ورقة عمل بعنوان

الحاسب الجنائي في الدول الغربية: دراسة استطلاعية

د. هند بنت سليمان الخليفة
أستاذ مساعد- قسم تقنية المعلومات
كلية علوم الحاسب ونظم المعلومات
جامعة الملك سعود – الرياض
hendk@ksu.edu.sa

ملخص:

شهد تخصص الحاسب الجنائي في السنوات الماضية اهتماماً واسعاً من قبل العديد من المؤسسات الأمنية حول العالم نظراً لانتشار استخدام أجهزة الحاسب الآلي وشبكة الانترنت كوسائط تخزينية ووسائل لتبادل البيانات ونقلها. وأضحت هذه الأجهزة التقنية تستخدم كأدلة شاهدة خلال المحاكمات في الجرائم الحاسوبية التي تهدد الأمن القومي أو التي تسيء استعمال الحاسب أو حتى لحل النزاعات المدنية.

يضاف إلى ذلك التطور الحاصل في الجرائم الحاسوبية وتنوع طرقها ووسائلها مما أجبر الأجهزة الأمنية والكيانات الأكاديمية المختصة بأمن المعلومات بطلب استحداث برنامج أكاديمي متفرع من تخصص علوم الحاسب موجه لدراسة وتحري الجرائم المعلوماتية، أطلق عليه تخصص الحاسب الجنائي (Computer Forensics).

وقد عكفت العديد من المؤسسات التعليمية حول العالم والمدعومة من قبل الإدارات الأمنية على تطوير مناهج أكاديمية في تخصص الحاسب الجنائي والمتفرع من علوم الحاسب، بحيث يغطي المنهج التعليمي جميع الجوانب الأخلاقية والقانونية والعلمية للتخصص، وتمنح المتقدم بعدها درجة علمية محددة (دبلوم أو بكالوريوس أو ماجستير) .

في هذه الورقة سأعمل على تعريف تخصص الحاسب الجنائي وتحديد أهدافه والمتطلبات والتحديات التي تواجه هذا التخصص، يلي ذلك استعراض لتجارب بعض الدول في تدريس هذا التخصص مع التركيز على المناهج المطروحة والأساليب الحديثة والأدوات والبرمجيات المستخدمة والمسارات المتوفرة. وأخيراً أختتم الورقة بتلخيص لأهم العناصر

الجوهرية المتوقع تواجدها في أي برنامج متكامل لتدريس تخصص الحاسب الجنائي ودورها في إعداد الكوادر البشرية المؤهلة في هذا التخصص.

مقدمة

أضحى استخدام جهاز الحاسب الآلي سمة بارزة لهذا العصر والذي يعكس التطورات التقنية الحاصلة في القرنين العشرين والواحد والعشرين. فلم يعد استخدام الحاسب الآلي محصوراً على مراكز البحث العلمي والشركات، بل أصبح بمقدور أي شخص يملك المقومات المادية الحصول على جهاز حاسب آلي أو أكثر.

ومن الملاحظ أن النظرة العامة لجهاز الحاسب الآلي هو اعتباره كوسيط تخزيني ووسيلة للاتصال بفضل وجود شبكة الانترنت، مما جلب معه أيضاً جانباً آخر وهو جانب الجرائم المعلوماتية. ففي إحصائية تقريبية للقضايا المعروضة في المحاكم الأمريكية، وُجد أن 85% من هذه القضايا تطلبت وجود أدلة رقمية [1].

وثمة توجه من قبل الكيانات الأكاديمية لإدماج مقرر الحاسب الجنائي في برامجها التعليمية المتخصصة في علوم الحاسب وذلك عن طريق: إما إعطاء مقرر أو أكثر ضمن الخطة الدراسية للدرجة العلمية، أو تخصيص درجة علمية كاملة (دبلوم أو بكالوريوس أو ماجستير) تفرد لتدريس هذا التخصص [1].

أما خارج الكيانات الأكاديمية فيمكن الحصول على مهارات الحاسب الجنائي عن طريق برمجيات تعليمية مثل التي تقدمها شركة VTC [2] أو برامج تدريبية تابعة لمؤسسات وجمعيات متخصصة مثل ما تقدمه الجمعية الدولية لامتحانات الحاسب الجنائي (ISFCE) [3] .

كما إن الاهتمام الحاصل في مجال الحاسب الجنائي قد ازداد خلال السنوات الخمس الماضية وخاصة في الولايات المتحدة لعدة أسباب منها تداعيات أحداث الحادي عشر من سبتمبر والفضيحة المالية لشركة أنرون Enron، فقد كانت لهذه الحادثتين وغيرها الأثر في توظيف برامج أكاديمية في مجال الحاسب الجنائي قادرة على تخريج كفاءات مؤهلة تقنياً وجنائياً للتحقيق والتحري في جرائم الحاسب والانترنت. وحتى يتطور هذا المجال لابد من بناء مناهج دراسية وفق أسس وقواعد علمية تسهم في عملية تطوير مجال الحاسب الجنائي.

من خلال هذه الدراسة تأمل الباحثة إعطاء صورة واضحة عن التقدم الحاصل في مجال الحاسب الجنائي في الدول الغربية، مع التركيز على استعراض تجارب هذه الدول في تدريس هذا التخصص والمناهج المطروحة والأدوات والبرمجيات المستخدمة والمسارات المتوفرة. وعليه فإن أهداف هذا البحث يتلخص في التالي:

1. معرفة طبيعية وأنواع البرامج الأكاديمية المطروحة في تخصص الحاسب الجنائي، وذلك للاستفادة من تجارب الدول الغربية في هذا المجال، وهذا الهدف نشأ من محورين:
   أ. إن البدء التدريجي في تحول المملكة إلى الحكومة الإلكترونية وتشجيع التعاملات الإلكترونية يتطلبان رفع الاحتياطات الأمنية لضمان سرية وسلامة وصحة المعلومات المتداولة وأيضا التصدي للأعمال الإجرامية مثل عمليات النصب والاحتيال وسرقة البطاقات الائتمانية أو انتحال الهوية. وهذه الاحترازات تتطلب بالطبع إلى وجود كوادر بشرية على قدر عال من المهنية الأمنية والتكنولوجية للتحري وتتبع مثل هذه الحالات.
   ب. ظهور نظام مكافحة جرائم المعلوماتية والذي أقره مجلس الوزراء السعودي مؤخراً برئاسة خادم الحرمين الشريفين الملك عبدالله بن عبدالعزيز –حفظه الله– يعني أن الدولة بحاجة لأشخاص مؤهلين يمكنهم من تجريم مرتكبي هذه التجاوزات وإثباتها بالأدلة التقنية والفنية، مستندين بذلك على أسس علمية وشرعية.
2. إطلاع العاملين في المؤسسات الأمنية على التطورات الحديثة في مجال تدريس الحاسب الجنائي، خصوصاً أن المملكة العربية السعودية تعمل دائماً على مواكبة التطورات العلمية والبحثية في مجال العلوم الأمنية وذلك للتصدي لأي أعمال إجرامية بصفتها الإلكترونية والتي لا يقره ديننا الحنيف.

ولكي يحقق البحث أهدافه، قامت الباحثة بصياغة عدد من التساؤلات التي تساعد في تغطية جميع جوانب الدراسة الاستطلاعية في هذا المجال على النحو التالي:

1) ما هي أنواع البرامج الأكاديمية المتوفرة والمدة الزمنية لها؟
2) ماهية المواد المطروحة في مثل هذه البرامج؟
3) ما هي تحديات ومتطلبات التخصص ومجالات العمل؟
4) ما هي المعايير المطلوبة لاستحداث برنامج في مجال الحاسب الجنائي؟

بناءً على ما سبق، ستتناول ورقة البحث هذه في أجزائها الخمس ما يلي: الجزء الأول سيتطرق للتعريف بالحاسب الجنائي وأهميته. يليه الجزء الثاني الذي يستعرض الأدوار العملية الممكن القيام بها عند العمل في مجال الحاسب الجنائي. الجزء الثالث سيتناول أنواع البرامج الأكاديمية المتخصصة التي تمنح درجة علمية في مجال الحاسب الجنائي. أما الجزء الرابع فسيعرض بعضاً من تجارب الدول الغربية وتحديداً في الولايات المتحدة و المملكة المتحدة وألمانيا في مجال تدريس

الحاسب الجنائي. وفي الجزء الأخير ستختتم الورقة بمناقشة التجارب السابقة مع تلخيص لأهم العناصر المتوقع تواجدها في أي برنامج يتناول تخصص الحاسب الجنائي ودورها في إعداد الكوادر البشرية المؤهلة في هذا المجال.

الحاسب الجنائي: ماهيته وأهميته

نشأ مجال الحاسب الجنائي منذ ثورة الحواسيب الشخصية في الثمانينات [11]، ويهتم هذا المجال بالعمل على تحديد وحفظ واسترجاع وتحليل وتوثيق البيانات الحاسوبية التي يزعم أنها استخدمت في الجرائم المرتكبة بواسطة جهاز الحاسب [6].

يعتبر تخصص الحاسب الجنائي علم تطبيقي متفرع من علم الأدلة الجنائية (Forensics science) والتي لها جذورها في الطب الشرعي، لذا فهو يختلف في أهدافه عن تخصص أمن الحاسبات (Computer security) الذي يهدف لحماية أجهزة الحاسب والشبكات من الأعمال التخريبية والاختراقات [6]. كما يتفرع من تخصص الحاسب الجنائي تخصص دقيق مهتم بالشبكات والانترنت يسمى تخصص الشبكات/الانترنت الجنائي (Network/Internet forensics) يهتم بالتحري والتحقيق بجرائم الشبكات [10].

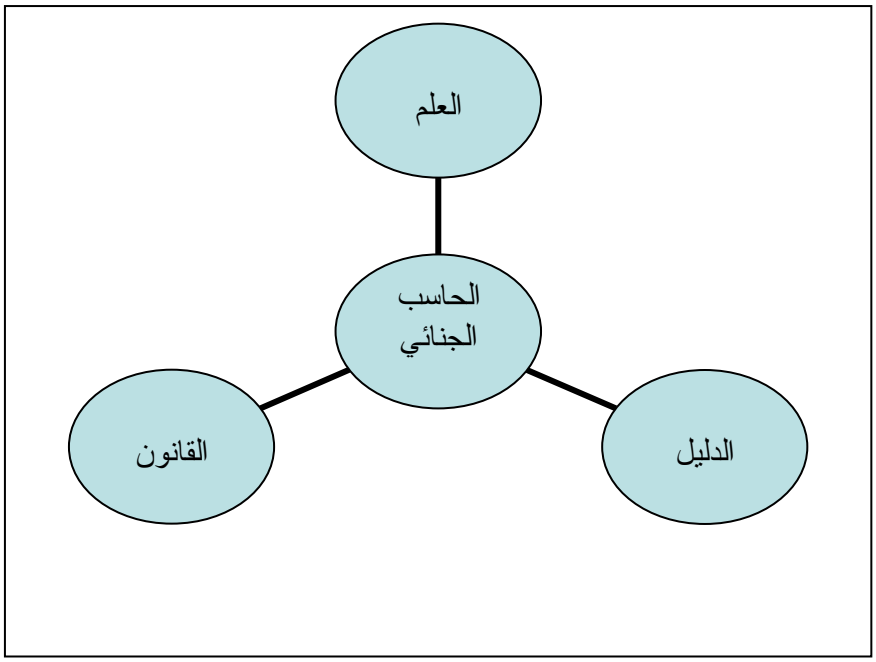
وهناك ستة نماذج منهجية عند التحقيق في جرائم الحاسب لخصها كومبي وورن [31] في التالي:

- **نموذج لوسنت (Lucent Model)**: أو ما أطلق عليه نموذج (Three A's) ويتكون من: الاكتساب(Acquire) والتصديق (authenticate) والتحليل (analyze).
- **نموذج (KPMG)**: وقد اقترحه الضابط Rodney McKemmish من الشرطة الاسترالية، ويتكون النموذج من أربع عناصر عند التحقيق وهي: التعرف على الدليل الرقمي، والاحتفاظ بالدليل الرقمي، تحليل الدليل الرقمي، وعرض الدليل الرقمي.
- **نموذج (Dittrich and Brezinski)**: وينسب هذا النموذج لشخصين الأول Brezinski ويعمل في مركز الاستخبارات الأمريكية والثاني يدعى Dittrich ويعمل كخبير أمني في جامعة واشنطن. يتكون النموذج من ست خطوات هي: إعداد الخطة، وحماية مكان الجريمة، وتوثيق الموجود في مكان الجريمة، والبحث عن أدلة، والاحتفاظ بها ثم معالجتها.
- **نموذج جامعة ييل (Yale University)**: قام بصياغة هذا النموذج Eoghan Casey المشرف الأمني لأنظمة جامعة ييل. النموذج مكون من ست خطوات هي: الإعدادات القبلية، التخطيط، التمييز، الاحتفاظ والتوثيق والجمع، التصنيف والمقارنة وأخيراً إعادة بناء الجريمة.

- **نموذج (Mitre)**: مقترح هذا النموذج هو Gary Palmer من شركة Mitre الأمنية، ويتكون النموذج من عنصرين هما: علاقة الأدلة بالجريمة وموثوقية الأدلة المستخلصة.
- **نموذج مكتب العدل الأمريكية (US Department of Justice)**: في التشريع الموجود في دليل مكتب العدل الأمريكية عن الجرائم الالكترونية، ذكر الدليل أربع إجراءات متبعة عند البحث في أجهزة الحاسب وهي: البحث في جهاز الحاسب وطباعة محتوياتها أثناء التحري، البحث في جهاز الحاسب وعمل نسخ من محتويات بعض ملفاته، عمل نسخة من محتويات الجهاز في موقع الجريمة وبعدها، فصل جميع الأجهزة المتصلة بالحاسب وجمعها لأخذها لمعمل الحاسب الجنائي.

وعلى الرغم من اختلاف هذه النماذج في إجراءاتها إلا أنها تتفق جميعاً في كون أي تحقيق في الحاسب الجنائي يتبع الإجراءات التالية هي: استخلاص وكشف البيانات والاحتفاظ بها، وتحليلها ثم توثيقها وعرضها كأدلة جنائية.

وتوضح الصورة 1 الأطراف المكونة لمجال الحاسب الجنائي وهي: 1) العلم بمجال الحاسب والإنترنت وكيفية استخدامهما بكفاءة في التحقيق والتحري واستخلاص الأدلة، 2) الدليل وذلك بمعرفة ما يمكن استخدامه كدليل في المحكمة، 3) القانون وهي معرفة الخطوات اللازمة لتجريم المشتبه به [29].



صورة 1: الأطراف المكونة لمجال الحاسب الجنائي

ويرجع السبب في الاهتمام الشديد بمثل هذا التخصص في وقتنا الحالي تحديداً، إلى زيادة الجرائم الإلكترونية والتهديدات المحتملة باستخدام أجهزة الحاسب والانترنت سواء كان ذلك على مستوى الشركات أو مستوى الدول. وقد بدأ هذا المجال بالازدهار في الدول الغربية، خاصة في الولايات المتحدة والمملكة المتحدة وذلك مع تصاعد التهديدات الأمنية على تلك الدول.

الأدوار العملية

يمكن تقسيم الأدوار العملية الذي يقوم بها العامل في مجال الحاسب الجنائي إلى أربعة أقسام وفقاً لتقسيمات ياسينساك وآخرون [11] وهي كالتالي:

1) **فني حاسب جنائي (Technician)**: وهو شخص يملك مهارات فنية وتقنية لاستخلاص الأدلة الرقمية، وقد يحمل درجة الدبلوم أو البكالوريوس في تخصص الحاسب الجنائي.
2) **صناع القرارات المؤسسية (Enterprise policy maker)**: وهم أشخاص مخولين لصنع القرارات داخل المؤسسة، ويتطلب ذلك معرفة جيدة بالحاسب والعلوم الجنائية.
3) **محترف حاسب جنائي (Forensics professional)**: بالرغم من وجود تخصص فني حاسب جنائي إلا أن وجود محترف حاسب جنائي مهم ليكون حلقة الوصل بين الفني وصناع القرار في أي كيان إداري. فالمحترف يعمل على ترجمة سياسات أي مؤسسة أو كيان أمني إلى إجراءات فعلية يقوم بها الفني.
4) **الباحثون (Researchers)**: وهم أشخاص من حملة الماجستير أو الدكتوراه يقومون بأبحاث لتطوير مجال الحاسب الجنائي.

في هذه الورقة سيتم التركيز على المناهج الأكاديمية لفني ومحترفي الحاسب الجنائي.

البرامج الأكاديمية

في السنوات الماضية زاد الطلب على وجود كوادر بشرية مؤهلة في تخصص الحاسب الجنائي، وقد انعكس هذا الزخم في الطلب على البرامج الأكاديمية المطروحة في المؤسسات الأكاديمية.

في هذا الجزء من الورقة سأقوم باستعراض لأنواع البرامج المطروحة و الدرجات العلمية الممنوحة بناءً على دراسة حديثة قام بها تيلور وآخرون [1] ودراسة سابقة قام بها قوتستوك وآخرون [6].

1) برنامج الدبلوم (مدته سنتان)

يزود برنامج الدبلوم في الحاسب الجنائي المتدرب بالمهارات الكافية للعمل كفني حاسب جنائي. يعني ذلك أن البرنامج يعمل على تأهيل الملتحق فنياً، وذلك بتدريبه على الأدوات المستخدمة في التحري الرقمي، ومعرفياً وذلك بتزويده بالمهارات المطلوبة للعمل كفني في الحاسب الجنائي.

معظم المواد المدرسة في الدبلوم عبارة عن مواد مستلة من تخصص علوم الحاسب، مثل أنظمة التشغيل وأمن المعلومات. كما أن هذه الدبلومات لا تتعمق في تدريس البرمجة وخوارزمياتها مثل مادة تراكيب البيانات (Data Structures).

من المؤسسات الأكاديمية التي تقدم مثل هذه البرامج: كلية المجتمع في مقاطعة بتلر (Butler County Community College) [4] و كلية سبوكين للمجتمع (Spokane Falls Community College) [5]. وللحصول على قائمة شاملة لبرامج الدبلوم المطروحة في الولايات المتحدة يمكن الرجوع للورقة [6].

2) درجة البكالوريوس

تختلف برامج البكالوريوس في الحاسب الجنائي اعتماداً على القسم الذي يقدم هذا البرنامج. فأقسام مثل المحاسبة و الاقتصاد و القانون و الحاسب الآلي، كلها تمنح درجة البكالوريوس في الحاسب الجنائي بحيث يتناول الجانب الكبير من هذه الدرجة أصل التخصص مع التركيز على جزء الحاسب الجنائي، أو أن يكون برنامج البكالوريوس مخصص كليةً للحاسب الجنائي كما سنرى لاحقاً في هذه الورقة.
وغالباً ما تكون المواد المطروحة في مثل هذه البرامج عبارة عن مواد هجينة من تخصصات كعلوم الحاسب والأدلة الجنائية والقانون والعلوم الإنسانية والأمنية.

من الجامعات التي تقدم مثل هذه البرامج: كلية بردو (Purdue College) [7] وجامعة جون هوبكنز (John Hopkins University) [8]. وللمزيد حول برامج البكالوريوس يمكن زيارة موقع e-Evidence [9].

3) درجة الماجستير

على العكس من الدرجات السابقة، لاحظ تيلور وآخرون أن درجة الماجستير ليس لها برنامج معياري محدد، وذلك نابع من اختلاف التخصص الأم الذي يأتي منه الملتحق بهذا البرنامج. فبعض برامج الماجستير تتطلب من الملتحق أن يقوم بدراسة بعض المواد كمتطلبات سابقة قبل الشروع في الدرجة العلمية، مثل مادة الأدلة الجنائية، والعدالة القانونية وأمن الحاسبات وغيرها.

من الجامعات التي تقدم مثل هذه البرامج: جامعة بردو (Purdue University) وجامعة جورج واشنطن (George Washington University) [17].

4) **شهادات متخصصة**

تمنح بعض الجامعات ومراكز التدريب شهادات متخصصة في الحاسب الجنائي، ولكن هذه الشهادات لا يقابلها أي درجة علمية بل تعامل معاملة الدورات القصيرة والشهادات الدولية. فيما يلي عرض لبعض منها:

1) **شهادة مختبر/فاحص للحاسب** Certified Computer Examiner (CCE): هذه الشهادة تقدمها الجمعية الدولية لامتحانات الحاسب الجنائي [3]. من متطلبات هذه الشهادة أن يكون المتقدم ممن ليست لديهم سوابق جنائية وأن يجتاز ثلاثة اختبارات في هذا المجال. يحتوي الامتحان على جزأين: تحريري و آخر عملي، ويجب على المتقدم لهذا الامتحان أن يكون قد أتم وحدات تدريبية في مجال الحاسب الجنائي، أو يملك خبرة عملية كافية. وتبدو هذه الشهادة واحدة من أكثر الشهادات شعبية ومعترف بها على نطاق واسع [1].

2) **شهادة محلل حاسب جنائي** GIAC Certified Forensics Analyst (CFA): تقدم منظمة GIAC[1] شهادة محلل حاسب جنائي، الغرض منها هو الاعتراف بأن الشخص الحاصل على هذه الشهادة لديه المعرفة والقدرة والمهارة المتطورة للتعامل مع سيناريوهات الحوادث الجنائية الرقمية، وإجراء التحريات الجنائية على شبكة الإنترنت أو الأجهزة الشخصية. وعلى المرشح لهذه الشهادة أن يكمل امتحانين على الانترنت يحتوي على 75 سؤالاً متعدد الاختيار. كما يجب على حامل الشهادة أن يجدد الاختبار كل أربع سنوات.

3) **شهادة محقق جرائم حاسوبية وشهادة فني حاسب جنائي** Certified Computer Crime Investigator (CCCI) and Certified Computer Forensics Technician (CCFT)

تعتبر شبكة الجريمة التكنولوجية العليا (High Tech Crime network) إحدى المجموعات غير الربحية المكونة من مختصين في إنفاذ القانون (law enforcement) وأمن المعلومات من 15 دولة. تمنح هذه المجموعة

[1] http://www.giac.org

عدد من الشهادات المعتمدة في الحاسب الجنائي منها شهادة محقق جرائم حاسب (CCCI) وشهادة فني حاسب جنائي (CCFT) وغيرها. وتشمل احتياجات الحصول على شهادة من هذه المجموعة إتمام بعض الدورات التدريبية في التحقيق والتحري في جرائم الحاسوب وتوثيقها.

4) **شهادة مختبر/فاحص حاسب جنائي** Certified Forensic Computer Examiner (CFCE):
توفر الرابطة الدولية لأخصائيي التحقيقات الحاسوبية (IACIS) تدريب للموظفين المكلفين بإنفاذ القوانين وغيرهم من التأهل لعضوية الرابطة [19]. تتضمن متطلبات الحصول على الشهادة اختبار تحريري أو الالتحاق في دورة تدريبية لمدة أسبوعين يمنح بعدها الملتحق شهادة مختبر/فاحص حاسب جنائي.

5) **شهادة محلل جرائم إنترنت** (CSFA Cyber Security Forensics Analyst): في هذه الشهادة يجب على الملتحق أن ينهي ثلاث متطلبات هي: تزكية من مكتب التحقيقات الفدرالية FBI بعدم وجود سوابق إجرامية، والاتفاق على ميثاق أخلاقيات المهنة واجتياز الاختبار التحريري على مدى ثلاثة أيام [20]. يتضمن الاختبار التحريري على أسئلة اختيار متعدد تغطي سيناريوهات فعلية لما سيوجهه المحقق في العالم الفعلي.

على الرغم من وجود هذا التنوع في الشهادات المتخصصة إلا أن هناك جهود في الولايات المتحدة وبإيعاز من المجلس التشريعي لشهادات الأدلة الجنائية الرقمية (Digital Forensic Certification Board (DFCB)) لتوحيد هذه الشهادات الممنوحة من مختلف الجهات تحت مظلة ومنهج موحد يشرف على إعداده أطراف من الكيانات الأمنية في الدولة وجهات أكاديمية وأخرى خاصة تخضع لمعايير قياسية للجودة والكفاءة [1].

تحديات تدريس الحاسب الجنائي

يعتبر تخصص الحاسب الجنائي مثله مثل بقية التخصصات العلمية، فهو بحاجة لإمكانيات مادية ضخمة وأخرى إعدادية. بيد أن التحضير لبرنامج متكامل وشامل في تخصص الحاسب الجنائي بحاجة لوقت وجهد كبير. في هذه الورقة سأذكر عدداً من التحديات التي تواجه تدريس هذا التخصص مستقاة من دراسات سابقة في هذا المجال:

1) الحاجة لميزانية كبيرة لتغطية متطلبات معمل الحاسب الجنائي، فعلى سبيل المثال ذكر سذرلاند أن تكلفة إنشاء معمل في جامعة قلامورقان (Glamorgan) للحاسب الجنائي يتطلب قرابة 60 ألف جنيه إسترليني [21].

2) الوقت والجهد الكبير الذي يستغرقه الإعداد لحالات دراسية فعلية (Case studies) مشابه لتلك التي يمكن أن يواجهها الطالب في أرض الواقع [23].
3) قلة الكوادر المؤهلة في هذا المجال للمساعدة في العملية التدريبية [11, 12].
4) قلة المصادر التعليمية والمراجع والكتب الدراسية المتخصصة [13].
5) إجراءات قبول صارمة نتيجة لحساسية هذا المجال [6].

الأدوات والبرمجيات المستخدمة

كما أسلفت، فإن مجال الحاسب الجنائي هو علم عملي تطبيقي بحاجة لتجهيزات معملية تضم أدوات ومعدات معدة خصيصاً للقيام بالإجراءات التطبيقية. فإلى جانب وجود أجهزة الحاسب بمختلف أنواعها (أجهزة شخصية، خادمات، موجهات، جدران نارية، إلخ) وملحقاتها (طابعات، وحدات تخزين مستقلة، أقراص مرنة ومدمجة، إلخ) فالمعمل بحاجة إلى برامج متخصصة أيضاً سواء كانت أنظمة تشغيل (ويندوز، ماكنتوش، لينكس/يونكس) أو برمجيات تقليدية (مثل برنامج الأوفس) أو حتى أدوات للتحري.

تنقسم الأدوات المستخدمة في مختبر الحاسب الجنائي إلى فئتين: برامج مجانية ومفتوحة المصدر وبرامج تجارية. كما أن فرنسيا وكلينتون [15] في ورقتهم التي تحدثوا فيها عن متطلبات تجهيز معمل حاسب جنائي مثالي بناءً على دراسة مستفيضة لتجارب سابقة، قد قسموا البرامج المستخدمة في معمل الحاسب الجنائي إلى ثلاثة أقسام هي: برامج النسخ المطابق (Imaging)، وبرامج التحليل (Analysis)، وبرامج التمثيل البصري (Visualization).

- **برامج النسخ المطابق:** تعمل هذه البرامج على أخذ نسخة طبق الأصل من البيانات الموجودة في الجهاز الإلكتروني من دون الإضرار بتكاملية أو مصداقية البيانات.
- **برامج التحليل:** تعمل برامج التحليل على عملية الكشف واكتشاف الأدلة والمعلومات التي قد لا تكون واضحة تماما أو قد تكون مخبأة. بعض هذه البرامج تعتمد على تقنية تنقيب البيانات والتي تساعد في التنبؤ بالأحداث أو اكتشاف أنماط إجرامية معينة في البيانات.
- **برامج التمثيل البصري:** تساعد مثل هذه البرامج على تصوير أنماط البيانات بشكل بصري ليسهل على المحقق فهم تمثيل البيانات وترابطها.

جدول 1 يعطي أمثلة لبعض أشهر البرامج المستخدمة في معمل الحاسب الجنائي مع وصف لطريقة عملها ونظم التشغيل التي تعمل عليها.

جدول 1: وصف بعضاً من البرامج المستخدمة في معمل الحاسب الجنائي

البرنامج	نظام التشغيل	وصف البرنامج
EnCase[2] تجاري	DOS, Windows NT, 2000	برنامج يعمل على نسخ وفحص البيانات في الأقراص الصلبة، وحدات التخزين والأجهزة الكفية.
SectorSpyXP مجاني	Windows 2000 and XP	برنامج قوي قادر على فحص وتحليل البيانات في الأقراص بمستويات دنيا (Sector Level)، مع إمكانية البحث داخل هذه البيانات.
Gnuplot[3] مفتوح المصدر	UNIX, IBM OS/2, MS Windows, DOS, Macintosh	برنامج للتمثيل البصري. يعمل هذا البرنامج عن طريق تزويده بملف يحتوي على بيانات معينة ثم يقوم البرنامج بتصوير هذه البيانات على شكل رسم ثنائي أو ثلاثي الأبعاد.

كما لخص ايرباشير في ورقته [16] توصيات حلقة النقاش التي أقيمت في مدينة موسكو عام 2002 عن تعليم وتدريب مؤهلين في الحاسب الجنائي، وذكر أهمية وجود معمل حاسب جنائي مهيأ تهيئة كاملة سواء كان من ناحية الكوادر المؤهلة لإدارتها والإشراف عليها أومن ناحية إعدادها عتادياً.

تجارب سابقة

استناداً إلى ما ذكر سابقاً من مقدمة في مجال الحاسب الجنائي وفروعه وأدواته، سأعمل فيما يلي على استعراض تجارب عملية من كل من الولايات المتحدة والمملكة المتحدة وألمانيا في تدريس هذا التخصص. ولا يعني تركيزي على هذه الدول إغفال بقية الدول الأخرى، ففي أوروبا على سبيل المثال، يقوم حلف شمال الأطلسي- الناتو (NATO)- والانتربول بعمل دورات تدريبية وبرامج في أمن المعلومات للبلدان الحليفة. وفي منطقة آسيا والمحيط الهادئ، يجري مركز بحوث الشرطة الاسترالي (Australasian Center for Policing Research (ACPR)) ، عددا من الدورات التدريبية للملتحقين في استراليا ونيوزلندا [15].

[2] http://www.encase.com/
[3] http://www.gnuplot.info/

تجارب من المملكة المتحدة وألمانيا

بدأ الاهتمام بالتحقيق في جرائم الحاسب في المملكة المتحدة منذ أكثر من عقدين من الزمان. حيث قامت شرطة السكوتلاند يارد في عام 1985م بفتح وحدة تابعة لمكتب التحقيقات لديها تحت مسمى جرائم الحاسب (Computer Crime Unit) مهمتها عقد دورات تدريبية في مجال الحاسب الجنائي إلى جانب دورها كوحدة للتحقيق والتحري في جرائم الحاسب [11]. بعد ذلك تتالت عملية فتح مراكز تدريبية للجرائم الحاسوبية من قبل الكيانات الأمنية في الدولة، ولكن كل هذه المراكز كانت تعمل كجهة مستقلة و لم يتم التنسيق فيما بينها.
في منتصف عام 1990م قامت الكلية الملكية للعلوم العسكرية في شريفينام (Shrivenham) بعقد دورات قصيرة للتدريب على الحاسب الجنائي. تناولت هذه الدورات معلومات في القانون والإجراءات العسكرية والخدمات الأمنية. وفي عام 1997م بعد أن تم الاعتراف من قبل الشرطة في المملكة المتحدة بأهمية وجود برامج تدريبية متكاملة في الحاسب الجنائي، توسعت الكلية الملكية للعلوم العسكرية في برنامجها التدريبي لتفتتح في عام 2002م درجة الماجستير في هذا المجال [11].

وفي ورشة عمل بعنوان الحاسب الجنائي[4] والذي أقيم في نوفمبر من عام 2006م في جامعة نورث أمبريا (Northumbria)، قدم الدكتور سذرلاند من جامعة قلامورقان (Glamorgan)[5] [21] عرض تقديمي احتوى على معلومات تتناول عدد الجامعات في المملكة المتحدة التي تقوم بتدريس الحاسب الجنائي كدرجة علمية (دبلوم، بكالوريوس، ماجستير)، حيث بلغ عددها بناء على إحصائية من موقع مجتمع المعلومات الأوروبي (Eurim)[6] أكثر من عشرين مؤسسة أكاديمية من ضمنها جامعة برادفورد وليدز ورويال هالوي (Royal Holloway) التابعة لجامعة لندن. كما تطرق الدكتور سذرلاند للخطة المثالية لدرجة البكالوريوس في الحاسب الجنائي المكونة من ثمانية فصول (أربع سنوات دراسية). وتتضمن الخطة مواد في البرمجة وقواعد البيانات والرياضيات والإحصاء وتنقيب البيانات والأخلاقيات والشبكات والحاسب الجنائي، كما هو موضح في صورة رقم 2.

كما احتوت ورشة العمل على عرض لتجربة ريتشال ألدرسون (Rachel Alderson) طالبة في السنة الثانية في تخصص الحاسب الجنائي من جامعة نورث أمبريا، تحدثت فيها عن رؤيتها وتقييمها للمواد المدرسة والصعوبات والمخاوف التي تواجهها في هذا التخصص [22].

---

[4] http://www.ics.heacademy.ac.uk/events/displayevent.php?id=139
[5] http://www.glam.ac.uk/coursedetails/685/51
[6] http://www.eurim.org.uk/

Figure 1—Typical Four-year Schedule for Bachelor of Science Degree in Computer Forensics	
Semester 1	**Semester 5**
56.117 Introduction to Computer Forensics	56.317 Forensic Analysis in a Windows Environment
56.123 Visual Basic 1	56.357 Database Design
43.101 Introduction to Criminal Justice	
Semester 2	**Semester 6**
53.111 Finite Mathematics	91.326 Introduction to Fraud Examination
56.223 Visual Basic 2	56.348 Data Mining
Semester 3	**Semester 7**
56.217 Computer Forensics File Systems 1	56.417 Advanced Topics in Computer Forensics
53.141 Introduction to Statistics	56.476 Network Applications
91.120 Accounting for Small Business	
Semester 4	**Semester 8**
56.218 Computer Forensics File Systems 2	Internship
53.185 Discrete Mathematics	
28.295 Business Ethics	

صورة 2: خطة مقترحة لدرجة البكالوريوس في الحاسب الجنائي مأخوذة من
Staley, A.B. Inch, S. Shaperro, M. (2006) *From CSI to the Classroom: Developing a computer foreniscs degree program.* ISACA, www.isaca.org

كما وصف أيرون وآخرون [23] تجربة جامعة نورث أمبريا (Northumbria) في تدريس الحاسب الجنائي وتقييم الطلبة الملتحقين لهذا البرنامج. وذكروا أن المواد المدرسة في تخصص الحاسب الجنائي عبارة عن توازن بين الجزء النظري والعملي من التخصص. كما ركزوا في الورقة على أهمية تدريس أخلاقيات الحاسب الجنائي وتجربة طلبتهم خلال السنة الدراسية الأخيرة بالقيام بصياغة معايير أخلاقيات العمل في الحاسب الجنائي من واقع تجربتهم. أما من جانب تقييم الطلبة للمنهج الأكاديمي المطروح من قبل الجامعة، فقد ذكروا أن التقييم الايجابي للمنهج كان راجعاً للتعاون المثمر مع القطاعات الأمنية الحكومية والمؤسسات الأمنية الخاصة والمكاتب الاستشارية ومطوري برمجيات الحاسب الجنائي في خلق تطبيقات عملية استفاد منها الطالب في برنامجه الأكاديمي.

وفي دراسة مقارنة لدورنسيف وآخرون [24] تناولت الاختلافات والتشابه في تدريس الحاسب الجنائي بين منهج جامعة نورث أمبريا (Northumbria) في المملكة المتحدة ومنهج جامعة روث (RWTH Aachen) من ألمانيا، لاحظ دورنسيف وآخرون خلال دراستهم ندرة في برامج الحاسب الجنائي المطروحة من قبل المؤسسات الأكاديمية الألمانية. كما أن غالبية البرامج الموجودة في البرنامج الألماني عبارة عن مقررات مضافة لدرجة البكالوريوس في الحاسب أو في ماجستير إدارة الأعمال.

كما ركزت المواد المطروحة في التجربة الألمانية على الجانب الأمني في الحاسب الجنائي أكثر من تركيزها على المواد في القانون والتشريع الجنائي في الجرائم الحاسوبية. وقد يكون السبب في ذلك لوجود نقص خبرة في استخدام أدلة الحاسب في القضايا المرفوعة لدى المحاكم الألمانية.

ويختتم الباحثون ورقتهم بذكر أن التجربة البريطانية تعتبر أكثر نضجاً وخبرة في تدريس الحاسب الجنائي مقارنة بالتجربة الألمانية. فالتجربة البريطانية تعتمد على تدريس الطالب مهارات استخدام أدوات الحاسب الجنائي، بينما تقوم التجربة الألمانية على تدريب الطالب على بناء وتحسين الأدوات الموجودة. وهذا ما يميز التجربة الألمانية على نظيرتها البريطانية، حيث أن التجربة الألمانية لا تهدف لتدريب طلبتها على استخدام الأدوات بل جعل الطالب مهيأً للعمل كباحث في مجال أمن المعلومات ومطور لأدوات في الحاسب الجنائي. يعني ذلك أن التجربة الألمانية في تدريس الحاسب الجنائي مركز على جانب علوم الحاسب مع وجود بعض المواد من القانون، على العكس تماماً التجربة البريطانية والتي اشتمل برنامجها الأكاديمي على مزيج من علوم الحاسب والقانون والعلوم الأمنية وغيرها.

تجارب من الولايات المتحدة

بدأ الاهتمام بتدريس الحاسب الجنائي كوحدة دراسية مستقلة في جامعة وسط متشيجن (Central Michigan University) بعد أحداث الحادي عشر من سبتمبر [11]. وقد جذبت الوحدة الدراسية العديد من الطلبة المهتمين بفهم كيفية التحقيق في جرائم الحاسب الآلي. بعدها توالت طرح الجامعات لبرامج أكاديمية تعمل على تدريس الحاسب الجنائي كتخصص مستقل متفرع من تخصص علوم الحاسب.

ففي دراسة مسحية أجراها قوتستوك وآخرون [6] عام 2005م على 32 برنامجاً أكاديمياً لتدريس تخصص الحاسب الجنائي موزعة كالتالي: ثمان منها برامج دبلوم مدته سنتين، وأربع منها برامج بكالوريوس، و13 منها شهادات متخصصة و سبع منها برامج دراسات عليا (ماجستير). تبين أن درجة الدبلوم تناولت مواد في نظم تشغيل الشبكات وأمن الحاسبات مع مادة أو أكثر تتناول كيفية تأمين البيانات على نحو فعال وكيفية استخراج البيانات لحفظها لحين استخدامها في المحكمة وكيفية إيجاد آثار النشاط الإجرامي في البيانات.كما أن البرنامج يحتوي على مواد في القانون ذات صلة بالتعامل مع الأدلة الجنائية. وقد لاحظ قوتستوك وآخرون أنه من بين برامج الدبلوم المطروحة، هناك فقط برنامج واحد أهتم بتدريس البرمجة كمادة مستقلة، يضاف إلى ذلك عدم اهتمام برامج الدبلوم بتدريس قواعد البيانات وتراكيب البيانات في أي من برامجها المطروحة.

بالنسبة لبرامج الشهادات المتخصصة، فتتراوح المدة الدراسية فيها ما بين خمسة أيام مكثفة إلى سنة دراسية متكاملة. وتتناول المواد المطروحة مقدمة في الحاسب الجنائي، وأمن المعلومات وتأمين المعلومات، وأحياناً نظم التشغيل ومادة في العدالة الجنائية والتشريعات القانونية.

أما بالنسبة لدرجة البكالوريوس، فقد وجد قوتستوك وآخرون خلال مسحهم أن البرامج المطروحة لهذه الدرجة تختلف بشكل كبير من جامعة لأخرى بناءً على تفرع التخصص من القسم العملي. فالبرامج المطروحة من قبل أقسام مثل المحاسبة أو علوم الحاسب أو القانون الجنائي تتناول في البداية مواد في أصل التخصص في أول البرنامج ومن ثم يتم التركيز في مستويات عليا على تخصص الحاسب الجنائي.

بيد أن درجة الماجستير في الحاسب الجنائي هي أكثر الدرجات تفاوتاً في دعمها للمواد المدرسة في هذا التخصص، ويرجع السبب في ذلك لاختلاف الخلفيات العلمية للملتحقين ببرامج الدراسات العليا. فعلى سبيل المثال، خريج قانون جنائي أو أدلة جنائية قد يتطلب منه دراسة متطلبات سابقة في علوم الحاسب والعكس في حالة كون الخريج من كلية علوم الحاسب.

وتجدر الإشارة هنا إلى أن جميع البرامج المذكورة سابقاً تختلف في شروط الالتحاق للدرجة المطلوبة، فبعضها يشترط وجود شهادة جامعية في تخصص علوم الحاسب أو قانون جنائي (برامج الدراسات العليا) والبعض الآخر قد يتطلب معرفة بسيطة باستخدام الحاسب (برامج الدبلومات).

جدول 2: توزيع المواد حسب وجودها في كل برنامج أكاديمي، ✓ تعني موجودة بالكامل، ⊘ تعني موجودة في بعض البرامج، ✗ تعني غير موجودة.

المادة / الدرجة	دبلوم	بكالوريوس	دراسات عليا	شهادة متخصصة
حاسب جنائي	✓	✓	⊘	✓
أمن الحاسبات وتأمين المعلومات	✓	⊘	⊘	✓
نظم التشغيل	✓	⊘	⊘	⊘
برمجة	⊘	⊘	⊘	✗
أخلاقيات	⊘	⊘	⊘	⊘

العدالة الجنائية والقانون	✓	✓	⊘	⊘
تربية عامة	✓	✗	✗	✗
مواد مختارة في علوم الحاسب أو تقنية المعلومات	✗	⊘	⊘	✗
مواد مختارة في أصل التخصص أو مواد عامة	⊘	⊘	⊘	✗

جدول 2 يلخص الدرجات العلمية للدراسة التي أجراها قوتستوك وآخرون وذلك بذكر المواد المطلوبة في كل درجة ومدى دعم كل درجة علمية لها. ويلاحظ من الجدول أن برنامج الدراسات العليا هي أكثرها مرونة في دعم المواد المختلفة يليها برنامج البكالوريوس ثم الدبلوم. كما أن الجدول يبين غياب واضح لمواد علمية كالرياضيات والإحصاء في البرامج الأكاديمية التي تناولها قوتستوك وآخرون في دراستهم.

أما في ورقة زو وفيك [14] فقد قاما بتقديم وصف للمقررات المطلوبة في تخصص الحاسب الجنائي لتلبي حاجات البرنامج الأكاديمي لدرجة البكالوريوس في علوم الحاسب بجامعة ولاية ديكوتا (Dakota State University). يهدف المقترح لتزويد الطالب بأساسيات الحاسب الجنائي بحيث يؤهلهم للعمل كمحللين جنائيين في مجال جرائم الحاسب. البرنامج المقترح يشمل المواد التالي:

1) **أساسيات الحاسب الجنائي (Computer Forensics Fundamentals)**: في هذه المادة، يتعلم الطلاب المفاهيم والمبادئ الأساسية في الحاسب الجنائي. ويغطي منهج المادة المواضيع التالية: تصنيف الأدلة الرقمية، وإجراءات الضبط والحفاظ على الأدلة، وأنواع جرائم الحاسب والانترنت ، والتحليل الإحصائي لجرائم الحاسوب. كما يتعلم الطلاب كيفية البحث واسترجاع المعلومات للعثور على أدلة باستخدام بعض الأدوات المشتركة. وأخيراً تناقش المادة المواضيع المتعلقة بالإجراءات القانونية واللوائح والقوانين باختصار.

2) **الدفاع والأدلة الجنائية المعاكسة (Defense and Forensic Countermeasures)**: تركز هذه المادة على استخدام الأدوات الدفاعية لتأمين الشبكة وكيفية استخدام هذه الأدوات مع مختلف نظم التشغيل والمنهجيات اللازمة لحماية الشبكة من خلال التدابير الدفاعية. المادة تتضمن مقدمة في طرق

الاختراقات وردود الفعل الضرورية والإجراءات المتبعة لمسئول الشبكة. كما تقدم المادة حالات تستخدم لوصف الهجمات الفعلية. وتهيئ المادة الطلاب على اكتساب مهارات الكشف والتحقيق ونظم وإجراءات المراجعة.

3) **حاسب جنائي متقدم (Advanced Computer Forensics)**: تتناول المادة المواضيع المستجدة في مجال الحاسب الجنائي. حيث يتعرف الطلاب على استخدام مهارات التحليل الشامل باستخدام أدوات التحليل (مثل برنامج EnCase 6) بالإضافة إلى كيفية استخدام الأدوات والتطبيقات الأخرى. وسيكون التركيز بشكل خاص على نظام الملفات (NTFS) لتعريف الطلاب على كيفية عمل نظام الملفات في ويندوز. ويقترح زو وفيك أن تكون المادة عبارة عن مزيج من المحاضرات، واستعراض للأدوات بقيادة المدرب، والتمارين العملية التي تركز على أدوات التحليل.

4) **التحقيق والحاسب الجنائي (Computer Forensics and Investigations)**: تركز هذه المادة على تعليم الطلاب متطلبات تحليل أنماط حركة البيانات في الشبكة وتتبع مصدرها، مثل تحليل البريد الالكتروني ورسائل الأجهزة النقالة. كما تشمل المادة الالتزامات المرتبطة بجمع الأدلة والشهادة في قاعة المحكمة.

5) **الإنترنت الجنائي (Internet Forensics)**: تعرف هذه المادة الطالب على مجموعة الأدلة المستقاة من الانترنت والبرامج. ويتم التركيز على استخدام أدوات وتقنيات التحليل لتحديد واسترجاع الأدلة المستقاة من الانترنت بطريقة سليمة. والمادة بطبيعة الحال تطرح حلولاً للمشاكل التي قد يواجهها الطالب أثناء التحليل. كما تتناول المادة طرق استرجاع البيانات وأدوات وممارسات لاستعادة المعلومات المساعدة في التحقيقات. يتعلم الطلاب خلال المادة طرق إظهار البيانات المخبئة بواسطة تقنيات التشفير والترميز ، وطرق إظهار كلمات السر المحمية.

6) **إدارة الأمن اللاسلكي الجنائي(Management of Wireless Forensic Security)**: تركز هذه المادة على دراسة التكنولوجيا اللاسلكية من منظور جنائي للمساعدة في التحقيق. يتعلم الطالب خلالها المفاهيم الأساسية للاتصالات التي تساعد على فهم إمكانيات وحدود مختلف التقنيات اللاسلكية.

7) **مشروع حاسب جنائي (Computer Forensics Project)**: يعتمد المشروع على تقديم سيناريو قائم من مسرح الجريمة ويطلب من كل طالب إجراء تحليل مفصل للبيانات في مختبر الحاسب الجنائي.

8) **قانون الانترنت (cyberlaw)**: يعرف قانون الانترنت على أنه دراسة أخلاقيات استخدام التكنولوجيا و النظام القانوني لإدارتها سواء في مكان العمل أو الانترنت. تركز المادة على القضايا المتعلقة بالتجارة الالكترونية، والتكنولوجيا، والملكية الفكرية والانترنت.

أما الباحث لو من جامعة ولاية ميتروبولتن (Metropolitan State University) [13] فقد تناولت ورقته تجربة جامعة ولاية ميتروبولتن في تصميم خطة دراسية لبكالوريوس في الحاسب الجنائي والتي بدء في تدريس هذا التخصص عام 2005 بواقع 124 ساعة دراسية للبرنامج ككل. كما ذكرت الورقة تجارب استحداث برنامج حاسب جنائي في جامعات أخرى في الولايات المتحدة، ثم تطرق الباحث لكيفية قيامهم بتطوير برنامج الحاسب الجنائي، والمنهجية التي اتبعوها في بناء البرنامج المقترح، وذلك بتحليل متطلبات سوق العمل. بعدها خلص الباحث لأهمية وجود أربع محاور رئيسية في البرنامج المقترح وهي (محور نظم التشغيل والشبكات، ومحور أمن الحاسب والمعلومات، ومحور الإجراءات والتقنيات و محور التحليل والعرض)، وقدتم إدراج مواد جاهزة من قسم علوم الحاسب لتغطية المحور الأول والثاني ومواد من قسم القانون والعدالة الجنائية والعلوم الشرطية مع تقنينها لخدمة مجال الحاسب لتغطية المحور الثالث والرابع. كما أن الورقة استعرضت الخطة الدراسية الكاملة لدرجة البكالوريوس موزعة على ثمانية فصول دراسية، والخطط المستقبلية لتطوير البرنامج.

وفي نفس السياق، تناولت ورقة كسلر وسشيرلينغ [25] تجربة كلية تشامبلين (Champlain College) في إعداد برنامج للحاسب الجنائي كدرجة بكالوريوس وكدبلوم. فقد بدأت الكلية بتقديم درجة البكالوريوس في الحاسب الجنائي منذ عام 2003م بعد تصاعد الطلب من قبل الدولة على وجود مثل هذه التخصصات نظراً لانتشار استخدام الحاسب والإنترنت والأجهزة الرقمية وعلاقتها كوسائط تخزينية للكشف عن الجرائم الرقمية. وتطرقت الورقة لخطوات نشأة البرنامج من إعداد الهيئة الاستشارية والتعاون مع الكيانات الأمنية ذات العلاقة إلى تحديد أهداف البرنامج ولوائحها التنظيمية والإدارية. بعدها تناولت الورقة شرح مفصل للمواد الإعدادية والأساسية والمتقدمة في التخصص، كما أن الورقة تحدثت عن تجربة طرح البرنامج للدارسة عن بعد بواسطة الانترنت [28] .
ويتضمن برنامج البكالوريوس مادتين في القانون (القانون الجنائي والقانون التجاري)، وخمس مواد في الحاسب وتقنية المعلومات وهي (إدارة الملفات والبرامج ، نظم التشغيل ، والبيانات ، والاتصالات وأمن الشبكات الحاسوبية) ، وثماني مواد في الحاسب الجنائي وهي (تحليل الوسائط الرقمية ، التحقيق الجنائي والحاسب الجنائي بجزأيه الأول والثاني).

وفي ورقتين لترويل وآخرون [26,27] ذكروا في الورقة الأولى [26] تجربة استحداث برنامج بكالوريوس ودراسات عليا في معهد روتشستر للتكنولوجيا (Rochester Institute of Technology) مع التركيز على أهداف كل برنامج والنتائج المتوقعة منه مع ذكر بعضاً من المشاريع المقترحة للدرجتين، وفي الورقة الثانية [27] ذكروا فيها تقييمهم للبرنامج بعد مرور سنة من تنفيذه وخاصة فيما يتعلق بالتحضيرات المعملية والتمارين العملية في مختبر الحاسب الجنائي وتلخيص للدروس المستفادة من تجربتهم.

أما معهد القوات الجوية للتكنولوجيا (Air Force Institute of Technology) فقد طرح ثلاث مسارات للدراسات العليا في الحاسب الآلي وهي: العمليات السايبرية (Cyber Operations)، علوم الحاسب (Computer Science)، وهندسة الحاسب (Computer Engineering)، مع إعطاء مواد موجهة لتخصص الحاسب الجنائي في هذه المسارات، حسب ما ذكر في ورقة بيترسن وآخرون [29].
المواد المطروحة للحاسب الجنائي في هذه المسارات تغطي خمسة مجالات هي: الأخلاقيات والإجراءات القانونية، العلوم الجنائية الأساسية، التقاط وتحليل الأجهزة الرقمية، الإنترنت الجنائي، وأدوات التحليل الرقمي.
ثم تطرقت الورقة لبعض المشاريع وسيناريوهات التمارين المعملية التي يعمل الطالب عليها، كمشروع الاختراقات وتتبع المخترق وتمرين استعادة الملفات بعد عملية تهيئة الجهاز وتغيير نظام التشغيل وتمرين آخر لرصد ورسم موقع الجريمة وتصويرها. كما ألمحت الورقة أيضاً لنوعية الأجهزة والإعدادات المخبرية لمعمل المعهد والبرامج المستخدمة.

وأخيراً، تتناول ورقة هارسون [29] بالتفصيل التحضيرات اللازمة لخلق مشاريع معملية في تخصص الحاسب الجنائي.

مناقشة وخلاصة التجارب السابقة

من خلال التجارب السابقة يتضح بجلاء الطلب المتزايد على عقد برامج أكاديمية وتدريبية في تخصص الحاسب الجنائي وذلك نتيجة لانتشار التعامل مع الحاسب والإنترنت واستخدامها في قضايا تمس أمن الدول أو في القضايا المالية والأخلاقية.
و على الرغم من الاختلاف المتفاوت بين البرامج المطروحة في نفس الدولة (كما هي التجربة الأمريكية) أو بين البرامج في الدول المختلفة (كما هي التجربة البريطانية والألمانية)، إلا أنها تتفق على أهمية تأهيل الملتحق بهذه البرامج من الناحية الأخلاقية والتقنية. يضاف إلى ذلك، أن الاختلاف الحاصل في كثافة المواد المقدمة لكل برنامج يعتمد على القسم الذي استحدث هذه الدرجة، وبما أن تركيز هذه الورقة قد تمحور حول تدريس تخصص الحاسب الجنائي المتفرع من قسم علوم الحاسب، يعني ذلك أن الأقسام الأخرى مثل المحاسبة والقانون وغيرها والتي طرحت تخصص للحاسب الجنائي في قسمها لم يتم التركز عليها في هذه الورقة وذلك لتحول بعضها تحت مظلة قسم علوم الحاسب كما أشار لذلك لو في ورقته [13] وأيضاً لفتح المجال للمهتمين بعمل دراسات مقارنة أكثر عمقاً.

وحسب ما تم الاطلاع عليه في التجارب السابقة هناك توجه للمطالبة باستحداث تخصص أكاديمي مستقل للحاسب الجنائي غير تابع لأي قسم أكاديمي يتمتع باستقلاليته البحثية والتطويرية وفي نفس الوقت يكون مزيج لمواد من قسم علوم الحاسب والقانون والاقتصاد والعلوم الأمنية وغيرها من الأطراف ذات العلاقة.

كما نستخلص من التجارب السابقة بعض العناصر الجوهرية المفترض تواجدها في أي برنامج أكاديمي لتدريس تخصص الحاسب الجنائي والمخرجات المتوقعة من هكذا برنامج وهي:

1. أهمية وجود معمل حاسب جنائي مهيأ عتادياً وبرمجياً.
2. التكاملية بين المحاضرات المطروحة والتمارين المعملية هي من أبرز عوامل نجاح تدريس مواد تخصص الحاسب الجنائي، لذا لابد من بذل مجهود كبير لخلق تمارين معملية فاعلة وواقعية.
3. مع أن بعض البرامج أغفلت وجود مادة للإحصاء والرياضيات، إلا أنه من الأهمية بمكان وجود هاتين المادتين وذلك لأنهما تساعدان الملتحق على فهم نتائج تحقيقاته والتعبير عنها باستخدام طرق علمية صحيحة.
4. أهمية تغطية مناهج البرنامج الأكاديمي للإجراءات المعيارية عند التحقيق والتحري في جرائم الحاسب الجنائي والمكونة من: استخلاص وكشف البيانات والاحتفاظ بها، وتحليلها ثم توثيقها وعرضها كأدلة جنائية.
5. استضافة خبراء من مختلف القطاعات الأمنية والأكاديمية والمؤسساتية لعكس صورة حية عن الحياة العملية للعامل في مجال الحاسب الجنائي ونقل خبراتهم داخل هذه الكيانات.
6. خريج الحاسب الجنائي لابد أن يكون ملماً بمهارات عدة منها المهارات التقنية والمهارات المهنية الاحترافية والمهارات التواصلية كتابياً وخطابياً. أي أن من المتوقع من خريج الحاسب الجنائي أن يلم بمهارات أساسية منها: (أ) أن تكون لديه خلفية جيدة بجهاز الحاسب وكيفية عمله وأيضاً قادر على التعامل مع مختلف الأجهزة والبرمجيات. (ب) أن يكون لديه خلفية جيدة في القانون ليكون قادراً على فرز وتقييم الأدلة ذات الصلة. (ج) أن يكون على خبرة ودراية بأحكام التشريع الجنائي، والامتثال للمنهج العلمي السليم عند توثيق الجرائم. (د) أخيراً، لا بد من العامل في مجال الحاسب الجنائي الحكم بحيادية بعيداً عن سياق التوتر النفسي والنزعات الذاتية أو المكاسب الشخصية، وهذا يستدعي ضرورة التأكيد على تدريس منهج متكامل ومكثف في قضايا الأخلاقيات المهنية.

الخاتمة

في هذه الورقة تم التعرف على مجال الحاسب الجنائي وعرض تجارب بعض الدول في تدريسه كتخصص مستقل أو كتخصص متفرع من علوم الحاسب. ويتضح من استعراض البرامج السابقة في الحاسب الجنائي أن هذا المجال هجين (أي متعدد التخصصات multi-disciplinary) ويستقي مواده من مختلف التخصصات مثل العدالة الجنائية و القانون، والأخلاقيات، والعلوم الأمنية، وعلوم الحاسب، وتكنولوجيا المعلومات. ولبناء برنامج متكامل في الحاسب

الجنائي لابد من مراعاة عوامل مختلفة منها عامل الإمكانات المادية والكوادر البشرية المؤهلة بالإضافة لعوامل تربوية مختصة بتصميم البرنامج الأكاديمي المناسب والمواكب للتطورات في هذا المجال.

وبالطبع حتى تتبنى الجهات المهتمة في المملكة برنامجاً متكاملاً في الحاسب الجنائي لابد من النظر في مناهج الدول الأخرى مع تقنينها لخدمة التشريع في المملكة العربية السعودية وخاصة فيما يتعلق بالأخلاقيات والقوانين الجنائية، كما أن على أي برنامج مستحدث للحاسب الجنائي تلمس احتياجات الكيانات الأمنية في المملكة.

المصادر الأجنبية

[1] Taylor C., Endicott-Popovsky B., and Phillips A., (2007). "Forensics Education: Assessment and Measures of Excellence". In Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering. pp. 155-165. IEEE Computer Society.

[2] Computer forensics Training Video CD VTC, online http://www.vtc.com/, last accessed 30, July 2007.

[3] The International Society of Forensic Computer Examiners, online http://www.isfce.com/, last accessed 30, July 2007.

[4] Butler County Community College, Computer Forensics, online http://www.bc3.edu/academics/technology/compforensics.htm, last accessed 30, July 2007.

[5] SFCC, Spokane Falls Community College Computer Forensics, http://www.spokanefalls.edu/TechProf/InfoSys/CertForensics.aspx, last accessed 30, July 2007.

[6] Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S. and Stein, M., (2005). "Computer forensics programs in higher education: a preliminary study", SigCSE '05. pp. 147-151 ACM Press.

[7] Purdue College, Computer Forensics, http://www.cerias.purdue.edu/research/forensics/, last accessed 30, July 2007.

[8] John Hopkins University, http://undergraduate.jhu.edu/it/index.cfm?action=curriculum&areacode=306&majorcode=306C, last accessed 30, July 2007.

[9] e-Evidence, Digital Forensics Education, http://www.e-evidence.info/education.html, last accessed 30, July 2007.

[10] Isner, J. (2003). "Computer Forensics: An Emerging Practice in the Battle Against Cyber Crime", SANS Institute, Bethesda, Maryland.

[11] Yasinsac, A., Erbacher, R., Marks, D., Pollitt, M., and Sommer, P. (2003). "Computer Forensics Education". IEEE Security & Privacy, July/August 2003, pp.15-23.

[12] Fernandez J. D., Smith S., Garcia M. and Kar D. (2005). *Computer forensics: a critical need in computer science programs*. Journal of Computing Sciences in Colleges. pp. 315 - 322.

[13] Liu J., (2006). "Developing an Innovative Baccalaureate Program in Computer Forensics". In proceedings of the 36th ASEE/IEEE Frontiers in Education Conference. San Diego, CA. IEEE Computer Society.

[14] Figg, W. and Zhou Z. (2007). A *computer forensics minor curriculum proposal*. Journal of Computing Sciences in Colleges. Vol 22(4). pp. 32 - 38.

[15] Francia G. and K. Clinton. (2005). "Computer Forensics Laboratory and Tools," Proceedings of the 3rd Annual CCSC MidSouth Conference. April 1-2, 2005.The Journal of Computing Sciences in Colleges. Vol 20(6). pp. 143-150.

[16] Erbacher R., (2002). "Computer Forensics: Training and Education". Available online http://citeseer.ist.psu.edu/561426.html, last accessed 3, July 2007.

[17] George Washington University, Available online http://www.gwu.edu/~forensic/htci.htm, last accessed 3, July 2007.

[18] High Tech Crime Network, Certification Requirements, Available online http://www.htcn.org/cert.htm, last accessed 4, July 2007.

[19] IACIS, CFCE Certification, Available online http://www.iacis.info/iacisv2/pages/training.php, last accessed 4, July 2007.

[20] Cyber Security Institute, CSFA, Available online http://www.cybersecurityinstitute.biz/, last accessed 4, July 2007.

[21] Sutherland I., (2006). "Challenges in Teaching Computer Forensics", Available online http://www.ics.heacademy.ac.uk/events/displayevent.php?id=139. last accessed 4, July 2007.

[22] Alderson R. (2006). "Computer Forensics – the Student Experience ". Available online http://www.ics.heacademy.ac.uk/events/displayevent.php?id=139. last accessed 4, July 2007.

[23] Irons, A. D., Laing, C., Anderson, P., (2006) Pedagogic Innovation in Teaching Computer Forensics, paper presented at 7th Annual HE Academy Conference for Subject Centre for Information and Computer Sciences, Trinity College, Dublin, 29 – 31st August 2006.

[24] Dornseif, M., Freiling, F. C., Holz, T., Irons, A. D., Laing, C., Mink, M., and Anderson P., (2006) 'Comparative Study of Teaching Forensics at a University Degree Level', IMF 2006, International Conference on IT-Incident Management & IT-Forensics, October 18 - 19, Stuttgart, Germany.

[25] Kessler G. and Schirling M., (2006). *The Design of an Undergraduate Degree Program in Computer & Digital Forensics*. Journal of Digital Forensics, Security and Law. Vol 1(3). Online http://www.jdfsl.org/.

[26] Troell, L., Pan, Y., and Stackpole B., (2003). "Forensic Course Development". In Proceeding of the 4th conference on Information technology education. ACM Press. pp. 265 - 269.

[27] Troell L., Pan Y. and Stackpole B., (2004). "Forensic course development: one year later". In Proceedings of the 5th conference on Information technology education - CITC5 '04. ACM Press. pp. 50-55.

[28] Kessler G., (2007). “Online Education in Computer and Digital Forensics: A Case Study”. In Proceedings of the 40th Annual Hawaii International Conference on System Sciences. IEEE Computer Society. pp. 264a.

[29] Peterson G. L., Raines R. A. and Baldwin R. O., (2007). “Graduate Digital Forensics Education at the Air Force Institute of Technology”. In HICSS '07: Proceedings of the 40th Annual Hawaii International Conference on System Sciences. IEEE Computer Society. pp. 264c.

[30] Harrison, W. (2006). *A term project for a course on computer forensics*. Journal on Educational Resources in Computing (JERIC). Vol 6(3). p. 6. ACM Press.

[31] McCombie, S. and Warren, M. (2003). "Computer Forensic: An Issue of Definitions." In Proceedings of the first Australian computer, Network and information forensics. Available online http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2003/forensics/pdf/14_final.pdf. Last accessed 7, July 2007.