باسمه تعالی

طرح درس جهت ارائه در نیمسال تحصیلی اول ۱۴۰۳-۱۴۰۲

دانشکده	**مهندسی برق و کامپیوتر**	**گروه**	**معماری سیستم‌های کامپیوتری**
رشته	**جرم‌یابی دیجیتال**	**مقطع**	**کارشناسی ارشد**
نام درس	**اصول جرم‌یابی دیجیتال**	**نوع درس**	**پایه** ☑ **نظری** ☐ **تخصصی** ☐ **عملی** ☐ **اختیاری** ☐ **نظری-عملی** ☑
تعداد واحد	**۳**	**نام اساتید**	**حسین همائی و صادق درّی نوگورانی**
دروس پیش‌نیاز	**ندارد**	**تلفن دفترکار**	**۳۹۰۵ و ۵۰۹۸**
دروس هم‌نیاز	**ندارد**	**پست الکترونیک**	homaei@modares.ac.ir dorri@modares.ac.ir

✓ **اهداف درس:**

۱. آشنایی با فرایندهای پی‌جویی دیجیتال
۲. آشنایی با ابزارها و تجهیزات جرم‌یابی دیجیتال
۳. آشنایی با نحوه جمع‌آوری داده‌های فرّار و ماندگار به منظور جرم‌یابی دیجیتال
۴. تحلیل شواهد دیجیتال بر روی حافظه‌های دائم و موقت
۵. آشنایی با انواع سیستم‌فایل‌ها
۶. آشنایی با نحوه مقابله با روش‌های ضد جرم‌یابی دیجیتال

✓ **رئوس مطالب و برنامه ارائه در کلاس:** (در صورتی که واحد عملی یا نظری-عملی بود، نوع آموزش در توضیحات بیان شود)

شماره هفته	موضوع جلسه درس	توضیحات
جلسات هفته اول	مقدمات	معرفی درس، تعاریف اولیه، معرفی دوره‌های مشابه و فرصت‌های شغلی، وظایف متخصصین جرم‌یابی دیجیتال
جلسات هفته دوم	پی‌جویی دیجیتال	انواع پی‌جویی دیجیتال، فرایند پی‌جویی دیجیتال
جلسات هفته سوم	آزمایشگاه جرم‌یابی دیجیتال	طرح آزمایشگاه، ویژگی‌های ایستگاه‌های کاری، نیازمندی‌های سخت‌افزاری و نرم‌افزاری، وظایف افراد آزمایشگاه، کارکرد ابزارها
جلسات هفته چهارم	اصول کار با داده‌های رقمی	سازمان‌دهی داده‌ها، فرایند بوت، ساختار دیسک
جلسات هفته پنجم	مقدمات رمزنگاری	روش‌های رمز کردن و رمزگشایی، امضای رقمی، مدیریت کلید، توابع درهم‌ساز
جلسات هفته ششم	جمع‌اوری داده‌ها	فرمت‌های ذخیره‌سازی شواهد دیجیتال، روش‌های جمع‌آوری داده‌ها، اعتبارسنجی داده‌های جمع‌آوری شده، معرفی ابزارها
جلسات هفته هفتم	تحلیل شواهد	جستجوی داده‌ها و فایل‌ها، بررسی فایل‌های گرافیکی، استخراج و بازیابی داده‌ها، داده‌های مخفی، بازیابی گذرواژه، نهان‌نگاری
جلسات هفته هشتم	جلسه اول: اصول سیستم‌فایل جلسه دوم: سیستم‌فایل FAT	مفاهیم اولیه، نحوه استفاده فایل‌ها از فضای فیزیکی دیسک، پارتیشن‌ها، انواع داده‌های سیستم‌فایل، اجزاء و جزئیات سیستم‌فایل FAT
جلسات هفته نهم	سیستم‌فایل NTFS	معرفی، ساختار رکوردها، آشنایی با خصیصه‌ها، شماره‌گذاری کلاسترها، جزئیات تفسیر داده‌ها

جلسه دهم	رمز کردن داده در سیستم‌فایل	روش رمزنگاری و رمزگشایی فایل‌ها و پوشه‌ها، رمز کردن همه دیسک، روش‌های ذخیره‌سازی کلید
جلسات هفته یازدهم	سیستم‌فایل Ext4 لینوکس	معرفی، اجزاء، Inodeها، لینک‌های سخت و نرم
جلسات هفته دوازدهم	تحلیل وقایع ثبت شده	استفاده از ابزارهای لینوکسی برای تحلیل لاگ، لاگ‌های وب، رخدادهای ویندوز
جلسات هفته سیزدهم	جرم‌یابی زنده	اهمیت و اصول جرم‌یابی زنده، جمع‌آوری داده‌ها از حافظه موقت، اولویت‌بندی، بررسی کار با ابزار Volatility در یک مثال عملی
جلسات هفته چهاردهم	جلسه اول: جرم‌یابی زنده (ادامه) جلسه دوم: پاک‌سازی رسانه	جرم‌یابی ماشین مجازی و استفاده از ماشین مجازی برای جرم‌یابی، بررسی یک مثال عملی از آسیب‌پذیری ابزارهای جرم‌یابی دیجیتال روش‌های امن پاک‌سازی رسانه
جلسات هفته پانزدهم	مقابله با ضد جرم‌یابی	روش‌های جلوگیری از جرم‌یابی توسط مهاجمین و راه‌های مقابله با آن
جلسات هفته شانزدهم	جرم‌یابی ایمیل	معماری و پروتکل‌های ایمیل، امنیت ایمیل، بررسی سرآیندهای ایمیل، آزمایش سرورهای ایمیل، معرفی ابزارهای عملی

✓ **روش ارزشیابی:**

سمینار (۲ نمره)، تمرین‌ها و پروژه‌ها (۴ نمره)، امتحانات (۱۴ نمره)

✓ **منابع :**

[1] B. Nelson, A. Phillips, and C. Steuart. *Guide to computer forensics and investigations*. 6th edition, Cengage Learning, 2019.
[2] B. Carrier. *File system forensic analysis*. Addison-Wesley Professional, 2005.
[3] S. Ostrovskaya, and O. Skulkin. *Practical Memory Forensics: Jumpstart effective forensic analysis of volatile memory*. Packt Publishing, 2022.
[4] M. K. Robinson. *Digital Forensics Workbook: Hands-on Activities in Digital Forensics*. CreateSpace Independent Publishing Platform, 2015.
[5] N. Moustafa. *Digital Forensics in the Era of Artificial Intelligence.* CRC Press, 2022.
[6] R. Lee, Windows Forensic Analysis Course, SANS Institute, 2017.
[7] John Tai, Computer Forensic Investigator Course, Feb. 2022