

ОБЛАСТ ИНФОРМАТИЧКИ ТЕХНОЛОГИИ

ПРАКТИЧЕН СЛУЧАЈ БР. 2 - Анализа на дневници на настани во компјутерски систем

До вешто лице: АА

Нарачател: ББ

Барање за изготвување на Вешт наод и мислење од област информатички технологии

Почитуван,

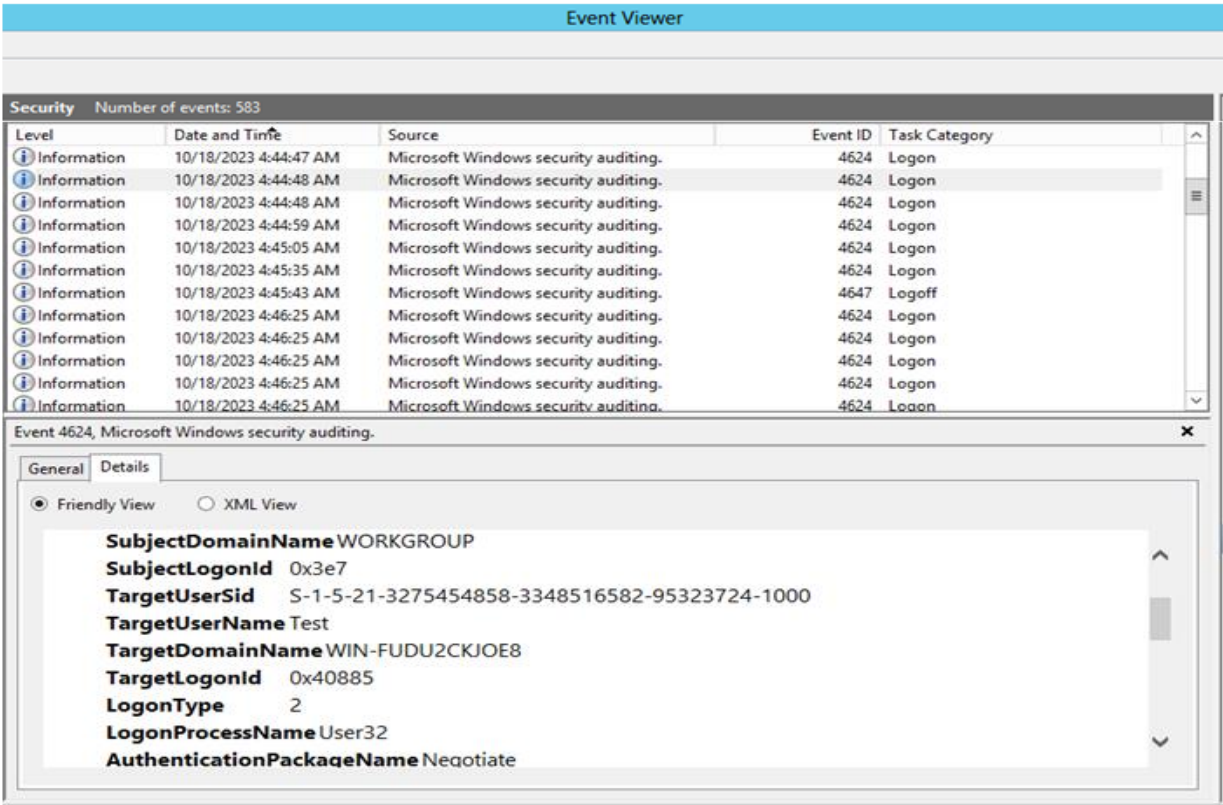
Пред Основниот суд ВВ, се води постапка 22/2025, каде што како тужител се јавува ДД, а тужен е ББ. За потребите на постапката, потребно е да се изготви Вешт наод и мислење од областа на информатичките технологии, во кои треба да се изврши анализа на дневници со записи за настани во предметниот компјутерски систем и да се даде одговор на следните околности (1-5), кои се однесуваат на записите прикажани на Сликите 1 -7 , дадени во прилог на ова Барање.

1. Кога е стартуван системот?
2. Кое е името на корисничкиот профил искористено за најава на системот?
3. Колку пати и во кои временски моменти корисникот се најавил на системот?
4. Дали се обидел корисникот да стартува апликација/сервис за кои нема привилегии?
5. Дали постојат записи во дневникот System од нерегистрирани извори?

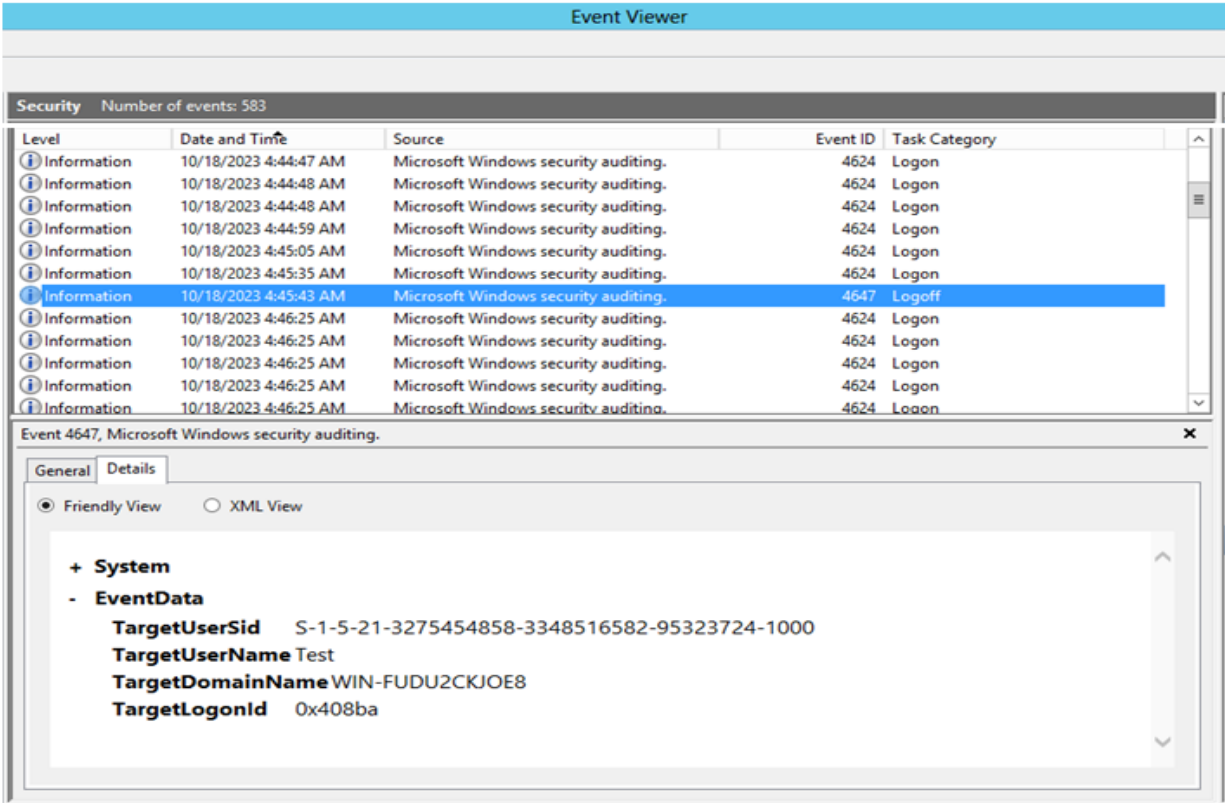
Со почит,

ББ

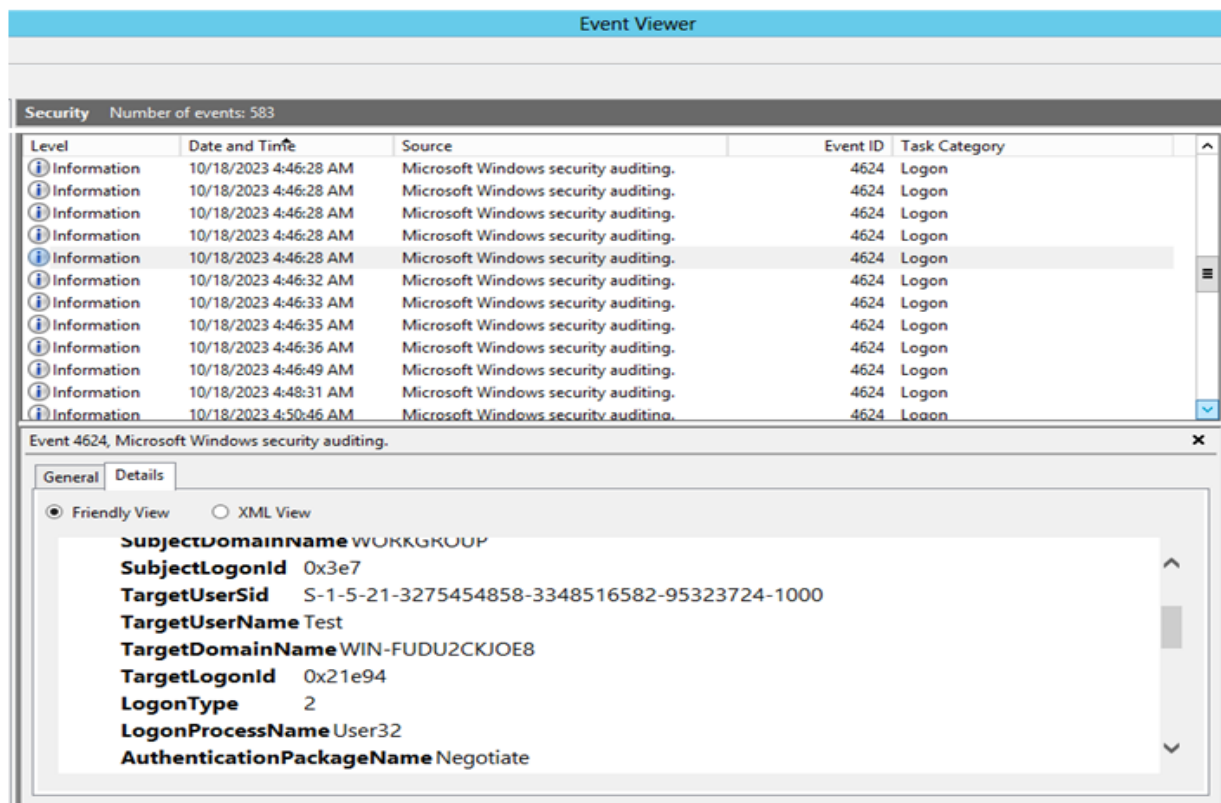
Прилог кон Барањето за вештачење:



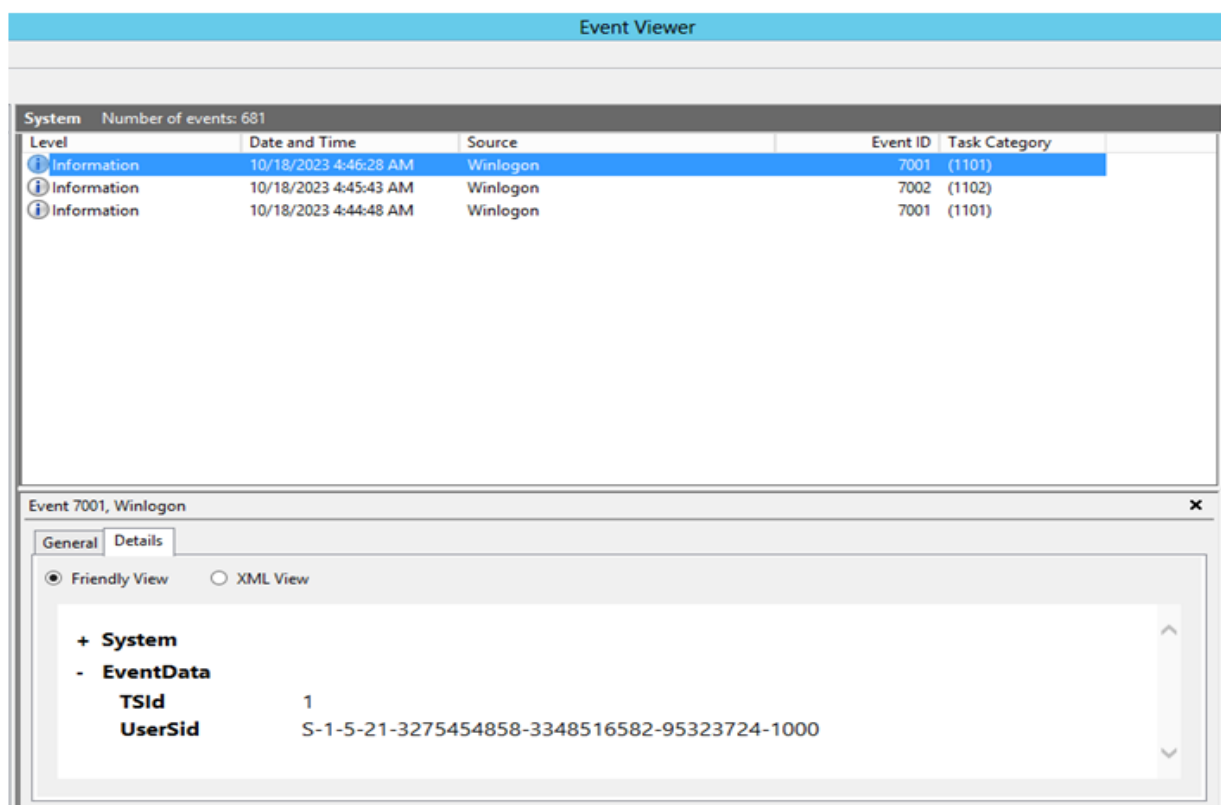
Слика 1.



Слика 2.



Слика 3.



Слика 4.

Event Viewer

System Number of events: 681

Level	Date and Time	Source	Event ID	Task Category
Information	10/18/2023 4:44:41 AM	Service Control Manager	7036	None
Information	10/18/2023 4:44:41 AM	EventLog	6013	None
Information	10/18/2023 4:44:41 AM	EventLog	6005	None
Information	10/18/2023 4:44:41 AM	Service Control Manager	7036	None
Information	10/18/2023 4:44:41 AM	Dhcp-Client	50036	Service State Event
Information	10/18/2023 4:44:41 AM	Dhcp-Client	50103	Service State Event
Information	10/18/2023 4:44:41 AM	Dhcp-Client	50036	Service State Event
Information	10/18/2023 4:44:41 AM	Service Control Manager	7036	None
Information	10/18/2023 4:44:41 AM	DHCPv6-Client	51046	Service State Event
Information	10/18/2023 4:44:41 AM	Service Control Manager	7036	None
Information	10/18/2023 4:44:41 AM	Kernel-General	16	None
Information	10/18/2023 4:44:41 AM	Service Control Manager	7036	None

Event 6013, EventLog

General Details

The system uptime is 15 seconds.

Log Name: System

Source: EventLog

Event ID: 6013

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 10/18/2023 4:44:41 AM

Task Category: None

Keywords: Classic

Computer: WIN-FUDU2CKJOE8

Слика 5.

Event Viewer

System Number of events: 681

Level	Date and Time	Source	Event ID	Task Category
Information	10/18/2023 4:44:50 AM	Service Control Manager	7036	None
Information	10/18/2023 4:44:50 AM	Service Control Manager	7036	None
Information	10/18/2023 4:44:50 AM	Service Control Manager	7036	None
Warning	10/18/2023 4:44:50 AM	DistributedCOM	10016	None
Information	10/18/2023 4:44:50 AM	Service Control Manager	7036	None
Information	10/18/2023 4:44:51 AM	Service Control Manager	7036	None
Information	10/18/2023 4:44:51 AM	Service Control Manager	7036	None

Event 10016, DistributedCOM

General Details

The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID {21B896BF-008D-4D01-A27B-26061B960DD7} and APPID {03E09F3B-DCE4-44FE-A9CF-82D050827E1C} to the user WIN-FUDU2CKJOE8\Test SID (S-1-5-21-3275454858-3348516582-95323724-1000) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.

Log Name: System

Source: DistributedCOM

Event ID: 10016

Level: Warning

User: S-1-5-21-3275454858-334851

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 10/18/2023 4:44:50 AM

Task Category: None

Keywords: Classic

Computer: WIN-FUDU2CKJOE8

Слика 6.

Event Viewer

System Number of events: 681

Level	Date and Time	Source	Event ID	Task Category
Information	10/18/2023 4:52:20 AM	Service Control Manager	7036	None
Information	10/18/2023 4:52:29 AM	Service Control Manager	7036	None
Warning	10/18/2023 4:52:39 AM	e1i68x64	27	None
Information	10/18/2023 4:59:07 AM	Kernel-General	24	(11)
Information	10/18/2023 4:59:07 AM	Kernel-General	1	(5)
Information	10/18/2023 4:59:07 AM	e1i68x64	32	None
Information	10/18/2023 4:59:08 AM	Display	4107	None

Event 27, e1i68x64

General Details

The description for Event ID 27 from source e1i68x64 cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

Intel(R) 82574L Gigabit Network Connection

Log Name: System

Source: e1i68x64

Event ID: 27

Level: Warning

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 10/18/2023 4:52:39 AM

Task Category: None

Keywords: Classic

Computer: WIN-FUDU2CKJOE8

слика 7.