# چه کسانی ، چه زمانی از کجا به کدام فایل های شما کنجکاو بوده اند؟

**چه کسانی ، چه زمانی از کجا به کدام فایل های شما کنجکاو بوده اند؟**

**پس از خواندن این مقاله دیگر به راحتی می توانید به موارد زیر پی ببرید:**

**همه افرادی که به منابع Share شده شما متصل می شوند را شناسایی کنید؟**

**همه فایل هایی که مورد بازدید و دستکاری مجرم قرار گرفته را شناسایی کنید؟**

**همه فایل هایی که مجرم نتوانسته آن ها را دستکاری کند را شناسایی کنید؟**

**سطح دسترسی های مجرم را شناسایی کنید؟**

**و اگر کمی بیشتر اهل کارآگاه بازی باشید در اینصورت Computer Name، MAC Address، پورت های باز کامپیوتر او را هم شناسایی کنید و ....**

**فرض کنید من در کامپیوترم فولدرهایی را به اشتراک گذاشته ام . برخی از آن ها را هم به صورت مخفی Share کردم. به دلیل مهم بودن فایل های به اشتراک گذاشته شده مهم است که بدانم چه کسانی ، چه زمانی و از کجا به این فایل ها دسترسی داشته اند.**

**برای پی بردن به این موضوع ما به یک Policy نیاز داریم. یک Policy فوق محرمانه که در کامپیوترمان و در Group Policy وجود دارد که در آنجا خاک می خورد. Policy محرمانه ای که فقط افراد حرفه ای آن را می شناسند و از آن بهره می برند. این Policy فوق محرمانه " Audit Detailed File Share " نام دارد.**

## Audit Detailed File Share Policy را بیشتر بشناسید...

این Policy به شما اجازه می دهد تا بتوانید تلاش هایی را که برای دسترسی به منابع Share شده شما صورت می گیرد، ثبت کنید. این Policy یعنی **Detailed File Share** هر بار که کسی بخواهد به فایل یا فولدری از منابع Share شده شما دسترسی داشته باشد، یک Event را ثبت می کند. برخلاف Policy مشابه آن یعنی File Share (و نه Detailed File Share ) که فقط یک Event را برای تمام Connection های برقرار شده به منابع Share شده ثبت می کند، Detailed File Share به ازای هر فایل و فولدری که مورد دسترسی قرار می گیرد، یک Event ثبت می کند که شامل اطلاعات کاملی در مورد سطح دسترسی ها و ضوابط دسترسی (Allow Access) یا عدم دسترسی (Deny Access) خواهد بود. در صورتی که Detailed File Share Policy را فعال کنید، در این صورت هرگاه کسی بخواهد به فایل و فولدری از منابع Share دسترسی پیدا کند، یک Audit Event در کامپیوتر شما ثبت می شود. به این نکته توجه کنید که می توانید این Policy را طوری پیکربندی کنید که حتی اگر کاربر نتواند به فایل Share شده دسترسی داشته باشد، باز هم این Audit Event ایجاد شود و خبر ناکام بودن دسترسی را به شما بدهد.

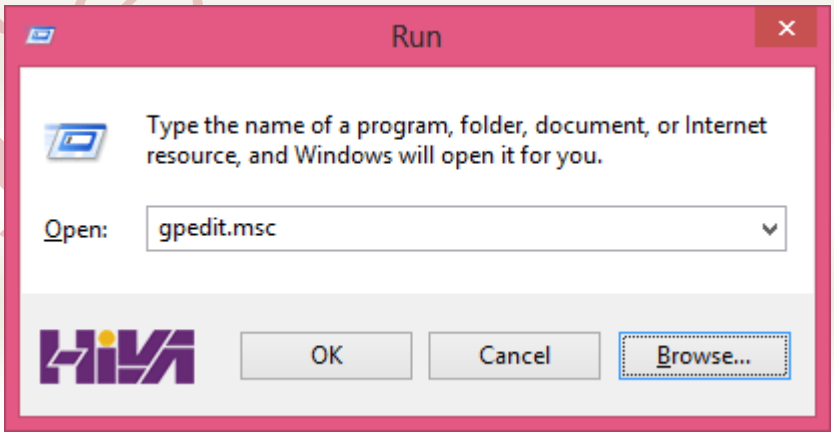
به این نکته توجه کنید که اگر این **Policy** را بر روی **Domain Controller** فعال کنید به دلیل دسترسی های فراوان کلاینت ها به **SYSVOL** که به طور پیشفرض **Share** هست، تعداد **Log** های زیادی ثبت خواهد شد که فضای زیادی را شغال خواهد کرد.

## Detailed File Share کجاست و چطور آن را فعال کنیم؟

برای فعال کردن Detailed File Share باید ابتدا وارد Group Policy شوید. چطوری؟

### روش حرفه ای ها برای ورود به Group Policy :

- دکمه های Win+R را فشار دهید.
- عبارت gpedit.msc را تایپ و Enter کنید.




### روش معمولی برای ورود به Group Policy :

در منوی Start عبارت **Group Policy** را جستجو کنید و بر روی **Edit group policy** کلیک کنید تا کنسول Group Policy باز شود.

یافتن **Detailed File Share** :

وارد شاخه زیر از Group Policy شوید:

**Computer Configuration >> Windows Settings >> Security Settings**

**Advanced Audit Policy Configuration <<**

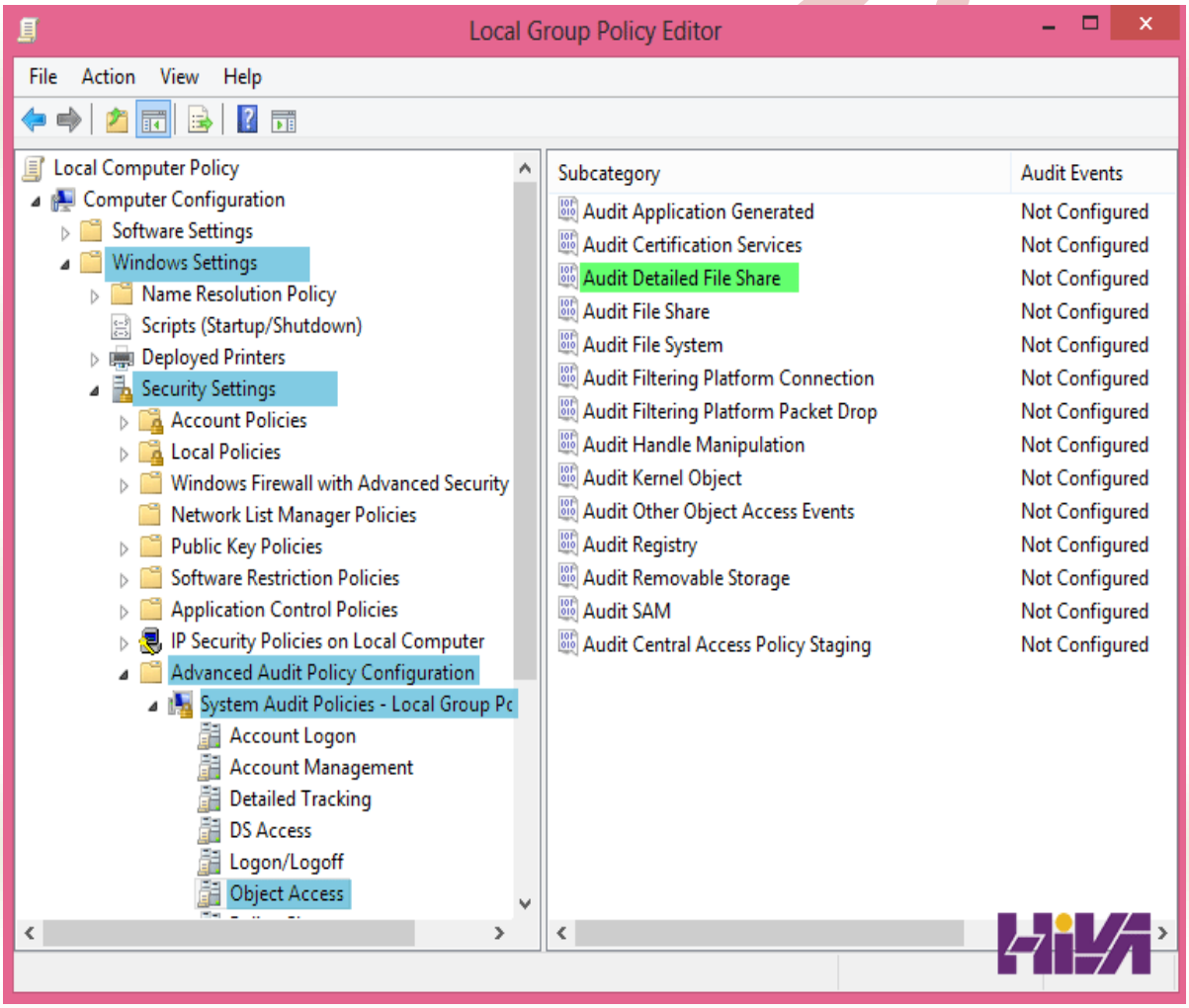
## System Audit Policies-Local Group Policy Object <<

**Object Access <<**

## Audit Detailed File Share <<

**<< در بیابان گر به شوق کعبه خواهی زد قدم**

**<< سرزنش ها گر کند خوار مغیلان غم مخور**



فعال کردن و پیکربندی **Detailed File Share Policy** :

بر روی Audit Detailed File Share کلیک کنید

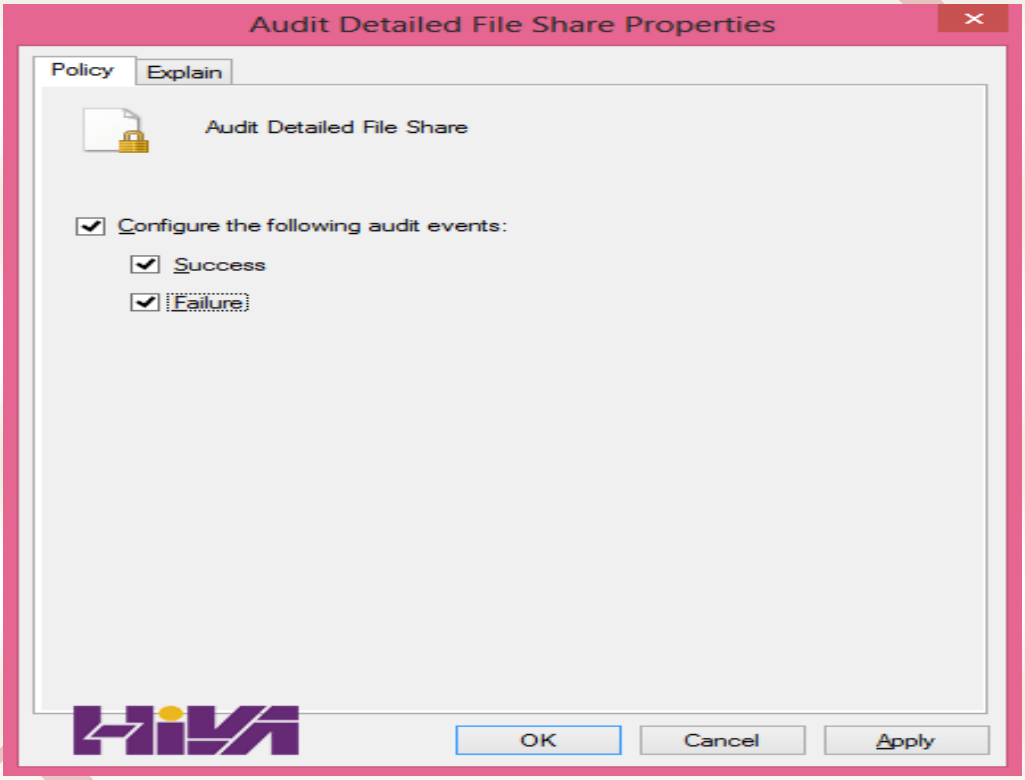
در تب Policy گزینه **Configure the following audit events** را تیک بزنید.

**Success** :

با فعال کردن این گزینه تمام دسترسی های موفقیت آمیز به منابع Share شده ثبت خواهند شد.

**Failure** :

با فعال کردن این گزینه تمام دسترسی هایی که به منابع Share ناکام بوده اند ثبت خواهند شد.




پس از OK کردن، این Policy فوق محرمانه از این پس در حالت آماده باش خواهد بود.

سناریو :

شما یک لپ تاپ دارید که در آن فایل هایی را Share کرده اید. بعضی از آن ها کاری هستند مثلا فولدر Share شده با نام MyWork Files بعضی از آن ها فایل های شخصی هستند مثلا پوشه Personal و بعضی دیگر فایل های محرمانه که آن ها را به صورت مخفی **Share** کرده اید و فقط افراد خاصی از Share بودن آن ها باخبرند مثل پوشه Secret. اکنون با لپ تاپتان وارد یک مکان عمومی ( مانند کتاب خانه یا کافی نت یا سایت دانشگاه ) شده

اید و در کنجی نشسته اید. از آنجایی که در هرجایی ( به ویژه مکان های عمومی ) افراد کنجکاو وجود دارند، پس حتما از سر کنجکاوی، شما را که در کنجی نشسته اید مورد کنجکاوی خود قرار داده اند و احتمالا تلاش می کنند به کامپیوتر شما متصل شوند و به منابع Share شما فقط نگاهی بیندازند( همینجوری جهت کنجکاوی (فقط)).

حالا وقت آن است که ببینید...

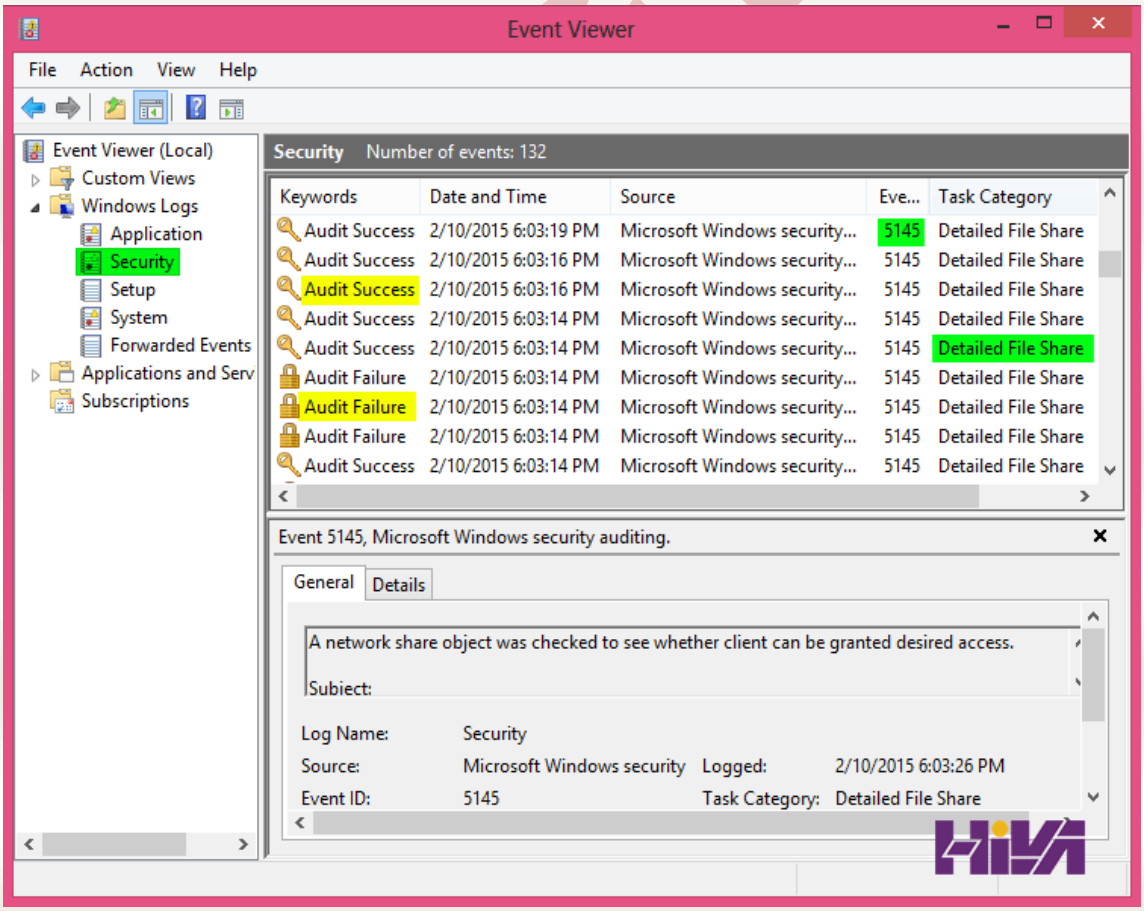
چه کسانی ، چه زمانی از کجا به کدام فایل های شما کنجکاو بوده اند؟ به چه فایل هایی دسترسی داشته اند؟ به چه فایل هایی دسترسی نداشتند؟ سطح دسترسی آن ها چقدر بوده است.

برای این کار باید وارد Event Viewer شوید و Event هایی را که توسط Detailed File Share به ثبت رسیده اند، بررسی نمایید.

۱- ابتدا به صورت زیر وارد Event Viewer می شویم:

در منوی Start عبارت Event Viewer را تایپ کنید و بر روی گزینه ای با نام Event Viewer یا View event logs کلیک کنید.

۲- در پنجره باز شده در منوی سمت چپ بر روی Security کلیک کنید.

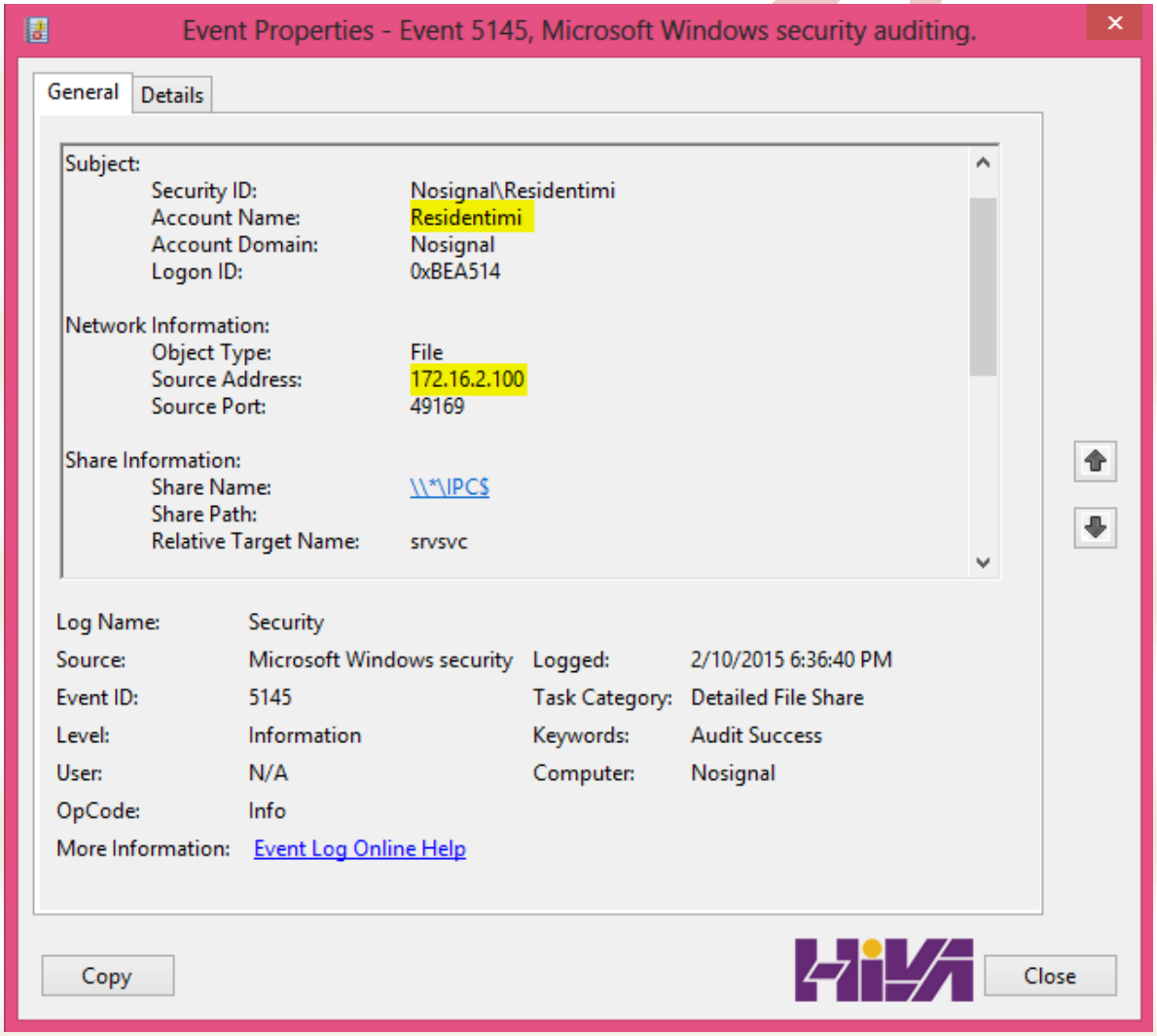


در سمت راست به دنبال Event هایی با Event ID برابر با ۵۱۴۵ و Task Category برابر با Detailed File Share بگردید. همانطور که در تصویر بالا می بینید Event هایی با کیورد Audit Success هستند که به این معنی هستند که کاربر با موفقیت کار خود را بر روی منابع Share انجام داده است و آن هایی که با کیورد Audit Failure هستند به معنی ناکامی کاربر در کار با منابع Share است. البته باید به این نکته توجه کنید که کارهایی که کاربر می تواند با منابع Share انجام دهد چیزی خارج از محدوده Permission های تعریف شده برای او نیست. پس زمانی که فرد کنجکاو کاری را انجام می دهد که Permission آن را دارد به ازای آن یک Audit Success ثبت می شود و اگر کار را انجام دهد که Permission آن را ندارد به ازای آن یک Audit Failure ثبت می شود.

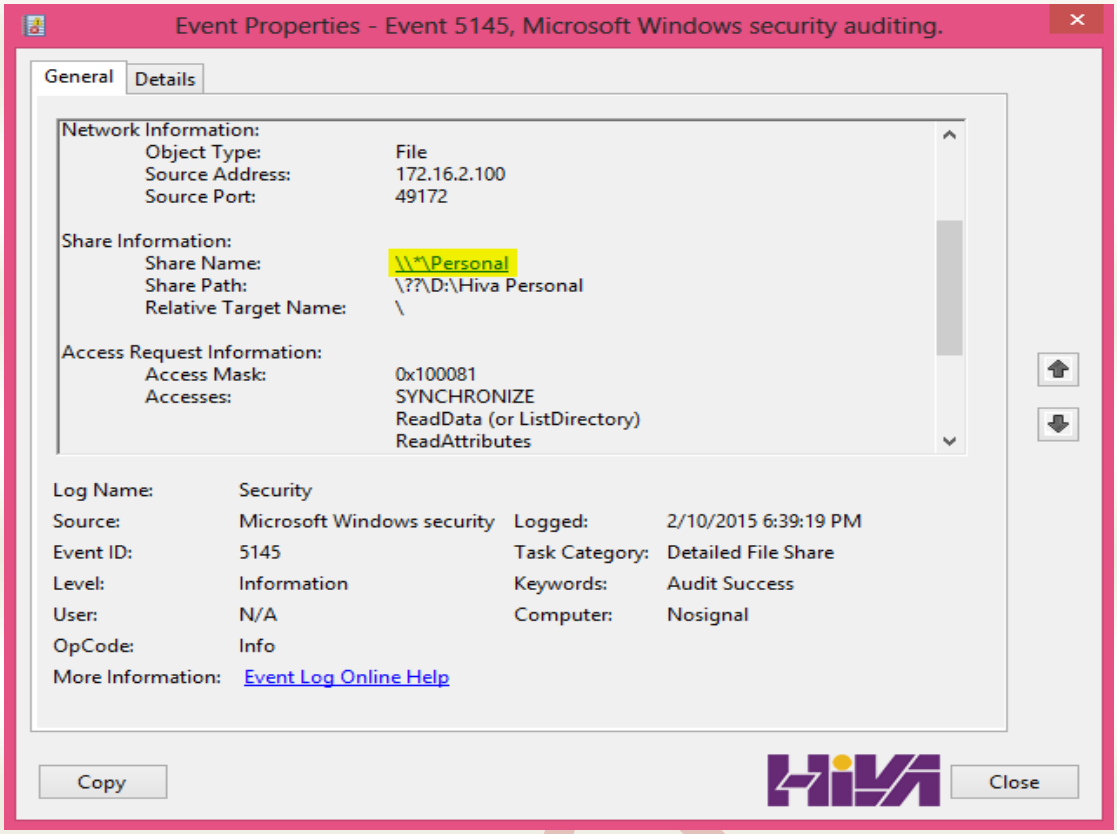
مثال:

فرد کنجکاو ۱- وارد منابع **Share** کامپیوتر شما می شود و ۲- وارد پوشه **Personal** می شود و بعد ۳- بر روی فایل **Documents.docx** کلیک می کند و بعد ۴- می خواهد آن را پاک کند در این صورت :

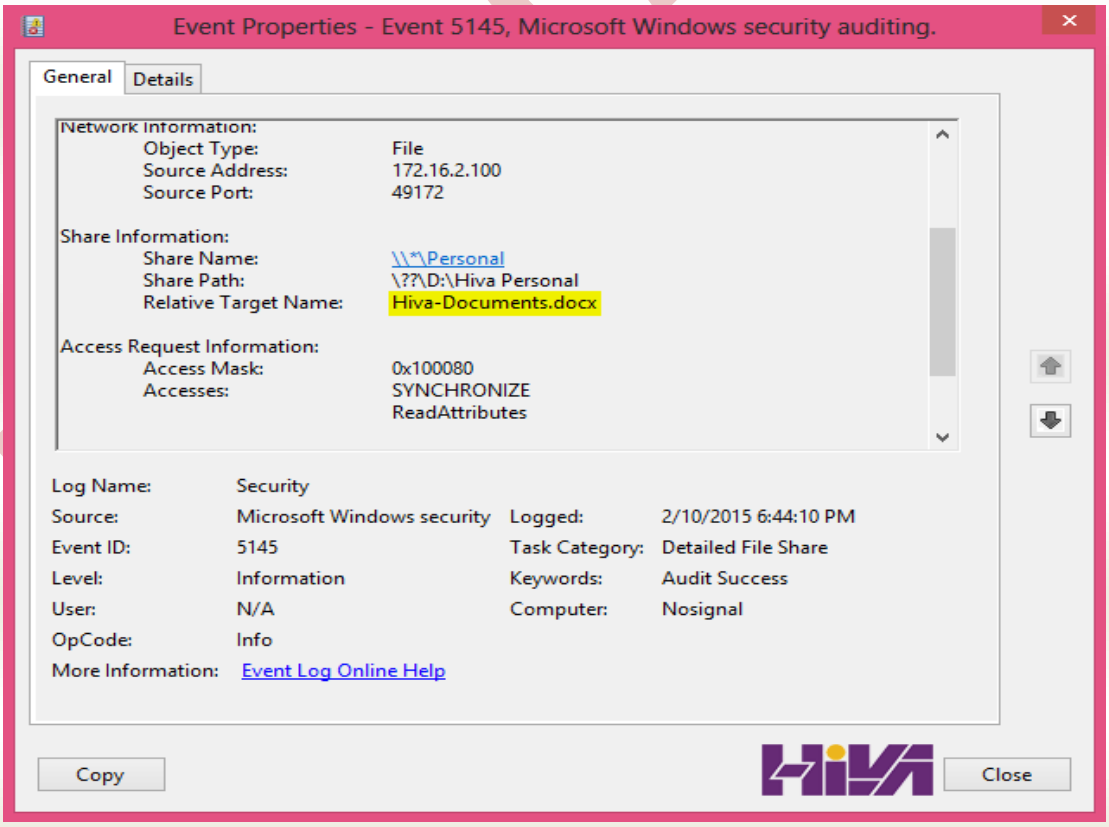
۱-



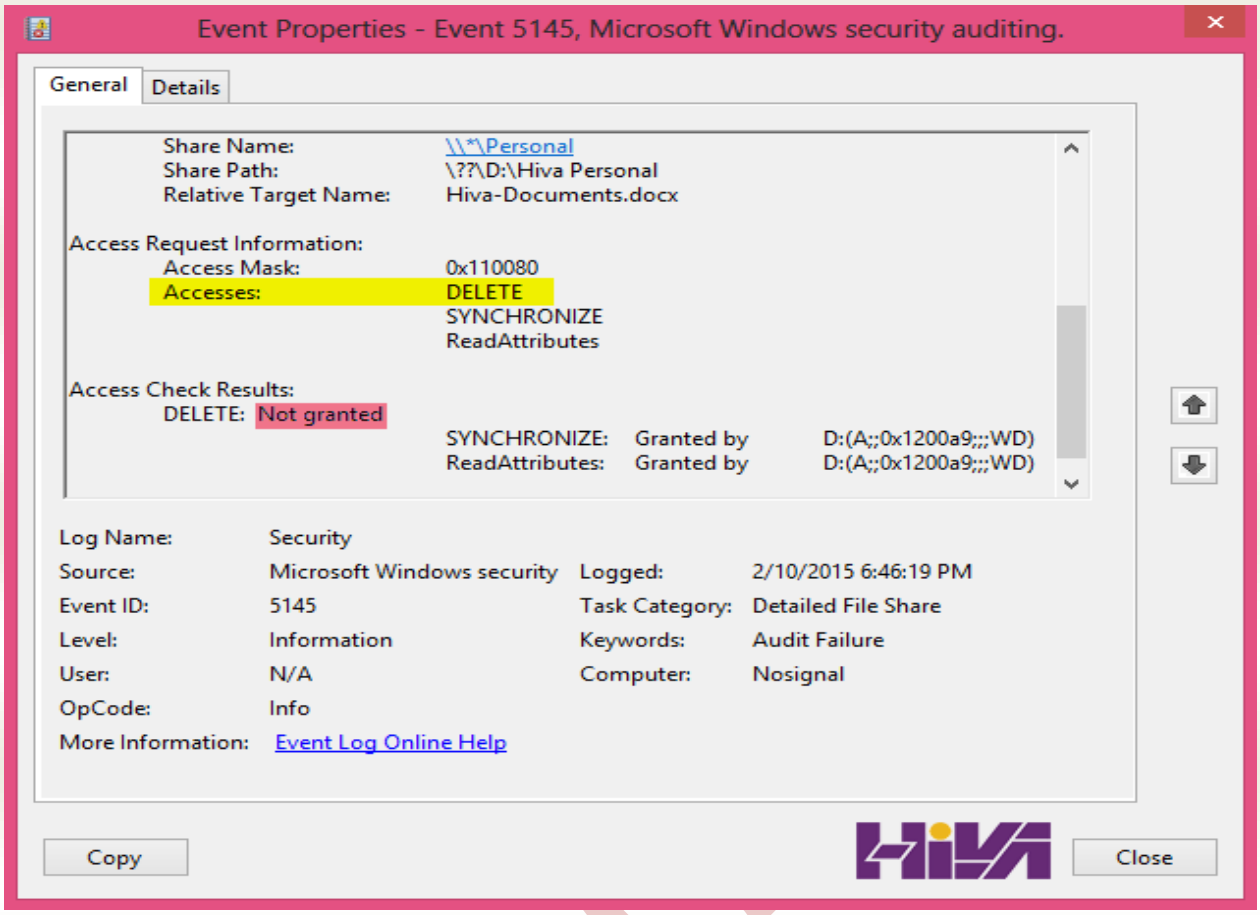

۲-


Event Properties - Event 5145, Microsoft Windows security auditing.
General
Details
Network Information:
Object Type: File
Source Address: 172.16.2.100
Source Port: 49172
Share Information:
Share Name: *\Personal
Share Path: \??\D:\Hiva Personal
Relative Target Name: \
Access Request Information:
Access Mask: 0x100081
Accesses: SYNCHRONIZE
ReadData (or ListDirectory)
ReadAttributes
Log Name: Security
Source: Microsoft Windows security
Logged: 2/10/2015 6:39:19 PM
Event ID: 5145
Task Category: Detailed File Share
Level: Information
Keywords: Audit Success
User: N/A
Computer: Nosignal
OpCode: Info
More Information: Event Log Online Help
Copy
Close

-۳


Event Properties - Event 5145, Microsoft Windows security auditing.
General
Details
Network Information:
Object Type: File
Source Address: 172.16.2.100
Source Port: 49172
Share Information:
Share Name: *\Personal
Share Path: \??\D:\Hiva Personal
Relative Target Name: Hiva-Documents.docx
Access Request Information:
Access Mask: 0x100080
Accesses: SYNCHRONIZE
ReadAttributes
Log Name: Security
Source: Microsoft Windows security
Logged: 2/10/2015 6:44:10 PM
Event ID: 5145
Task Category: Detailed File Share
Level: Information
Keywords: Audit Success
User: N/A
Computer: Nosignal
OpCode: Info
More Information: Event Log Online Help
Copy
Close

-۴




**حداقل اطلاعاتی که از Log های بالا به دست می آوریم به قرار زیر است:**

**کاربر از کامپیوتری با IP ۱۷۲,۱۶,۰,۱۰۰ و در تاریخ ۱۰ / ۲ / ۲۰۱۵و در زمان ۶:۳۶:۴۰وارد منابع Share کامپیوتر ما شده است.**

**او برای ورود به کامپیوتر شما از نام کاربری Residentimi که از کاربران کامپیوتر شماست استفاده کرده است.**

**او ۲ دقیقه و ۴۱ ثانیه بعد وارد پوشه Personal شما شده است.**

**و ۴ دقیقه و ۵۱ ثانیه بعد بر روی فایل Documents.docx کلیک کرده است.**

**و ۲ دقیقه و ۹ ثانیه بعد می خواهد آن را پاک کند اما نمی تواند.**

**Permission کاربر برای پوشه Personal در سطح Read بوده است به همین دلیل در پاک کردن فایل ناکام بوده است.**

**برای این که اطلاعات بیشتری از این فرد کنجکاو به دست آورید کار های زیر را انجام دهید:**

**برای یافتن نام کامپیوتر او از فرمان زیر کمک بگیرید:**

**Ping  -a 172.16.0.100**

**و برای یافتن آدرس سخت افزاری او فرمان زیر را وارد کنید:**

**Nbtstat –A 172.16.0.100**