



**Namatek**  
True Education

# Forensics

[www.namatek.com](http://www.namatek.com)

فارنزیك چيست؟

## فهرست مطالب

۱. فارنژیک چیست؟
۲. انواع فارنژیک
۳. اهمیت جرم شناسی سایبری
۴. کاربرد فارنژیک چیست؟

اگر شما هم تا به حال طعمه حملات سایبری بوده باشید و یا با افرادی که این حادثه را متحمل شده اند در ارتباط بوده باشید برایتان سوال پیش آمده که فارنزیک چیست و به چه معناست؟ اغلب ما با شنیدن واژه جرم شناسی (Forensics)، صحنه هایی از فیلم های جنایی را به یاد می آوریم؛ اما باید بدانید که فارنزیک در دنیای کامپیوتر نقش مهمی بر عهده دارد.

در ادامه با ما همراه باشید تا شما را به طور کامل با جرم شناسی سایبری آشنا نماییم.

## #۱ فارنزیک چیست؟



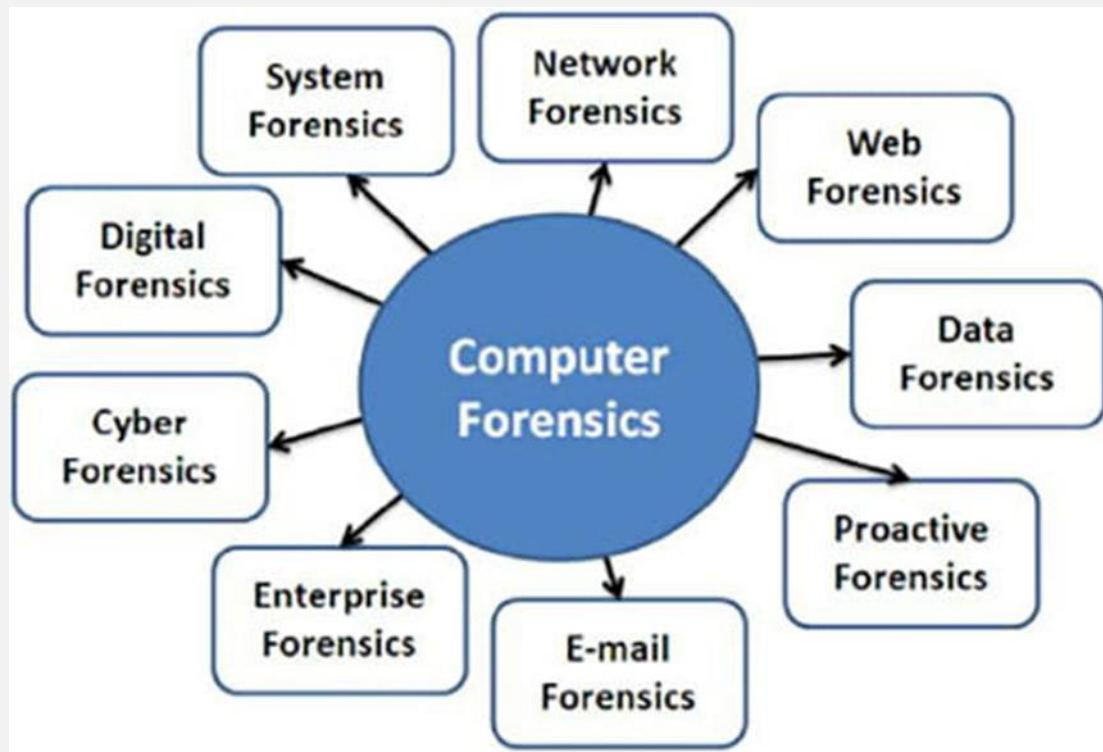
فارنزیک (Forensics) در لغت به معنای پزشکی قانونی است؛ اما مفهوم آن به جرم شناسی اشاره دارد. در این رشته، افراد به جمع آوری و تجزیه و تحلیل شواهد می پردازند. در حوزه علوم رایانه ای نیز در پاسخ به پرسش

فارنژیک چیست، می توان همین جمله را بیان کرد. در حقیقت در جرم شناسی سایبری گرد هم آوری و آنالیز اطلاعات، با بررسی سیستم های دیجیتال صورت می گیرد که برخی از آن ها عبارتند از:

- سیستم های رایانه ای (computer systems)
- شبکه ها (networks)
- ارتباطات بی سیم (wireless communications)
- دستگاه ذخیره داده (storage device)

## #۲ انواع فارنژیک

انواعی از فارنژیک رایانه وجود دارند که هر کدام به بررسی جنبه خاصی از فناوری اطلاعات می پردازند.



منظور از برخی از شاخه های اصلی فارنزیک چیست؟

- فارنزیک پایگاه داده (Database forensics): در این شاخه به بررسی اطلاعات موجود در پایگاه اطلاعات و فراداده ها (metadata) می پردازند.
- فارنزیک ایمیل (Email forensics): در این نوع جرم شناسی دیجیتال به بازیابی و تجزیه و تحلیل ایمیل ها پرداخته خواهد شد.
- فارنزیک بدافزار (Malware forensics): در این شاخه از فارنزیک، واریسی کدها برای شناسایی بدافزارها و آنالیز آن ها صورت می گیرد.
- فارنزیک حافظه (Memory forensics): در این حوزه، جمع آوری اطلاعات ذخیره شده در حافظه پنهان کامپیوتر یا رم (RAM) به انجام خواهد رسید.



- فارنزیک موبایل (Mobile forensics): در این نوع از جرم شناسی سایبری، متخصصان به بررسی تلفن همراه می پردازند تا بتوانند در جهت بازیابی و آنالیز اطلاعات این دستگاه ها موثر واقع شوند. این داده ها می توانند در رابطه با مخاطبین، پیام های متنی ورودی و خروجی، تصاویر و ویدیوها باشند.
- فارنزیک شبکه (Network forensics): در این شاخه با مشاهده ترافیک شبکه و استفاده از ابزارهای فارنزیک به کشف شواهد مربوط به جرایم سایبری پرداخته می شود.

## #۳ اهمیت جرم شناسی سایبری

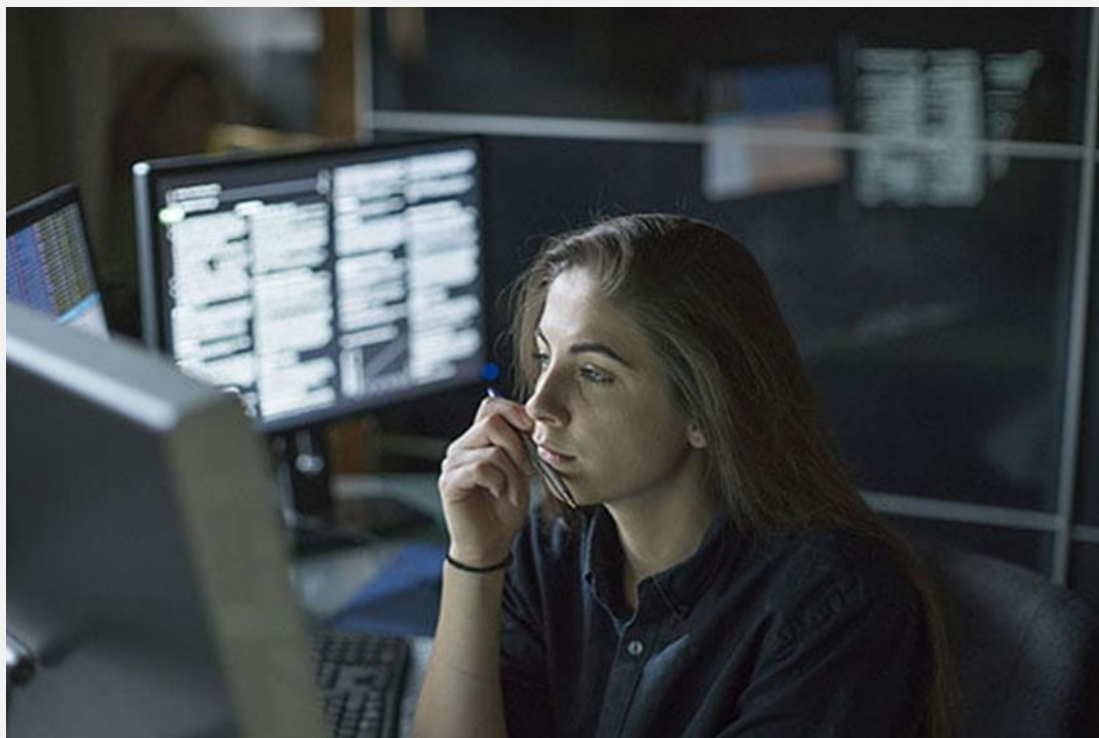
در ادامه پاسخ به فارنزیک چیست، لازم می دانیم به بیان اهمیت آن در جهان امروزی پردازیم. فضای مجازی می تواند تا حد زیادی حریم شخصی ما را تهدید کند؛ زیرا تمام کاربران آن، مطیع قوانین نیستند.



از آن جایی که جمع آوری اطلاعات در این فضا نسبت به کنار هم قرار دادن شواهد فیزیکی در دنیای واقعی تفاوت هایی دارد، پس باید شاخه تخصصی که همان فارنزیک سایبری است توسعه یابد. در ضمن با تجزیه و تحلیل شواهد مربوط به جرایم سایبری، متخصصان جرم شناسی دیجیتال می توانند به امنیت سایبری و افراد متخصص فناوری اطلاعات کمک کنند تا با ابزارهای دفاعی مناسب از سیستم ها و داده ها به خوبی محافظت نمایند. علاوه بر تمام موارد گفته شده، شواهد دیجیتال می توانند در دادگاه کیفری ارائه و در اثبات جرم موثر واقع شوند.

## #۴ کاربرد فارنزیک چیست؟

اکنون که تا حدودی با این که فارنزیک چیست و اهمیت آن آشنا شدید، قصد داریم به بررسی کاربرد آن بپردازیم.



برخی از مهم ترین کاربردهای جرم شناسی دیجیتال عبارتند از:

۱. کشف داده ها

متخصصان جرم شناسی رایانه به مجریان قانون کمک می کنند تا داده های مهم دستگاه های توقیف شده مانند لپ تاپ یا تلفن های همراه را کشف کنند.





## ۲. جبران خسارت

فازنریک سایبری شدت و میزان آسیب، نقض قوانین و حملات شبکه را تجزیه و تحلیل و سپس مشخص می کند. با دستیابی به دیدگاه درستی از آنچه اتفاق افتاده سازمان ها می توانند به جای کنار گذاشتن تمامی سیستم ها و اطلاعاتی که وجود دارد، از داده های سالم استفاده نمایند.



### ۳. ردیابی هکرها

شرکت های خصوصی که در زمینه جرم شناسی رایانه ای فعالیت دارند، خدمات مختلفی را در راه کمک به دیگر مشاغل ارائه می دهند که عبارتند از:

- ردیابی هکرها
- کشف منابع حملات سایبری
- شناسایی طرف مقصر



### ۴. امنیت شبکه

متخصصان فارنزیک دیجیتال در تقویت امنیت شبکه و حفاظت از سرورهای خصوصی نیز نقش مهمی ایفا می کنند تا از حملات هکرها



جلوگیری نمایند. ابزارهای مربوط به جرم شناسی رایانه ای، امور گوناگونی را در راستای کمک به موسسات مختلف به انجام می رسانند که به ترتیب عبارتند از:

- بازرسی داده ها
- تشخیص فعالیت های مشکوک
- شناسایی هکرها و کشف روش های آن ها
- طراحی بهترین دفاع در برابر حملات سایبری



سخن پایانی

همان طور که با دستیابی به پاسخ پرسش فارنزیک چیست دریافتید، جرم شناسی دیجیتال در جهان مدرن وظیفه حفاظت از حریم خصوصی افراد و اطلاعات شخصی آن ها را بر عهده دارد تا از حملات مجرمان سایبری در امان بمانند و یا بتوانند عامل این جرم ها را ردیابی کنند. امیدواریم

توانسته باشیم با ارائه این مطلب به تمامی سوالات شما در رابطه با  
فارنژیک پاسخ دهیم.