بررسی مدل های جرم شناسی رایانه ای برای رهگیری نفوذگر

محمدعلی مسلمی[1]، mo.a.moslemi@gmail.com
جواد وحیدی[2]، دانشگاه علم و صنعت ، jvahidi@iust.ac.ir

چکیده

فناوری و اینترنت بطور روزمره در حال رشد فزاینده ای می باشد به همین سبب جرائم رایانه ای مطابق با پیشرفت تکنولوژی با متد ها و روش های متفاوت در حال افزایش می باشد . متخصصان رایانه ای در علم فارنزیک با جمع اوری داده ای موجود در سطح سیستم و با آنالیز دقیق داده ها در رهگیری نفوذگر و ارائه گزارش به مراجع بالاتر نقش بسزایی را انجام می دهند.

کلمات کلیدی

computer forensic ؛ فارنزیک ؛ جرم شناسی کامپیوتری ؛ جرم شناسی دیجیتال ؛ آنالیز داده ها

۱. مقدمه

در دنیای مدرن استفاده از فناوری اطلاعات و پدیدارشدن تکنولوژی های پیشرفته در زندگی روزمره به امری اجتناب ناپذیری تبدیل شده است .بهره گیری از این فناوری ها تحولات متعددی در بشر ایجاد شده است این تحولات سبب شده در لابلای پیشرفت فناوری ها و تکنولوژی های به روز شده جرم و جنایت به روش های متعددی اتفاق بیافتد.از این رو تشخیص اینکه جرم و جنایت توسط چه فردی یا گروه ویا سازمانی وبواسطه چه دولتهایی و با چه ابزاری رخ داده است بسیار مشکل و قابل اهمیت می باشد.بنابراین نیازمند علمی در کامپیوتر برای جمع آوری شواهد و مستندات از سیستم قربانی هستیم که آن علم computer forensic نامیده می شود .جرایم کامپیوتری شاخه ای از علم جرم شناسی دیجیتال می باشد. این علم به جمع اوری شواهد در رایانه و رسانه های ذخیره سازی دیجیتال می باشد.این مقاله در مورد جرم شناسی کامپیوتر بحث خواهد کرد.

۲. تعریف فارنزیک

کلمه forensic در فرهنگ واژگان انگلیسی به فارسی بمعنای دادگاهی و مناظره ای ، در علوم مختلف از جمله رشته های پزشکی بمعنای پزشکی قانونی و در علم کامپیوتر جرم شناسی رایانه ای و در سایر علوم به جمع آوری و بررسی شواهد معنا شده است .

فارنزیک کامپیوتری به مجموعه ای از روش ها و تکنیک هایی برای کشف وجمع آوری شواهد لازم و کافی از تجهیزات کامپیوتری ، شبکه ای ،موبایل و....جهت حفظ داده و پردازش بر روی آن و در نهایت تهیه گزارش نهایی برای مراجع بالاتر می باشد.

۳. طرح سوال در فارنزیک

در علم جرم شناسی رایانه ای (فارنزیک) سوالات بسیاری در این زمینه مطرح شده است این سوالات شامل مواردی
اگر مورد نفوذ قرار بگیرید چه فرآیندی اعمال نمایید ؟
در صورت سرقت اطلاعات به دست نفوذگر آیا می توانیم ردپای از نفوذگران اینترنتی و سیستمی بدست آورید یا خیر؟
چگونه تنظیمات سیاست پیشگیرانه ای دربرابر نفوذگران اعمال می کنید؟
با مطالعه این مقاله و کتاب هایی که در زمینه computer forensic به چاپ رسیده و جستجو در اینترنت می توانید به سوالات مذکور پاسخ دهید

۴. هدف جرم شناسی دیجیتال

هدف اصلی این علم شناسایی ، حفظ ،تجریه و تحلیل از داده های دیجیتالی و رسانه های ذخیره سازی و ارائه مستندات و شواهد به مراجع بالاتر جهت رسیدگی می باشد.

با تنظیم سیاست های پیشگیرانه و اصولی و استفاده از ابزارها و نرم افزارهای در صورت نفوذ ،رهگیری نمایید.

۵. چالش های تحقیق

تحولات مداوم در فن آوری اطلاعات و ارتباطات برای فارنزیک چالش هایی ایجاد کرده است.
جرایم اینترنتی با توجه به کاربرد رایانه مورد استفاده وتحقیق در مورد جرم کامپیوتری منجر به توسعه این زمینه جدید به نام جرم شناسی کامپیوتر است.
چالش های عمده در جرایم سایبری شامل [1]:

- فقدان منابع داده های واقعی برای مطالعه و تجزیه و تحلیل اهداف
- وابستگی به کارآمدی و به آسانی در دسترس قرارگرفتن ابزار برای گرفتن و تجزیه و تحلیل داده ها
- محدودیت محیط پیرامون در طول کسب اطلاعات
- شواهد گوناگون
- دسترسی به داده ها - به ویژه اگر داده ها در سیستم های توزیع شده است
- حجم داده ها و زمان انجام گرفته یک تحقیق
- فقدان نهایی و تفاوت قوانین در سراسرکشورها
- تعداد بسیاری از پلت فرم سیستم عامل و سیستم فایل.

۶. انواع فارنزیک

فانزیک به دو سطح تقسیم می شود این دو سطح شامل :

- سطح پایین : شبکه های کوچک شرکت – سایت شخصی – سیستم شخصی (موبایل ،سیستم ،لب تاپ و....)
- سطح بالا: سطح ملی – وزارتخانه ها – سازمان های دولتی – نهادها و ارگانها

در سطوح پایین پس از نفوذ نفوذگر به سیستم قربانی به جمع آوری واستخراج داده از تجهیزات کامپیوتری وتهیه گزارش به مراجع قانونی و قضایی نمی پردازیم مگر در صورتی که سبب ضررو زیان بالایی به فرد وارد آید.

بطور مثال خالی شده حساب بانکی توسط نفوذگر به سایت شخصی افراد – سرقت رفتن اطلاعات افراد ازجمله عکس ، فیلم و ... از سیتم شخصی افراد

در سطح بالا با آگاه شدن دولت از وجود تروجان ها ، ویروسها و مواردی از این قبیل اقدام به مقابله با آن می کند . بطور مثال ویروس اکستاکس نت

در سطوح بالا به دو مفهوم بسیار مهم می پردازیم :

۱- Incident response

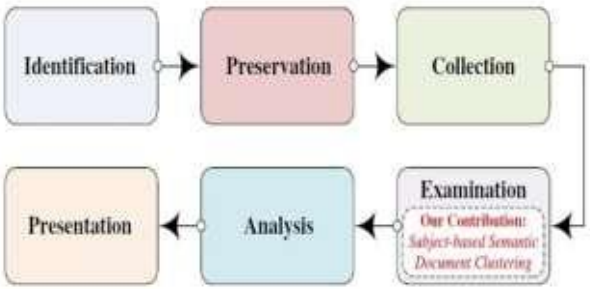
۲- First response

Incident response: مرکز پاسخگویی به رخ داد های امنیتی واردشده رایانه ای

First response: تیم یا فردی که برای اولین بار به محل وقوع حادثه و جرم حضور یافته و به بررسی عوامل رخ داده می پردازد

۷. پروسسه دیجیتال فارنزیک

سیستم قربانی توسط نفوذگر مورد حمله قرار می گیرد در این زمان ، مراحل انجام کار در فارنزیک پس از اجازه بررسی سیستم یا سایت و...با مجوز قانونی از مراجع بالاتر توسط تیم یا فرد مورد نظر طبق شکل ۱ می باشد[2]



شکل ۱- پروسسه دیجیتال فارنزیک

-اطلاعات ، اجزاها و نهادهای مختلف مرتبط با جرم را تعیین می کنیم .

-حفظ صحنه جرم و شواهد آن بدون هیچ گونه آسیب و تغییری

-جمع آوری اطلاعات (براساس violate&non-violate)

-تجزیه وتحلیل داده ها و اطلاعات جمع آوری شده وارزیابی توسط ابزارها

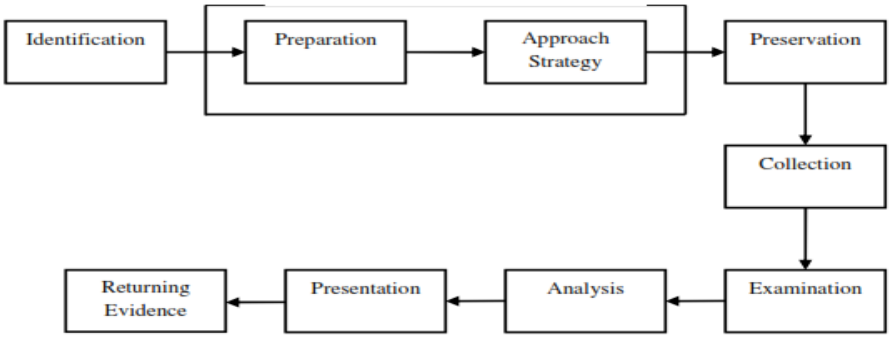
-ارائه مستندات و تهیه گزارش نهایی بصورت طبقه بندی شده به مراجع بالاتر

۱۰.خلاصه مدل فارنزیک دیجیتالی

خلاصه مدل فارنزیک دیجیتال شامل ۹ جزءاست که طبق شکل ۲ شرح داده شده است :[3]

- شناسایی: این به شناسایی و شناسایی نوع حادثه کمک می کند .
  تأثیر بر مراحل یا مرحله دیگر این مدل.
- آماده سازی: آماده سازی روش ها، تکنیک ها، ارزیابی های جستجو
- راهبرد رویکرد: این است که فرمول روش ها و رویکردهای مورد استفاده درجمع آوری شواهد.
- حفظ: این موضوع به حفظ صحنه جرم و حفظ شواهد کمک می کند.
- جمع آوری: مجموعه از روش های استاندارد برای ضبط صحنه فیزیکی انجام می شود
- امتحان: این به دنبال یافتن شواهد مربوط به مظنون مربوط به جرم است.
- تجزیه و تحلیل: بازرسی از اهمیت محصولات مورد بررسی.
- ارائه: شرح همه مراحل درگیر.
- بازگردانی شواهد: بازگشت منابع دیجیتال به صاحب حق.

در این مدل فاز سوم تا حدودی تکثیر مرحله دوم آن است.



شکل ۲- خلاصه مدل دیجیتال فارنزیک

۱۱.چارچوب تحقیق در رویداد مبتنی بر جرم شناسی دیجیتال

چارچوب رویداد مبتنی بر بررسی جرم شناسی دیجیتال طبق شکل ۳ طراحی و پیشنهاد شد[4] .بر اساس حوادثی که دارای مرحله آمادگی، مرحله استقرار ،بررسی جرم و جنایت فیزیکی، صحنه جرم دیجیتال مرحله تحقیق و مرحله ارائه در آن بود با این حال، این چارچوب مورد نیاز برای هر فاز انعطاف پذیر بوداما برای تحقیقات خوب نبود .

شکل ۳- رویداد مبتنی بر جرم شناسی دیجیتال

۱۲.ده مکان برتر برای جمع آوری شواهد[5]

- فایل های تاریخچه اینترنت
- فایل های موقت اینترنتی
- فضای خالی / غیر اختصاصی
- لیست دوستان، سوابق شخصی اتاق چت
- گروه های اخبار / لیست های باشگاه / ارسال
- تنظیمات، ساختار پوشه، نام فایل
- تاریخ ذخیره سازی فایل
- نرم افزار / سخت افزار اضافه شده است
- قابلیت اشتراک گذاری فایل
- نامه های الکترونیکی

۱۳.روش متداول جرم شناسی رایانه ای

- کامپیوتر را خاموش نکنید
- تنظیمات سخت افزاری سیستم را مستند کنید
- سیستم کامپیوتری را به مکان امن منتقل کنید
- پشتیبان گیری جریان بیتی از هارد دیسک و فلاپی دیسک را ایجاد کنید
- داده ها را بر روی تمام دستگاه های ذخیره سازی تأیید کند
- تاریخ سیستم و زمان سیستم را مستند نمایید
- لیستی از کلمات کلیدی جستجو را ایجاد کنید
- ارزیابی فضای غیر اختصاصی (فایل های پاک شده)

- شناسایی فایل ها، برنامه ها و ناهنجاری های ذخیره سازی
- ارزیابی ویژگی های برنامه.

14.فایل های مخفی و موقت

فایلهای مخفی و موقت نقاط بسیار مهم برای نفوذگران می باشد.نفوذگران حملات خود را بااستفاده از فایلهایی ، برای اتصال فایلهای مخفی و موقت بطور مستمر و یکپارچه و با پایداری بسیار بالا نیاز دارند انجام می دهند.
علت استفاده نفوذگران از این فایلها بدلیل مخفی بودن وموقت بودن آن می باشدو کاربران اهمیت چندانی برای آن قائل نیستند و آن را بررسی نمی کنند.
نفوذگران با این غفلت کاربران از نقاط حساس، استفاده کرده و فایلها را به آن اتصال می دهند تا دسترسی خود را دائمی نمایند.پوشه ای که نفوذگران از ان استفاده می کنند بنام App data نام دارد.

15.بازرس یا تیم متخصص فارنزیک

در علم فارنزیک کسب اطلاعات توسط تیم یا بازرس فارنزیک بسیار قائل اهمیت می باشد بطوری که با کشف موارد بسیار زیاد در اقدامات فارنزیک موجب سهولت شدن فرآیند موجود می شود.
در اقدامات فارنزیک کشف موارد زیر کمک بسیار زیادی به تیم یا بازرس فارنزیک می کند این موارد به شرح زیر می باشد:

۱- تعداد افرادی که به سیستم قربانی بطور فیزیکی یا ریموت دسترسی داشته اند را مشخص کند.
۲- نام کاربری و رمزعبور افرادی که از سیستم قربانی استفاده شده است، بررسی نماید.
۳- بازه زمانی را مشخص نماید.(هفتگی ، روزانه، ساعت)
۴- در بازه زمانی مشخص شده ، برنامه ها ،ابزارها،فایل و فولدر و ... را مشخص نماید.
۵- اتصال به اینترنت و درگاههای موجود را بررسی نماید.
۶- فایلهای دانلود و آپلود شده بر روی مرورگرو یا سروروسایت را بررسی نمایند.
۷- موتورهای مختلف جستو بررسی و آنالیز شود.
۸- کمک جرم شناسی کامپیوتر به پرونده های منابع انسانی / استخدام

تجزیه و تحلیل جرم شناسی کامپیوتر به طور فزاینده ای برای کسب و کارها مفید است .رایانه ها می توانند شواهدی در بسیاری از موارد رسیدگی به منابع انسانی داشته باشند، از جمله موارد آزار جنسی، ادعاهای تبعیض، ادعاهای خاتمه اشتباه و دیگران .شواهد موجود در سیستم های پست الکترونیکی، سرورهای شبکه و رایانه های شخصی کارکنان وجود دارد .با این حال، به علت سهولت که داده های کامپیوتری دارند می تواند دستکاری شود، اگر جستجو و تجزیه و تحلیل توسط یک متخصص جرم شناسی کامپیوتر ارائه نشود، احتمالا از دادگاه خارج می شود. [6]

۱۶. جرم سایبری

با توجه به توسعه فناوری ، سارقان اینترنتی و سیستمی با روش ها ومتدهای متفاوتی دست به سرقت می زنند. براین اساس حملاتی که از طریق سارقان صورت می گیرد به دو دسته می توان تقسیم کرد:

۱- حملات داخلی

۲- حملات خارجی

حملات داخلی :

این حملات توسط افراد ناراضی در سازمان ویا شرکت صورت می پذیرد. این افراد گزینه ای بسیار مهم برای نفوذ به سیستم سازمان یا شرکت می باشندو سارقان برای بدست آوردن اطلاعات طبقه بندی شده از آنها استفاده می کنند. مدیران ارشد باید به این نکته درباره کارمندان ناراضی توجه خاصی داشته باشند.

حملات خارجی:

با استفاده از کارمندان ناراضی و یا ابزارها و برنامه های کاربردی برای از بین بردن اعتبار سازمان یا شرکت .

۱۷. نمونه هایی از جرائم سایبری

- جعل و تقلب رسانه های دیجیتال
- دسترسی به اطاعات طبقه بندی شده با عبور از سیاست های امنیتی
- حملات انکار سرویس
- فراردادن انواع بدافزارها در سیستم رایانه ای سازمان یا شرکت

۱۸. نتیجه

به دلیل افزایش جرائم سایبری و توسعه اینترنت و گسترش تکنولوژی علم جرم شناسی کامپیوتری صورت گرفته است در این مقاله ، موارد بسیاری از فارنزیک کامپیوتری مورد بررسی قرار گرفته است .
پس از بررسی عناوین گسترده طبقه بندی داده ها،حفظ ، تجزیه وتحلیل، حجم اطلاعات ، زمان سپری شده ، مولفه های اصلی
در علم فارنزیک می باشد
با توجه به پیشرفت تکنولوژی و اهمیت روزافزون امنیت رایانه امروز و جدی بودن جرایم اینترنتی برای متخصصان کامپیوتر مهم است که متدها و روشهایی را که در جرائم کامپیوتری استفاده می شود را درک کنند وبا استفاده از ابزارها و برنامه های کاربردی بتوانند به رهگیری نفوذگر بپردازند.

مراجع:

[1]. Asha Joseph, K. John Singh.Review of Digital Forensic Models and A Proposal For Operating System LevelEnhancements. International Journal of Computer Science and Information Security (IJCSIS),
   a. Vol. 14, No. 11, November 2016
[2]. Shraddha More, Anita Chaudhari,BrizelRodrigues,St.John.Digital Forensic Investigation Using Subject-based Semantic Document Processing. 978-1-5090-5256-1/16/$31.00,2016 IEEE
[3]. David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP. FORENSIC COMPUTING MODELS: TECHNICAL OVERVIEW .Computer Science & Information Technology (CS & IT)05, pp. 207–216, 2012.
[4]. Sara Sarwar Mir, Umar Shoaib, Muhammad Shahzad Sarfraz. Analysis of Digital Forensic Investigation Models .International Journal of Computer Science and Information Security (IJCSIS),
   a. Vol. 14, No. 11, November 2016
[5]. Miss.P.Sumathi, Mrs.G.Saktheeswari, Mrs.C.Kuyin , Jayaraj Annapackiam. Need for a Computer Forensics in Crime Evidence . International Journal of Engineering Technology, Management and Applied Sciences, February 2016, Volume 4, Issue 2, ISSN 2349-4476
[6]. http://www.computerforensics.com/hr-employ.html