تكون بمثابة دليل على البراءة، مثل إثبات وجود ظروف قاسية تؤثر على المتهم .

- الشك في موثوقية أدلة الادعاء: إذا تمكن محامو الدفاع من التشكيك في مصداقية أدلة الادعاء، فيمكن اعتبار ذلك تبرئة .

ومن الأهمية بمكان تقديم أدلة البراءة بشكل فعال في المحكمة لضمان اتخاذ قرار عادل.

وهذا المفهوم جزء أساسي من مبدأ "المتهم بريء حتى تثبت إدانته" في العدالة الجنائية .



مبدأ قرينة البراءة هو مفهوم قانوني ينص على أن لكل طرف في الدعوى الجنائية الحق في تقديم الأدلة والشهادات المؤيدة لدعواه.

وتقع على عاتق النيابة مسؤولية تقديم الأدلة التي تثبت التهم. ويعني هذا المبدأ أن المسؤولية الأساسية عن تقديم الأدلة تقع على عاتق الطرف المدعي، وليس الطرف المتهم بالجريمة.

الفصل 02



وفي إطار النظام القانوني، هناك توازن بين الاتهام والدفاع، مما يتيح للدفاع فرصة تقديم الأدلة التي تثبت براءة المتهم.

وتقوم المحكمة بتقييم جميع الأدلة المقدمة من الطرفين وتقرر بناء على تلك الأدلة .

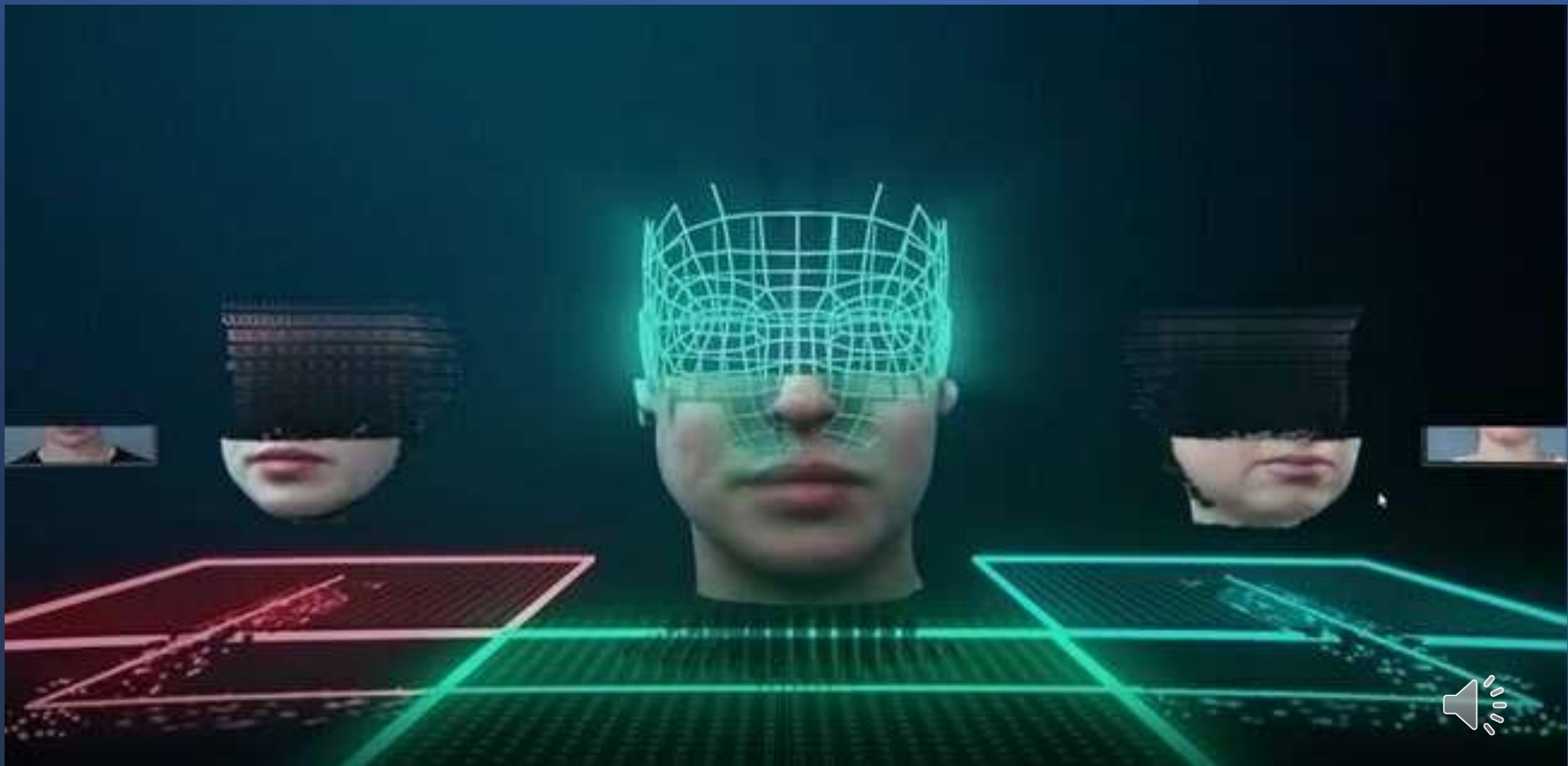


وهذا المبدأ يعزز مفهوم العدالة ويضمن حقوق الفرد في الدفاع عن النفس.
كما يساهم في تحقيق النزاهة والموضوعية في إجراءات العدالة الجنائية، مما يتيح للجميع تقديم الأدلة التي قد تلقي الضوء على حقيقة الأحداث .



إن النظر بعناية في هذا المبدأ أمر ضروري لضمان عدالة الإجراءات القانونية وتحقيق العدالة .







أصبح استخدام الأنظمة الرقمية في عملية الإثبات الجنائي ذا أهمية متزايدة في العصر الحديث.

ويتيح التقدم التكنولوجي جمع الأدلة وتخزينها وتحليلها بشكل فعال من خلال التقنيات الرقمية، مما يساهم في تعزيز الكفاءة في عملية العدالة الجنائية. فيما يلي بعض الطرق التي يمكن من خلالها استخدام الأنظمة الرقمية في عملية الأدلة الجنائية:



✓ الطب الشرعي الرقمي: يتضمن الطب الشرعي الرقمي جمع وتحليل البيانات الإلكترونية للتحقيق في الجرائم الإلكترونية. ويتضمن فحص أجهزة الكمبيوتر والخوادم والأجهزة المحمولة ووسائط التخزين الرقمية الأخرى لاستخراج الأدلة ذات الصلة.

✓ تقنيات المراقبة: توفر تقنيات المراقبة الرقمية، مثل أنظمة الدوائر التلفزيونية المغلقة والكاميرات المحمولة، أدلة مرئية يمكن أن تكون حاسمة في التحقيقات الجنائية. تساعد هذه التقنيات في مراقبة وتسجيل الأنشطة في الأماكن العامة.



✓ السجلات والوثائق الإلكترونية: يمكن أن يكون استخدام السجلات الإلكترونية، مثل رسائل البريد الإلكتروني والرسائل النصية وغيرها من الاتصالات الرقمية، بمثابة دليل في القضايا الجنائية. بالإضافة إلى ذلك، يمكن أن يكون التوثيق الإلكتروني للمعاملات والأنشطة ذا قيمة في تحديد الجداول الزمنية والاتصالات.

✓ البيانات البيومترية: يمكن استخدام التقنيات البيومترية، بما في ذلك أنظمة التعرف على بصمات الأصابع والوجه، لتحديد هوية الأفراد وربطهم بالأنشطة الإجرامية. يمكن أن تكون البيانات البيومترية بمثابة دليل قوي في التحقيقات.



- ✓ أدوات تحليل البيانات: تتيح أدوات وبرامج تحليل البيانات المتقدمة لوكالات إنفاذ القانون معالجة كميات كبيرة من المعلومات الرقمية بسرعة. يساعد هذا في تحديد الأنماط والعلاقات والشذوذات التي قد تكون ذات صلة بقضية جنائية.
- ✓ تقنية Blockchain: يمكن استخدام تقنية Blockchain، بطبيعتها الآمنة والشفافة، لإنشاء سجل مقاوم للتلاعب لأنواع معينة من المعاملات أو الأنشطة، مما يوفر مصدرًا موثوقًا للأدلة.
- ✓ شهادة الخبراء: قد تتضمن الأنظمة الرقمية شهادة خبراء في مجالات مثل الطب الشرعي الرقمي، والأمن السيبراني، وتحليل البيانات. يمكن لهؤلاء الخبراء تقديم رؤى حول صحة الأدلة الرقمية وأهميتها.





مبدأ اقتناع القاضي في الإثبات الجنائي



إن دمج الأنظمة الرقمية في عملية الأدلة الجنائية لا يؤدي إلى تبسيط التحقيقات فحسب، بل يثير أيضًا اعتبارات مهمة فيما يتعلق بقناعة القاضي بالأدلة المعروضة عليه.



يشير مبدأ اقتناع القاضي بالأدلة الرقمية في الأدلة الجنائية إلى أنه يجب على القاضي أن يقتنع بقوة وصحة الأدلة الرقمية المقدمة أمامه في سياق القضايا الجنائية.

يعكس هذا المبدأ مبدأً عامًا في العدالة الجنائية، وهو أن الأدلة المقدمة في المحكمة يجب أن تكون قوية وموثوقة بما يكفي لدعم الحكم .



وفي حالة الأدلة الرقمية، قد تتعلق هذه الأدلة بالبيانات الإلكترونية، مثل رسائل البريد الإلكتروني، وسجلات المكالمات، ولقطات الفيديو، والتسجيلات الصوتية، وغيرها من المعلومات المتعلقة بالتقنيات الرقمية.

ولكن حتى مع استخدام هذه الأدلة الرقمية، يجب أن يقتنع القاضي بدقة وقوة هذه الأدلة قبل اتخاذ أي قرارات.



تتضمن بعض العوامل التي قد يأخذها القاضي في الاعتبار عند تقييم الأدلة الرقمية ما يلي:

- ❑ مصداقية الأدلة: تقديم الأدلة بشكل يدل على مصداقيتها وصحتها يعزز قبول القاضي لها.
- ❑ تقنيات الحماية والأمن: ينبغي استخدام التقنيات الرقمية لحماية الأدلة من التلاعب أو التزوير، ويجب أن يكون هناك دليل على أن هذه التقنيات قد تم توظيفها بشكل فعال.



□ شهادات الخبراء: قد يحتاج القاضي إلى الاستعانة بخبراء في مجال التكنولوجيا الرقمية لتوضيح الأدلة وشرح كيفية جمعها وصلاحياتها.

□ التشريعات والسياسات: يعد الالتزام بالقوانين والسياسات المتعلقة بجمع وعرض الأدلة الرقمية أمرًا بالغ الأهمية.

إن ضمان اقتناع القاضي بالأدلة الرقمية يعزز موثوقية العدالة الجنائية ويساهم في اتخاذ قرارات قانونية عادلة ومبنية على الحقائق.



استخدام الأنظمة الرقمية في الإثبات الجنائي



تشمل الأدلة الجنائية الرقمية مجموعة واسعة من المعلومات والبيانات الإلكترونية التي يمكن استخدامها كأدلة في التحقيقات الجنائية. فيما يلي بعض الأمثلة الشائعة للأدلة الجنائية الرقمية:



سجلات الإنترنت:

سجل التصفح، بما في ذلك توقيت زيارة المواقع.
سجلات محرك البحث.

بريد إلكتروني:

رسائل البريد الإلكتروني والمرفقات.
عناوين البريد الإلكتروني وإرسال/استقبال المعلومات.



وسائل التواصل الاجتماعي:

محتوى المشاركات والتعليقات.
الصور ومعلومات الشبكة الاجتماعية.

الهواتف الذكية:

سجلات المكالمات والرسائل النصية.
تاريخ ووقت الاتصال بالخدمات والتطبيقات .



أجهزة الكمبيوتر والأجهزة الرقمية:

ملفات السجل والتاريخ.
الملفات المؤرشفة والمحذوفة.

الشبكات الرقمية:

عناوين IP وسجلات الاتصال.
سجلات الخادم والشبكة.



التشفير والأمن الرقمي:

تشفير البيانات والمفاتيح الرقمية.
سجلات الوصول ومحاولات القرصنة.

التكنولوجيا البيومترية:

البيانات البيومترية مثل بصمات الأصابع والتعرف على الوجه.
الوصول إلى السجلات بناءً على البيانات البيومترية.



التقنيات الرقمية الأخرى:

مستندات Word و Excel و PDF.
ملفات الوسائط المتعددة (الصوت والفيديو).



الفصل

02

أمثلة على القضايا الجنائية التي تتضمن أدلة رقمية



ومن المؤكد أن هذه بعض القضايا الجنائية التي تنطوي على أدلة رقمية:



حالة القرصنة:

يتضمن هذا النوع من الحالات التدخل غير المصرح به في أنظمة الكمبيوتر أو الشبكات. يمكن استخدام الأدلة الرقمية، مثل سجلات الخادم والبيانات المجزأة، لتحديد المتسللين وتتبع أنشطتهم.



حالات الاحتيال عبر الإنترنت:

تتضمن هذه الحالات عمليات احتيال تتم عبر الإنترنت، مثل الاحتيال المالي أو سرقة الهوية. يمكن استخدام الأدلة الرقمية، بما في ذلك بيانات تحويل الأموال عبر الإنترنت وسجلات البريد الإلكتروني، لتتبع الجريمة.



قضايا التجسس الصناعي:

وتدور هذه القضايا حول سرقة الأسرار التجارية أو التكنولوجيا. يمكن استخدام الأدلة الرقمية لتحليل تحركات المتسللين والوصول غير المصرح به إلى ملفات الشركة.



قضايا جرائم الحاسب الآلي:

تشمل هذه القضايا جرائم مختلفة، بما في ذلك انتهاك حقوق الطبع والنشر وانتهاك حقوق الملكية الفكرية وتوزيع البرامج الضارة. تلعب الأدلة الرقمية دورًا حاسمًا في تتبع الجرائم الإلكترونية وتحديد المسؤولين عنها.



حالات التنمر الإلكتروني:

تتضمن هذه الحالات مضايقة أو تسلطًا عبر الإنترنت. تعد الأدلة الرقمية، مثل محتوى البريد الإلكتروني وسجلات وسائل التواصل الاجتماعي، أمرًا بالغ الأهمية في التحقق في التسلط عبر الإنترنت وملاحقته قضائيًا.



قضايا الإرهاب الرقمي:

تتضمن هذه الحالات تحليل الأنشطة الرقمية للجماعات الإرهابية أو الأفراد الذين يستخدمون الإنترنت للتخطيط لهجمات إرهابية. تتضمن الأدلة الرقمية تحليل البريد الإلكتروني واختبارات التشفير.



وأخيرا، في ختام هذه المحاضرة الهامة تناولنا العديد من المواضيع المتعلقة بالأدلة الجنائية الرقمية:

- ❑ المبادئ العامة في الأدلة الجنائية الرقمية.
- ❑ صحة الأدلة الرقمية.
- ❑ قرينة البراعة.
- ❑ مبدأ حرية الإثبات الجنائي.
- ❑ الاستفادة من الأنظمة الرقمية في عملية الإثبات الجنائي.
- ❑ مبدأ قناعة القاضي في الإثبات الجنائي الرقمي.
- ❑ حيث يمكن أيضا الحصول على الأدلة الرقمية.
- ❑ نماذج للأدلة الرقمية.



شكراً لكم

