ادله الکترونیکی و تحلیل جرائم سایبری برای کارشناسان رسمی دادگستری

راهنمای جامع در کشف، تحلیل و ارزیابی ادله الکترونیکی و استنادپذیری با توجه به رویکردهای نوین فضای مجازی، رباتیک و هوش مصنوعی (به همراه موردکاوی‌های تشریحی و کاربردی)

با بهره‌گیری از آخرین منابع علمی، فنی و حقوقی داخلی و بین‌المللی، مبتنی بر قوانین ایران، شامل قانون جرائم رایانه‌ای، قانون تجارت الکترونیکی و آیین‌نامه استنادپذیری ادله الکترونیکی

نویسنده و مولف:

مهرداد تاج بخش (کارشناس رسمی دادگستری، رشته رایانه و فناوری اطلاعات)

عنوان کتاب: ادله الکترونیکی و تحلیل جرائم فضای مجازی برای کارشناسی رسمی دادگستری – راهنمای جامع در کشف، تحلیل و ارزیابی ادله الکترونیکی و استنادپذیری با توجه به کاربردهای نوین فضای مجازی، رباتیک و هوش مصنوعی (به همراه موردکاوی‌های تشریحی و کاربردی)

Title: Cyber Crime Investigation & Digital Forensics in Official Expertise (A practical guide with case studies & best practices)

نویسنده و مولف: مهرداد تاج‌بخش (کارشناس رسمی دادگستری)

ناشر: انتشارات اردلان

نوبت چاپ: اول

تاریخ چاپ: بهار ۱۴۰۴

شماره شابک: ۹۷۸-۹۶۴-۲۸۸۹-۰۲-۰

انتشارات اردلان: تهران، شمال میدان هفت‌تیر، خ ملایری پور غربی، پلاک ۱۰۲ واحد ۶

تلفن: ۸۶۰۷۱۲۴۶ (۰۲۱)

همراه/ واتس‌اپ: ۰۹۱۲ ۴ ۲۷۲ ۲۷۲

رایانامه: *mehrdad@highexpert.ir*

تارنمای کارشناس برتر (سفارش نسخه دیجیتال کتاب): *www.highexpert.ir*

فهرست مطالب

پیشگفتار

در جهان امروز، وابستگی روزافزون جوامع به فناوری‌های اطلاعاتی و ارتباطی، شکل‌گیری زیست‌بوم دیجیتال و گسترش تعاملات انسانی و سازمانی در فضای مجازی، بُعدی نوین و پیچیده به مفاهیم "جرم"، "دلیل" و «عدالت» افزوده است. وقوع جرائم رایانه‌ای، چالش‌های ناشی از هوش مصنوعی، سامانه‌های رباتیک، خودروهای خودران، پهپادها و اکوسیستم پیچیده اینترنت اشیاء، نه تنها نظام حقوقی کشورها را تحت‌تأثیر قرار داده‌اند، بلکه فرآیندهای کارشناسی رسمی دادگستری را نیز دچار تحولی بنیادی کرده‌اند.

در چنین شرایطی، "ادله الکترونیکی" به‌عنوان یکی از مهم‌ترین ابزارهای کشف حقیقت در رسیدگی‌های قضایی، جایگاهی بی‌بدیل یافته است. اما ماهیت متغیر، فناورانه و گاه پنهان این نوع از ادله، موجب شده است که ارزیابی، تحلیل و استنادپذیری آن‌ها، نیازمند دانش میان‌رشته‌ای دقیق و رویکردی نظام‌مند باشد.

این کتاب با عنوان "ادله الکترونیکی و تحلیل جرائم سایبری برای کارشناسان رسمی دادگستری" و با زیرعنوان "راهنمای جامع در کشف، تحلیل و ارزیابی ادله الکترونیکی و استنادپذیری با توجه به کاربردهای نوین فضای مجازی، رباتیک و هوش مصنوعی"، تلاشی است برای پر کردن این خلأ علمی و حرفه‌ای.

نگارش این کتاب با هدف ارائه راهنمایی کاربردی و تحلیلی برای کارشناسان رسمی دادگستری، قضات، وکلا، پژوهشگران و فعالان حوزه فناوری صورت گرفته است. در تدوین مطالب، ضمن بهره‌گیری از آخرین منابع علمی، فنی و حقوقی داخلی و بین‌المللی، از تجربه‌های میدانی، رویه‌های قضایی و اسناد بالادستی حقوق ایران از جمله قانون جرائم رایانه‌ای (۱۳۸۸)، قانون تجارت الکترونیکی (۱۳۸۲) و آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی (۱۳۹۳) استفاده شده است.

در ساختار کتاب، تلاش شده است تا علاوه بر مفاهیم نظری، به ابعاد عملیاتی، روش‌های کشف و مستندسازی ادله، ابزارهای تحلیل دیجیتال، چالش‌های حقوقی و اخلاقی، مدل‌های ارزیابی، و مهم‌تر از همه، کاربردهای نوین این مباحث در حوزه‌هایی همچون شبکه‌های اجتماعی، فضای ابری، سامانه‌های کلان نرم‌افزاری، ربات‌های انسان‌نما، خودروهای خودران، پهپادها و سامانه‌های *SDN* نیز پرداخته شود.

در پایان هر فصل، بخشی با عنوان "پاسخ به پرسش‌های متداول" گنجانده شده است تا مخاطب، با اطمینان و درک بهتر، مفاهیم و مباحث تخصصی را دنبال کند. همچنین موردکاوی‌های واقعی و چک‌لیست‌های کارشناسی در این کتاب گنجانده شده‌اند تا در فرآیند تهیه گزارش کارشناسی و تحلیل پرونده‌های فناورانه یاری‌رسان باشند.

امید است این اثر بتواند گامی مؤثر در ارتقای دانش کارشناسی کشور و تقویت نظام عدالت در عصر دیجیتال باشد.

فصل سوم) روش‌ها و ابزارهای کشف، تحلیل و مستندسازی ادله دیجیتال

تحلیل و کشف ادله دیجیتال، نیازمند بهره‌گیری از مدل‌ها، ابزارها و رویکردهای تخصصی و ساختاریافته است. در این فصل، ابتدا با مدل‌های استاندارد تحلیل دیجیتال مانند *DFRWS*، *ISO/IEC 27037* و *NIST* آشنا می‌شویم و نحوه تطبیق آن‌ها با الزامات حقوقی ایران بررسی می‌شود.

سپس ابزارهای تخصصی نرم‌افزاری و سخت‌افزاری در تحلیل داده‌های دیجیتال معرفی می‌گردند و اصول انتخاب ابزار متناسب با نوع پرونده مطرح می‌شود. در ادامه، چالش‌های فنی همچون رمزنگاری، حجم انبوه داده‌ها، ناشناس‌سازی، و پیچیدگی معماری شبکه‌ها (مانند *Cloud* ، *IoT* و *SDN*[1]) با معرفی راهکارها و ابزارهای تحلیلی تحلیل می‌شود.

این فصل همچنین به ملاحظات حقوقی، عملیاتی و تخصصی در فرآیند تحلیل می‌پردازد؛ از جمله رعایت زنجیره سلامت داده، مستندسازی، انتخاب ابزار معتبر، و مسئولیت‌های کارشناسی در تدوین گزارش. در بخش پایانی نیز کاربردهای عملی تحلیل دیجیتال در پرونده‌های واقعی مانند اختلافات قراردادی، حملات سایبری، جعل اسناد، نقض مالکیت فکری و افترای اینترنتی به تفصیل بررسی شده است.

این فصل، پایه فنی، حقوقی و کاربردی لازم برای تدوین یک گزارش کارشناسی معتبر و دفاع‌پذیر در زمینه ادله دیجیتال را فراهم می‌سازد.

۱–۳) مدل‌های استاندارد در فرآیند تحلیل دیجیتال

تحلیل ادله دیجیتال، از حیث فنی پیچیده و از منظر حقوقی حساس و مستعد اعتراض است. در فرآیند کارشناسی این نوع ادله، تنها نتیجه نهایی اهمیت ندارد، بلکه مسیر رسیدن به نتیجه، ابزارهای استفاده‌شده، مستندات، زمان‌بندی و رعایت اصول قانونی از اهمیت فوق‌العاده‌ای برخوردار است. به‌همین دلیل، استفاده از مدل‌های استاندارد تحلیل دیجیتال یک الزام حرفه‌ای برای کارشناسان رسمی دادگستری به شمار می‌رود.

این مدل‌ها چارچوبی گام‌به‌گام، قابل تکرار، مستند و منطبق با موازین بین‌المللی فراهم می‌سازند و در هماهنگی کامل با الزامات آیین‌نامه‌های داخلی از جمله آیین‌نامه استنادپذیری ادله الکترونیکی هستند.

- **ضرورت بهره‌گیری از مدل‌های استاندارد**

استفاده از مدل‌های تحلیلی استاندارد، اهداف زیر را محقق می‌سازد:

- حفظ زنجیره سلامت[2]
- قابلیت بازسازی و بررسی مجدد فرآیند کارشناسی
- مستندسازی دقیق و حرفه‌ای تمامی مراحل

[1] *Software Defined Network*
[2] *Chain of Custody*

- پیشگیری از نقض حقوق طرفین دعوی
- افزایش استنادپذیری گزارش کارشناسی در مراجع قضایی

مدل‌سازی، ارتباط فنی—حقوقی بین کارشناس و قاضی را برقرار می‌کند.

- **معرفی مدل‌های مرجع جهانی**
  - مدل *DFRWS (Digital Forensic Research Workshop)*

سال ارائه: ۲۰۰۱ – اولین چارچوب استاندارد تحلیل دیجیتال

مراحل:

۱) شناسایی[۳]

۲) حفظ داده[۴]

۳) گردآوری[۵]

۴) بررسی[۶]

۵) تحلیل[۷]

۶) ارائه[۸]

تأکید بر تفکیک فنی مراحل، حفظ داده اصلی و مستندسازی ابزارها و مسیر بررسی.

- مدل *ACPO* (بریتانیا)

تدوین‌شده توسط پلیس انگلستان

اصول کلیدی:

- عدم تغییر داده اصلی بدون مستندسازی
- ضرورت مستندسازی در تمام مراحل
- استفاده فقط از ابزارهای تأییدشده
- ارائه گزارش قابل دفاع در دادگاه

مناسب برای کاربردهای رسمی و قضایی، حتی در سطح پرونده‌های پیچیده.

- مدل *NIST SP 800-86* (ایالات متحده)

ارائه‌شده توسط مؤسسه ملی استاندارد و فناوری آمریکا

مراحل:

۱) آماده‌سازی[۹]

۲) جمع‌آوری

---

[۳] *Identification*
[۴] *Preservation*
[۵] *Collection*
[۶] *Examination*
[۷] *Analysis*
[۸] *Presentation*
[۹] *Preparation*

۳) بررسی
۴) تحلیل
۵) گزارش‌دهی[۱۰]

تطبیق‌پذیر با اکثر پرونده‌های قضایی و نیازهای کارشناسی رسمی در ایران.

- استانداردهای *ISO/IEC 27037* و *ISO/IEC 27042*

کاربرد جهانی برای شناسایی، گردآوری، حفظ و تحلیل شواهد دیجیتال

مزایای کلیدی:

- تعیین صلاحیت فرد تحلیل‌گر
- الزام به ابزار معتبر و ثبت‌شده
- ثبت دقیق زمان، مکان، اقدامات، هش داده‌ها و فرد مسئول در هر مرحله

برای استفاده در نهادهای حقوقی و فنی کشورهای مختلف از جمله ایران قابل انطباق است.

- **تطبیق مدل‌ها با فرآیند کارشناسی رسمی در ایران**

در ایران، مطابق با آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی، کارشناسان رسمی باید به‌گونه‌ای عمل کنند که:

- از داده اصلی نسخه‌برداری ایمن تهیه شود
- از ابزارهای تأییدشده استفاده شود
- زنجیره حفاظتی (زنجیره سلامت) حفظ شود
- تمامی اقدامات به‌طور مستند ثبت گردد

این مفاهیم، دقیقاً در مدل‌های *DFRWS*، *NIST*، *ACPO* و *ISO* نیز وجود دارند.

- **تطبیق زنجیره حفاظتی ایران با مدل‌های بین‌المللی**

زنجیره حفاظتی در آیین‌نامه‌های ایران معادل مستقیم "*Chain of Custody*" در مدل‌های بین‌المللی است. مطابقت تطبیقی آن‌ها را در جدول زیر ببینید:

مرحله	زنجیره حفاظتی (ایران)	مدل بین‌المللی متناظر
شناسایی منبع	تعیین دستگاه، رسانه، فضای ابری	*Identification (DFRWS)*
حفظ داده	تهیه نسخه قانونی، ثبت هش	*Preservation (DFRWS/NIST)*
گردآوری	استخراج اطلاعات با ابزار قانونی	*Collection (NIST/ISO)*
بررسی	جداکردن داده‌های مرتبط	*Examination (ACPO/NIST)*
تحلیل	تفسیر رفتار دیجیتال و مستندسازی	*Analysis* (همه مدل‌ها)
ارائه گزارش	مستند، دقیق، زمان‌مند	*Presentation (DFRWS) / Reporting (NIST)*

[۱۰] *Reporting*

نتیجه: الزامات قانونی ایران در زمینه استنادپذیری دیجیتال، به‌طور کامل قابل انطباق با مدل‌های تحلیل دیجیتال بین‌المللی هستند.

- توصیه‌های عملی برای کارشناسان رسمی
- از مدل‌های بین‌المللی به‌عنوان راهنمای عملی استفاده کنید
- ابزارها، نسخه‌ها، هش‌ها و زمان‌ها را دقیق مستند کنید
- داده اصلی را دست‌نخورده نگه دارید؛ تنها نسخه کپی را بررسی کنید
- گزارش نهایی را در قالبی تنظیم کنید که مسیر تحلیل در آن شفاف و گام‌به‌گام باشد
- مدل انتخابی را در گزارش معرفی کرده و فرآیند را بر اساس آن مستند کنید

تحلیل دیجیتال بدون مدل استاندارد، نه‌تنها ضعیف از نظر فنی است، بلکه در مراجع قضایی نیز با چالش روبه‌رو خواهد شد. مدل‌هایی چون *DFRWS* ، *NIST*، *ACPO* و *ISO* نه‌تنها ابزارهای بین‌المللی، بلکه راهکارهای عملی برای اجرای مفاد آیین‌نامه‌های داخلی ایران نیز هستند.

کارشناس رسمی حرفه‌ای، نه‌فقط داده‌ها، بلکه فرآیند برخورد با آن‌ها را نیز استانداردسازی می‌کند.

در دنیای پیچیده ادله الکترونیکی، مدل تحلیل، پشتوانه قانونی گزارش کارشناسی است.

۲–۳) لزوم مدل‌سازی در تحلیل ادله دیجیتال

تحلیل ادله دیجیتال برخلاف ظاهر فنی آن، فرآیندی صرفاً تکنیکی نیست. این تحلیل، نیازمند چارچوبی نظام‌مند، مستند، گام‌به‌گام و منطبق با اصول حقوقی است. در صورتی که روند تحلیل فاقد ساختار مشخص و قابل بازسازی باشد، نه‌تنها نتایج به‌دست‌آمده از نظر حقوقی قابل استناد نخواهند بود، بلکه ممکن است موجبات تضییع حقوق یکی از طرفین دعوی یا نقض زنجیره سلامت را فراهم آورد.

در همین راستا، "مدل‌سازی" به‌عنوان سنگ‌بنای فرآیند تحلیل دیجیتال، نقشی اساسی در تضمین اعتبار، شفافیت و تکرارپذیری گزارش کارشناسی دارد.

- **اهمیت ادله دیجیتال و تفاوت آن با سایر انواع دلیل**

ادله دیجیتال دارای ویژگی‌هایی است که آن را از دیگر انواع ادله (سند کتبی، شهادت، معاینه محل و سایر موارد) متمایز می‌سازد:

ویژگی	توضیح
پنهان‌بودن	ادله دیجیتال اغلب در بسترهایی غیرمستقیم مانند هارد دیسک، حافظه‌های جانبی، حافظه *RAM*، یا فضای ابری ذخیره می‌شوند و مستقیماً قابل رویت نیستند.
حساسیت بالا	کوچک‌ترین تغییر در داده‌ها، زمان دسترسی یا حتی اتصال به شبکه، می‌تواند ماهیت دلیل را تغییر دهد یا از بین ببرد.
نیاز به ابزار تخصصی	خوانش، استخراج، تحلیل و مستندسازی داده‌های دیجیتال نیازمند ابزارهای نرم‌افزاری و سخت‌افزاری ویژه و معتبر است.
قابلیت جعل یا دستکاری آسان	بر خلاف اسناد فیزیکی، داده‌های دیجیتال به‌راحتی قابل کپی، حذف، یا جعل هستند.
چندلایه بودن داده‌ها	داده‌ها ممکن است در لایه‌های مختلف سیستمی، اپلیکیشنی، شبکه‌ای یا فیزیکی پراکنده باشند.

نتیجه: بدون فرآیند مدل‌مند و مستند، اعتبار این دسته از ادله به‌راحتی قابل خدشه خواهد بود.

- **ضرورت مدل‌سازی در فرآیند تحلیل دیجیتال**

الف) تضمین زنجیره سلامت *(Chain of Custody)*

زنجیره سلامت به معنای ثبت کامل و دقیق مراحل:

- شناسایی
- انتقال
- نگهداری
- بررسی
- تحلیل
- گزارش

از زمان کشف دلیل دیجیتال تا زمان ارائه آن به مرجع قضایی است. مدل‌سازی فرآیند تحلیل، ابزاری برای ثبت گام‌به‌گام این زنجیره و جلوگیری از خدشه به تمامیت داده‌ها است.

مثال: در صورت عدم ثبت دقیق ابزار تحلیل‌شده، نسخه تهیه‌شده از داده، زمان دسترسی، و مشخصات کارشناس، ممکن است متهم یا شاکی ادعا کند داده‌ها تغییر یافته‌اند یا دستکاری شده‌اند.

ب) ایجاد تکرارپذیری[۱۱] و بازسازی فرآیند

[۱۱] *Repeatability*

یکی از اصول پذیرفته‌شده در دادرسی‌های کیفری و حقوقی، امکان بررسی مجدد گزارش کارشناسی توسط کارشناس ثانویه است. این امر تنها در صورتی ممکن خواهد بود که:

- مسیر تحلیل شفاف باشد
- ابزارها و تنظیمات آن‌ها ثبت شده باشد
- داده‌های ورودی و خروجی دارای کدهای هش[۱۲] معتبر باشند
- مستندسازی دقیقی از فعالیت‌های انجام‌شده وجود داشته باشد

در غیاب مدل مستند، فرآیند تحلیل قابل راستی‌آزمایی نخواهد بود.

ج) رعایت ملاحظات حقوقی و انطباق با آیین‌نامه‌ها

در قوانین ایران نیز، خصوصاً در "آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی"، بر اصولی مانند:

- حفظ اصالت داده
- استفاده از ابزارهای معتبر
- تهیه نسخه اصلی و نسخه تحلیل
- تفکیک بین جمع‌آوری و تحلیل

تأکید شده است.

مدل‌سازی فرآیند تحلیل، در واقع ضمانت اجرای همین اصول در عمل است.

د) سازگاری با استانداردهای بین‌المللی

در جهان، مدل‌هایی مانند *DFRWS* ، *NIST SP800-86*، *ACPO* و استانداردهای *ISO/IEC 27037*، فرآیند تحلیل دیجیتال را به‌صورت گام‌به‌گام و مستند تدوین کرده‌اند. استفاده از این مدل‌ها، کارشناسان را به سطحی از تحلیل می‌رساند که در مجامع بین‌المللی نیز قابل پذیرش است.

- **پیامدهای نبود مدل‌سازی**

وضعیت بدون مدل‌سازی	پیامد حقوقی و کارشناسی
مستندسازی ناقص	گزارش فاقد اعتبار قضایی
عدم ثبت ابزار و روش‌ها	قابل بازسازی نبودن فرآیند
تداخل تحلیل و گردآوری	نقض زنجیره سلامت
استفاده از ابزارهای غیررسمی	رد گزارش در دادگاه
تکیه بر حافظه شخصی	تشکیک در بی‌طرفی و دقت گزارش

مثال: در پرونده‌ای که فایل‌های سیستم حذف شده بود، کارشناس نتوانست ثابت کند که فایل‌ها در زمان تحویل اولیه موجود بوده‌اند، زیرا هیچ نسخه اولیه مستندی تهیه نکرده بود.

[۱۲] *Hash*

- **مزایای کاربردی مدل‌سازی برای کارشناسان رسمی**

مزیت	نتیجه عملی
شفافیت فرآیند	افزایش اعتبار و استنادپذیری گزارش
آموزش‌پذیری	انتقال تجربه به کارشناسان جوان یا همکاران
امکان دفاع در دادگاه	پاسخ به ایرادات و پرسش‌های قاضی یا وکیل
پیشگیری از اشتباهات رایج	کاهش احتمال تداخل مراحل یا نقض اصالت داده
الگوگیری برای گزارش‌های بعدی	تدوین رویه قابل استناد در مراجعات بعدی

تحلیل دیجیتال بدون مدل‌سازی مانند حرکت در تاریکی بدون نقشه است. کارشناس رسمی دادگستری، برای انجام کارشناسی دقیق، بی‌طرفانه و قابل دفاع، نیازمند مدل ساختاریافته‌ای است که در آن هر مرحله، ابزار، مستند، فرد مسئول و زمان اجرا مشخص باشد.

مدل‌سازی، نه‌تنها ابزار کارشناسی فنی، بلکه سپر حقوقی گزارش در برابر ایرادات و چالش‌های دادگاه است.

رعایت مدل استاندارد، گامی مهم در مسیر حرفه‌ای‌شدن کارشناسی رسمی در عصر دیجیتال است.

۳-۳) چالش‌های فنی در تحلیل داده‌های رایانه‌ای و شبکه‌ای

تحلیل داده‌های رایانه‌ای و شبکه‌ای برخلاف ظاهر تکنیکی آن، با چالش‌هایی مواجه است که نه‌فقط به مهارت فنی، بلکه به شناخت ساختار داده، نحوه جمع‌آوری، ابزارهای قابل استناد، رعایت زنجیره سلامت و محدودیت‌های قانونی وابسته است. این چالش‌ها در صورت عدم شناخت کافی، می‌توانند منجر به کاهش دقت تحلیل، رد گزارش در دادگاه و حتی نقض حقوق طرفین دعوی شوند.

در این بخش، مهم‌ترین چالش‌های فنی که کارشناسان رسمی در حوزه تحلیل داده‌های دیجیتال ممکن است با آن مواجه شوند، طبقه‌بندی و تحلیل شده‌اند.

- **چالش‌های فنی در تحلیل داده‌های رایانه‌ای**
  - ساختار پیچیده سیستم‌عامل‌ها و فایل‌ها

یکی از نخستین چالش‌هایی که کارشناسان رسمی دادگستری در تحلیل ادله دیجیتال با آن مواجه می‌شوند، تنوع و پیچیدگی ساختارهای سیستم‌عامل‌ها و فایل‌سیستم‌ها است. هر سیستم‌عامل (ویندوز، لینوکس، اندروید، مک، *iOS* و غیره) معماری خاصی دارد که نحوه ذخیره، نگهداری، حذف، لاگ‌برداری و رمزنگاری داده‌ها را متفاوت می‌سازد.

واژه‌نامه تخصصی فارسی به انگلیسی

واژه فارسی	ترجمه انگلیسی
ادله الکترونیکی	*Electronic Evidence*
جرائم سایبری / جرائم رایانه‌ای	*Cybercrime / Computer Crime*
کارشناسی رسمی دادگستری	*Official Judicial Expert*
تحلیل دیجیتال	*Digital Forensics*
زنجیره سلامت (شواهد)	*Chain of Custody*
اصالت دیجیتال	*Digital Authenticity*
لاگ (وقایع ثبت‌شده)	*Log File / Event Log*
متادیتا	*Metadata*
نسخه پشتیبان	*Backup*
هش‌کد (تابع درهم‌سازی)	*Hash Code / Hash Function*
امضای دیجیتال	*Digital Signature*
حریم خصوصی	*Privacy*
داده‌های شخصی	*Personal Data*
مجوز قضایی	*Judicial Warrant / Legal Authorization*
ضبط دیجیتال	*Digital Seizure*
تحلیل شبکه	*Network Analysis*
بازسازی رویداد	*Event Reconstruction*
نرم‌افزار تحلیل فورنزیک	*Forensic Analysis Software*
استخراج اطلاعات	*Data Extraction*
کشف فایل‌های حذف‌شده	*Deleted File Recovery*
بدافزار	*Malware*
حمله سایبری	*Cyber Attack*
نفوذ (غیردرجهت مجاز)	*Unauthorized Access / Intrusion*
بلاک‌چین	*Blockchain*
قرارداد هوشمند	*Smart Contract*
رمزدارایی / رمزارز	*Crypto Asset / Cryptocurrency*
خودروی خودران	*Autonomous Vehicle*
سامانه کنترل صنعتی(SCADA)	*SCADA (Supervisory Control and Data Acquisition)*
هوش مصنوعی	*Artificial Intelligence (AI)*
یادگیری ماشین	*Machine Learning (ML)*
تحلیل الگوریتم	*Algorithm Analysis*
داده‌های حجیم / کلان‌داده	*Big Data*

Digital Platform	پلتفرم دیجیتال
Security Vulnerability	آسیب‌پذیری امنیتی
Intrusion Detection System (IDS)	سیستم تشخیص نفوذ
Decryption Tool	ابزار رمزگشایی
Open-Source Software	نرم‌افزار متن‌باز
RAM Capture	ضبط حافظه*RAM*
Disk Imaging	تصویربرداری از دیسک (ایمیج‌برداری)
Legal Liability of Intelligent Systems	مسئولیت حقوقی سامانه هوشمند
Supplementary Expert	کارشناس مکمل
Defensible Expert Report	گزارش کارشناسی قابل دفاع
Algorithmic Behavior Analysis	تحلیل رفتاری الگوریتم
Data Regulation	تنظیم‌گری داده
Digital Governance	حکمرانی دیجیتال
Admissibility Criteria	معیار استنادپذیری
Technology-Focused Court	دادگاه تخصصی فناورانه
Detailed Documentation	مستندسازی دقیق
Live Digital Analysis	بررسی دیجیتال برخط

فهرست منابع و مراجع کتاب

منابع فارسی

عنوان	نویسنده / سازمان	ناشر / محل انتشار	سال
قانون جرائم رایانه‌ای	مجلس شورای اسلامی	روزنامه رسمی جمهوری اسلامی ایران	۱۳۸۸
قانون تجارت الکترونیکی	مجلس شورای اسلامی	روزنامه رسمی جمهوری اسلامی ایران	۱۳۸۲
آیین دادرسی کیفری (با اصلاحات اخیر)	قوه قضائیه	انتشارات جنگل / دیدار / یا دوره‌های آموزشی قضات	متغیر
تحلیل حقوقی ادله دیجیتال در آیین دادرسی کیفری ایران	دکتر عباس حسینی‌نیک	مجله دانش حقوق جزا	۱۳۹۸
اصول کشف و تحلیل ادله دیجیتال	محمدرضا عسگری	مرکز آموزش قوه قضائیه	۱۳۹۹
کارشناسی جرائم رایانه‌ای	هادی شاملو	انتشارات جنگل	۱۳۹۶
مجموعه مقالات همایش ملی جرائم سایبری	دبیرخانه همایش	دانشگاه علوم قضایی	۱۳۹۵
امنیت اطلاعات و جرائم سایبری	دکتر علی رستمی	انتشارات مجد	۱۴۰۰
مقدمه‌ای بر رایانش ابری و تأثیر آن در ادله دیجیتال	پژمان شریفی	مجله علمی-پژوهشی دانشگاه تهران	۱۴۰۱
بلاک‌چین، قراردادهای هوشمند و مسئولیت حقوقی	دکتر مهدی عیوضی	فصلنامه حقوق فناوری	۱۴۰۰

منابع انگلیسی

عنوان	نویسنده / نهاد	ناشر / محل انتشار	سال
Guide to Integrating Forensic Techniques into Incident Response (SP 800-86)	*National Institute of Standards and Technology (NIST)*	*U.S. Department of Commerce*	۲۰۰۶
ISO/IEC 27037: Guidelines for identification, collection and preservation of digital evidence	*ISO/IEC JTC 1/SC 27*	*International Organization for Standardization*	۲۰۱۲
The Budapest Convention on Cybercrime	*Council of Europe*	*Treaty No. 185*	۲۰۰۱
Electronic Evidence	*Stephen Mason & Daniel Seng (Eds.)*	*Institute of Advanced Legal Studies, London*	*۵th Edition*, ۲۰۲۱
Digital Forensics with Open Source Tools	*Cory Altheide & Harlan Carvey*	*Syngress*	۲۰۱۱
Blockchain and the Law: The Rule of Code	*Primavera De Filippi & Aaron Wright*	*Harvard University Press*	۲۰۱۸
Artificial Intelligence and Legal Liability	*European Parliament Think Tank*	*Policy Report*	۲۰۲۰

The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms	*Larry A. DiMatteo et al.*	*Cambridge University Press*	۲۰۱۹
Understanding Digital Evidence	*Joanne Taylor & Eric Stover*	*Academic Press*	۲۰۱۹
Cybercrime and Digital Forensics	*Thomas J. Holt et al.*	*Routledge*	*۳rd Edition*, ۲۰۱۸

اسناد و گزارش‌های بین‌المللی و نهادی

عنوان گزارش	نهاد / سازمان	سال
General Data Protection Regulation (GDPR)	*European Union*	*Effective* ۲۰۱۶ (۲۰۱۸)
Artificial Intelligence Act (AI Act)	*European Commission*	۲۰۲۱–۲۰۲۴ (در حال تصویب نهایی)
UNODC Manual on Cybercrime Investigation	*United Nations Office on Drugs and Crime*	۲۰۱۳
Council of Europe – Guidelines on Electronic Evidence	*Council of Europe*	۲۰۲۰
ENFSI Guidelines for Forensic Digital Evidence Examination	*European Network of Forensic Science Institutes*	۲۰۱۵
OECD Recommendation on Digital Security Risk Management	*OECD*	۲۰۱۵

جدول تطبیقی مدل‌های تحلیل ادله دیجیتال

ویژگی / مدل تحلیل	مدل NIST SP ۸۰۰-۸۶	مدل ISO/IEC ۲۷۰۳۷	مدل DFRWS (2001)	مدل ENFSI (اروپا)	مدل Event-based (Carrier)
سازمان توسعه‌دهنده	NIST (آمریکا)	ISO / IEC	Digital Forensic Research	European Network of Forensic	Brian Carrier (محقق مستقل)
مراحل اصلی تحلیل	جمع‌آوری، بررسی، تحلیل، گزارش	شناسایی، جمع‌آوری، مستندسازی، نگهداری	شناسایی، حفظ، جمع‌آوری، تحلیل، ارائه	شناسایی، جمع‌آوری، تحلیل، گزارش	تحلیل مبتنی بر رویدادها
مناسب برای چه نوع داده‌هایی	سیستم‌های رایانه‌ای، شبکه، موبایل	همه انواع شواهد دیجیتال	داده‌های سیستم‌عامل و فایل	سیستم‌های عملیاتی و جنایی	رویدادمحور، لاگ، SIEM
تأکید ویژه روی	فرآیندهای استاندارد در ارگان‌های دولتی	زنجیره سلامت (Chain of Custody)	ساختار منطقی تحلیل	مستندسازی و رویه‌های قضایی	بازسازی دقیق رفتار دیجیتال
مخاطب اصلی	کارشناسان رسمی، نهادهای دولتی	آزمایشگاه‌های رسمی و قضایی	پژوهشگران، دانشگاهیان	پلیس جنایی، آزمایشگاه‌های اروپایی	کارشناسان در تحلیل پیچیده
مزایا	استانداردسازی عملیاتی، قابل استفاده در اسناد رسمی	تأکید بر زنجیره سلامت، هماهنگی با ISO 27000	ساختار ساده و پایه‌ای	تمرکز بر دقت مستندات و گزارش	تحلیل عمیق بر اساس وقایع
محدودیت‌ها	گاه بیش از حد رسمی و بروکراتیک	برای موارد خاص نیاز به تکمیل دارد	قدیمی و فاقد پوشش فناوری‌های نوین	تخصصی بودن برای سیستم‌های قضایی اروپا	نیاز به داده‌های با جزئیات بالا
قابلیت تطبیق با نظام ایران	بالا	بالا	متوسط	نسبتاً پایین	بالا (در پرونده‌های خاص)

مدل‌های تکمیلی

- ***NIST SP 800-86***: یکی از پراستفاده‌ترین مدل‌های تحلیلی در ایالات متحده، که در بسیاری از رویه‌های قضایی مبنا قرار می‌گیرد.
- ***ISO/IEC 27037***: مناسب برای تطبیق با استانداردهای بین‌المللی و کاربردی در سیاست‌گذاری ملی.
- ***DFRWS***: مدلی پایه‌ای که برای آموزش و پژوهش همچنان مرجع است.
- ***ENFSI***: تمرکز بالا بر مستندسازی و قابل دفاع بودن در دادگاه‌ها، به‌ویژه در اتحادیه اروپا.
- **مدل مبتنی بر رویداد**[۱۳]: برای تحلیل حرفه‌ای لاگ‌ها، ترافیک شبکه و بررسی رفتاری بسیار کاربردی است.

[۱۳] *Carrier*

راهنمای جامع ابزارهای استاندارد مورد استفاده در فرایند تحقیق و تفحص ادله الکترونیکی

نام ابزار	دسته بندی	شرکت عرضه‌کننده	سال عرضه	محیط و زیرساخت	شرح عملکرد	کاربرد
FTK Imager	تصویرگری و پیش‌نمایش دیسک	*AccessData*	۲۰۰۴	*Windows* / نصب محلی	تهیه ایمیج قانونی USB از دیسک و پیش نمایش داده	تهیه نسخه قانونی از داده‌ها
EnCase	تحلیل جامع ادل دیجیتال	*OpenText*	۱۹۹۸	Windows / نصب محلی	تحلیل حرفه‌ای انواع دیسک، موبایل، ایمیل و اینترنت هیستوری	تحلیل کامل داده‌های پیچیده
Cellebrite UFED	استخراج داده موبایل	*Cellebrite*	۲۰۰۷	Windows + سخت‌افزار UFED	استخراج داده حتی از دستگاه‌های قفل شده با سخت‌افزار اختصاصی	استخراج داده‌های موبایل و پیام‌ها
X-Ways Forensics	تحلیل دیسک و فایل سیستم	*X-Ways*	۲۰۰۴	*Windows*	سبک و سریع برای تحلیل فایل سیستم‌ها و بازیابی داده	تحلیل دیسک در پرونده‌های قضایی
Magnet AXIOM	تحلیل جامع داده‌های دیجیتال	*Magnet Forensics*	۲۰۱۶	*Windows*	تحلیل داده‌های موبایل، رایانه، و کلود در یک محیط گرافیکی	تحلیل شواهد چند منبعی
Belkasoft Evidence Center	تحلیل داده‌های حافظه‌ی موبایل	*Belkasoft*	۲۰۱۰	*Windows*	تحلیل *RAM* ایمیل، پیام‌رسان و دیسک	تحلیل جامع ارتباطات دیجیتال
Oxygen Forensic Detective	استخراج داده‌های موبایل	*Oxygen Forensics*	۲۰۰۰	*Windows*	استخراج و تحلیل داده از موبایل، اپلیکیشن و کلود	تحلیل موبایل و داده‌های ابری
Passware Kit Forensic	رمزگشایی و بازیابی رمز	*Passware Inc.*	۲۰۰۷	*Windows*	شکستن رمز فایل‌ها، دیسک و *BitLocker* اسناد آفیس	رمزگشایی اسنادرمزدار
Elcomsoft Forensic	رمزگشایی و استخراج داده	*Elcomsoft*	۱۹۹۷	*Windows*	استخراج رمز عبور، داده‌های *iCloud* و بکاپ‌های *iOS*	بازیابی رمز و داده‌های موبایل
AccessData Forensic Toolkit (FTK)	تحلیل جامع ادله	*AccessData*	۱۹۹۷	*Windows*	تحلیل ایمیج‌ها، بازیابی فایل‌های حذف شده، جستجوی پیشرفته	تحلیل ادله در پرونده‌های قضایی
BlackLight	تحلیل *macOS* و *iOS*	*BlackBag Technologies*	۲۰۰۸	*macOS, Windows*	تحلیل دیسک‌های مک و بکاپ‌های *iOS*	تحلیل شواهد سیستم‌های *Apple*
ProDiscover Forensics	تخلیل دیسک و شبکه	*Technology Pathways*	۲۰۰۲	*Windows*	تحلیل دیسک و شبکه، جستجوی فایل‌ها، ساخت گزارش	تحلیل دیسک و ترافیک شبکه
Helix3	لایو فورنزیک و تحلیل	*e-Fense*	۲۰۰۴	*Linux Live CD*	لایو سی‌دی برای جمع‌آوری داده بدون دستگاری سیستم	لایو فورنزیک در صحنه جرم
Paraben E3	تحلیل موبایل و ایمیل	*Paraben Corporation*	۲۰۰۱	*Windows*	تحلیل دیوایس‌های موبایل، ایمیل‌ها و حافظه رم	تحلیل پیام‌رسان‌ها و ایمیل‌ها
Nuix Workstation	تحلیل داده‌های بزرگ	*Nuix*	۲۰۰۵	*Windows*	تحلیل مقیاس بزرگ داده‌های ایمیل، دیسک و اینترنت	تحلیل داده‌های گسترده
AD Enterprise	تحلیل شبکه و سازمانی	*AccessData*	۲۰۱۰	*Windows*	تحلیل زنده شبکه، جمع‌آوری شواهد از چند سیستم	تحلیل فورنزیک در سطح شبکه
F-Response	دسترسی زنده به دیسک	*F-Response*	۲۰۰۸	*Windows*	دسترسی زنده به دیسک‌ها و حافظه سیستم‌های راه دور	جمع‌آوری زنده داده

Paladin Forensic Suite	مجموعه ابزار *Live CD*	*SUMURI*	۲۰۰۹	*Linux Live*	*Live CD* یا ابزار فورنزیک متن باز برای بازیابی داده	تحلیل و بازیابی داده در محل
SafeBack	تصویرگری قانونی دیسک	*New Technologies Inc.*	۱۹۹۹	*DOS/Windows*	یکی از اولین ابزارهای ایمیج-گیری قانونی دیسک	تصویرگری قانونی برای شواهد

راهنمای جامع ابزارهای رایگان و متن باز مورد استفاده در فرآیند تحقیق و تفحص ادله الکترونیکی

نام ابزار	دسته بندی	شرکت عرضه‌کننده	سال عرضه	محیط و زیرساخت	شرح عملکرد	کاربرد
Autopsy	تحلیل دیسک	*Basis Technology*	۲۰۰۰	*Cross-platform* / متن‌باز	رابط گرافیکی *Sleuth Kit* جهت تحلیل فایل سیستم برای متادیتا و گزارش-گیری	تحلیل دیسک و بازیابی داده
Sleuth Kit	کتابخانه تحلیل فایل سیستم	*Brian Carrier*	۲۰۰۰	*Cross-platform* / متن‌باز	کتابخانه قدرتمند برای تحلیل ساختار سیستم در خط فرمان	تحلیل فایل سیستم
Volatility	تحلیل حافظه *RAM*	*Volatility Foundation*	۲۰۰۷	*Cross-platform / Python-based*	چارچوب تحلیل حافظه *Dump* شناسایی فرآیندها و رفتار بدافزار	تحلیل حافظه در رخدادهای امنیتی
Rekall	تحلیل حافظه *RAM*	*Google Security*	۲۰۱۴	*Cross-platform / Python-based*	تحلیل پیشرفته حافظه *Dump* افزونه‌های تعاملی	تحلیل دقیق حلفظه
Wireshark	تحلیل شبکه	*Wireshark Foundation*	۱۹۹۸	*Cross-platform* / متن‌باز	تحلیل ترافیک شبکه به‌صورت زنده، ضبط بسته‌ها و بازپخش	تحلیل تراقفیک و کشف نفوذ
Plaso (log2timeline)	تایم‌لاین سیستم	*Google Inc.*	۲۰۱۲	*Cross-platform / Python-based*	تبدیل لاگ‌ها به تایم‌لاین وقایع سیستم	بازسازی رویدادها
Caine	سیستم عامل فورنزیک	*Nanni Bassetti*	۲۰۰۹	*Linux Live*	توزیع لینوکس با ابزارهای فورنزیک متن‌باز	تحلیل صحنه جرم
DEFT Linux	سیستم عامل فورنزیک	*DEFT Labs*	۲۰۰۵	*Linux Live*	توزیع زنده لینوکس با لبزارهای تحلیل دیسک و شبکه	تحلیل داده به-صورت زنده

پروتکل‌های مورد استفاده در فرآیند تحقیق و تفحص ادله الکترونیکی

نام پروتکل	سال	کشور/مجمع	شرح مختصر	کاربرد در ادله و جرائم فضای مجازی
DFRWS	۲۰۰۱	انجمن *DFRWS*	نشست پژوهشگران و کارشناسان فورنزیک دیجیتال ادله دیجیتال را پایه‌گذاری کرد. این نشست مبنای علمی برای بسیاری از مدل‌های تحلیل دیجیتال است.	در طراحی مدل‌های فرآیند تحلیلدیجیتال و ایجاد رویه‌های عملیاتی استخراج و تحلیل داده‌های دیجیتال در جرائم سایبری
NIST SP 800-86	۲۰۰۶	موسسه ملی استاندارد و فناوری آمریکا	راهنمای ادغام تکنیک‌های فورنزیک در فرآیند پاسخ به رخدادهای امنیتی؛ چارچوبی برای استفاده منظم از ابزارهای تحلیل دیجیتال و حفاظت از زنجیره سلامت داده‌ها	در تحلیل رخدادهای امنیتی، ثبت شواهد دیجیتال، و تولید گزارش‌های کارشناسی معتبر در دعاوی مرتبط
ACPO	۲۰۰۳	انجمن روسای پلیس انگلستان	دستورالعمل ملی برای حفظ سلامت اصالت و زنجیره نگهداری شواهد دیجیتال؛ به عنوان راهنمای عملی برای ماموران پلیس و کارشناسان فورنزیک	در تضمین اصالت شواهد دیجیتال، مستندسازی مراحل جمع‌آوری و ارائه مدارک دادگاه‌ها
ISO/IEC 27037	۲۰۱۲	سازمان بین‌المللی استانداردسازی	استاندارد بین‌المللی برای شناسایی، جمع‌آوری، کسب و نگهداری شواهد دیجیتال؛ راهنمایی جامع برای حفظ زنجیره سلامت و رعایت اصول فورنزیک	در جمع‌آوری و مستندسازی ادله دیجیتال به‌ویژه در پرونده‌های چندجانبه و بین‌المللی
SWGDE	۱۹۹۸	گروه کاری علمی ادله دیجیتال	مجموعه دستورالعمل‌ها و بهترین شیوه‌ها برای تحلیل، ضبط و ارائه شواهد دیجیتال؛ به‌روزرسانی مداوم با توجه به تغییرات فناوری	در تدوین گزارش‌های کارشناسی استاندارد و انتخاب ابزارها و روش‌های تحلیل ادله دیجیتال
Budapest Convention	۲۰۰۱	شورای اروپا	نخستین معاهده بین‌المللی علیه جرائم سایبری؛ تعیین استانداردهای همکاری قضایی و تبادل اطلاعات بین کشورها	در پرونده‌های بین‌المللی مربوط به جرائم سایبری و ارائه ادله الکترونیکی در محاکم فراملی
EDRM	۲۰۰۵	انجمن *EDRM*	چارچوب مرجع برای مدیریت چرخه حیات داده‌های الکترونیکی؛ از شناسایی تا نگهداری و ارائه در دادرسی	در سازماندهی فرآیند کشف و ارائه ادله الکترونیکی در دعاوی تجاری و فناورانه
NIST SP 800-101	۲۰۰۷	موسسه ملی استاندارد و فناوری آمریکا	راهنمای تخصصی برای تحلیل و فورنزیک دستگاه‌های موبایل؛ روش‌های بازیابی داده و مستندسازی شواهد موبایل	در تحلیل شواهد مجود در تلفن‌های همراه و تجهیزات قابل حمل در جرائم فضای مجازی

Digital Forensics & Cyber Crime Investigation in Official Expertise

(A practical guide with case studies together new technologies approaches)

چکیده

کتاب **"ادله الکترونیکی و تحلیل جرائم فضای مجازی کارشناسی رسمی دادگستری»** به عنوان یک راهنمای جامع و کاربردی، به تبیین مبانی نظری، استانداردهای فنی، چارچوب‌های قانونی و رویه‌های تخصصی در کشف، تحلیل، ارزیابی و استناد به ادله دیجیتال در فضای فناوری‌های نوین می‌پردازد.

کتاب **"ادله الکترونیکی و تحلیل جرائم فضای مجازی کارشناسی رسمی دادگستری»** با تمرکز بر نقش محوری کارشناسان رسمی دادگستری در مواجهه با جرائم رایانه‌ای و اختلافات فناورانه، به بررسی دقیق فرآیندهای کارشناسی در پرونده‌های دیجیتال‌محور می‌پردازد و الزامات حقوقی، فنی و عملیاتی را در سطوح ملی و بین‌المللی تحلیل می‌کند.

در این کتاب، ضمن معرفی انواع ادله الکترونیکی، جایگاه آن‌ها در نظام دادرسی، چالش‌های حقوقی و فنی تحلیل داده‌های دیجیتال، و شیوه‌های مستندسازی ادله، به موضوعات تخصصی مانند جرائم فضای مجازی، تهدیدات هوش مصنوعی و رباتیک، اختلافات مالکیت فکری، و الزامات جمع‌آوری داده‌های ابری و رمزنگاری‌شده پرداخته شده است.

همچنین روش‌های پیشرفته تحلیل ادله در سامانه‌های صنعتی و فناوری‌های نوین (از جمله *ROS* ، *SCADA*، *SDN* و *G5*)، اصول استناد به بلاک‌چین در اثبات دیجیتال و ملاحظات اخلاقی در کارشناسی هوش مصنوعی به‌طور تحلیلی بررسی شده‌اند.

کتاب **"ادله الکترونیکی و تحلیل جرائم فضای مجازی کارشناسی رسمی دادگستری»** در کنار استفاده از بهترین تجربیات و آموخته‌های علم داده و هوش مصنوعی به عنوان ابزاری در کارشناسی رسمی دادگستری، با ارائه چک‌لیست‌های کاربردی، ساختارهای استاندارد گزارش کارشناسی، نمونه‌های عملی، تحلیل پرونده‌های سایبری و شرح مقررات ایران و استانداردهای جهانی، ابزار مؤثری برای ارتقاء دقت، صحت و استنادپذیری گزارش‌های کارشناسی رسمی در حوزه فناوری اطلاعات فراهم می‌آورد.

این اثر به عنوان یک منبع ضروری، پاسخگوی نیازهای کارشناسان رسمی دادگستری، وکلای فناوری، مدیران دعاوی فناورانه و پژوهشگران حوزه حقوق دیجیتال خواهد بود.

آشنایی با نویسنده کتاب

مهرداد تاج‌بخش متولد ۱۳۴۷ کارشناس رسمی دادگستری در رشته رایانه و فناوری اطلاعات؛ (عضو کانون کارشناسان رسمی دادگستری استان تهران) دارای کلیه صلاحیت‌های مصوب این رشته؛ ازجمله صلاحیت جرائم رایانه‌ای و فضای مجازی که از سال ۱۳۸۲ تا کنون بصورت مستمر به این امر اشتغال دارد.

مهرداد تاج‌بخش دانش‌آموخته‌ی مهندسی کامپیوتر در گرایش سخت افزار از دانشکده فنی دانشگاه تهران؛ کارشناسی ارشد در رشته مدیریت فناوری اطلاعات گرایش مدیریت دانش از دانشکده مدیریت و حسابداری دانشگاه شهید بهشتی تهران؛ کارشناسی ارشد در رشته مهندسی فناوری اطلاعات در گرایش امنیت اطلاعات از دانشکده مهندسی برق، الکترونیک و کامپیوتر دانشگاه تربیت مدرس تهران و دکتری مدیریت حرفه‌ای کسب وکار از دانشکده مدیریت و اقتصاد دانشگاه تربیت مدرس تهران می‌باشد. درحال حاضر برروی پروژه‌ی تحقیقاتی در مقطع دکتری در دانشگاه اتاگو نیوزیلند در موضوع بلاک‌چین و حقوق مالکیت فکری و معنوی و رسیدن به چارچوب زنجیره‌ی ارزش در این موضوع، مشغول به تحصیل و تحقیق می‌باشد.

مهرداد تاج‌بخش دارای بیش از ۳۵ سال سابقه فعالیت در حوزه‌ی رایانه و فناوری اطلاعات و بیش از ۲۲ سال سابقه کارشناسی بوده و تجربیات متعددی در بررسی و ارائه نظریه کارشناسی در خصوص پرونده‌های با موضوع جرائم رایانه‌ای و فضای مجازی در مراجع قضایی داشته است.

فعالیت‌های **مهرداد تاج‌بخش** مرتبط با کارشناسی رسمی دادگستری بشرح زیر می‌باشند:

- مسئول کمیسیون علمی و تخصصی ارزش‌گذاری دارایی‌های نامشهود و هوش مصنوعی شورای عالی کارشناسان رسمی دادگستری
- مشاور، مسئول و هماهنگ کننده امور رایانه و فناوری اطلاعات شورای عالی کارشناسان رسمی دادگستری
- عضو کمیسیون علمی و تخصصی رشته رایانه و فناوری اطلاعات شورای عالی کارشناسان رسمی دادگستری
- مدرس و ارائه‌کننده دوره‌های آموزشی و وبینارهای تخصصی در موضوعات کارشناسی رسمی دادگستری
- نوآور، کارآفرین و مالک تارنمای ***"کارشناس برتر highexpert.ir"***
  - عرضه کتب، موردکاوی‌ها و منابع الکترونیکی تخصصی و کاربردی در کارشناسی رسمی دادگستری
  - علم داده و هوش مصنوعی در کارشناسی رسمی دادگستری

شماره شابک: ۹۷۸-۹۶۴-۲۸۸۹-۰۲-۰

کارشناس برتر High Expert

موسسه فرهنگی و انتشاراتی اردلان