



UNIVERSITÀ  
DEGLI STUDI DI BARI  
ALDO MORO

# Corso di Informatica Forense

## Anno Accademico 2021/2022

PROGETTO DI INFORMATICA FORENSE  
*Activities Inspector* – Documentazione

Candidato: **Antonio Argentieri**



# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

## Sommario

Cos'è Activities Inspector .....	3
Requisiti di sistema.....	4
Elenco delle funzionalità.....	4
Funzionalità di Accensione/Spegnimento .....	5
Programmi installati .....	7
File recenti .....	8
File prefetch.....	9
Shellbags.....	10
Orari di LogOn / LogOff .....	11
Modifiche all'ora di sistema .....	14
Periferiche USB.....	16
Generazione del report finale .....	18



## Cos'è Activities Inspector

Activities Inspector è il software che consente di estrapolare informazioni dettagliate riguardanti l'utilizzo del PC.

I risultati raccolti dal software sono suddivisi per categoria. Di seguito le categorie di cui il software si compone:

- Accensione/Spegnimento.
- Programmi installati.
- File recenti.
- File di Prefetch.
- Shellbags.
- Logon/Logoff.

Le informazioni vengono elaborate dal software mediante analisi che coinvolgono il registro di sistema, eventi di Windows (eventi di sistema e di sicurezza) e file memorizzati in cartelle specifiche del file system.

Una volta prodotti i risultati sarà possibile esportarli per categoria in formato csv.



Figura 1 – Schermata di apertura del programma

Si tratta di un progetto *.NET Framework* sviluppato in *C#* e *WPF* attraverso l'ambiente di sviluppo Visual Studio 2019.

## Requisiti di sistema

Il software è disponibile solo per PC Windows e con sistema operativo da Windows Vista o superiore. La versione 32 o 64 bit è indifferente.

E' fortemente raccomandata l'esecuzione in modalità Amministratore al fine di poter utilizzare le funzionalità basate sull'analisi di dati dal registro di sistema.

Il software può essere eseguito senza alcuna installazione al fine di non alterare il reperto stesso dal quale le informazioni vengono acquisite.

Non sono richieste invece, specifiche hardware particolari.

## Elenco delle funzionalità

Activities Inspector consente all'utente di condurre un'analisi basata su molteplici aspetti che coinvolgono il *registro di sistema*, gli *eventi di Windows* e *file system*.

In fase di esecuzione non è obbligatorio eseguire l'analisi completa di tutte le funzionalità. E' l'utente a richiamare la (o le) funzionalità desiderate attraverso l'apposito menu sulla sinistra dell'interfaccia.

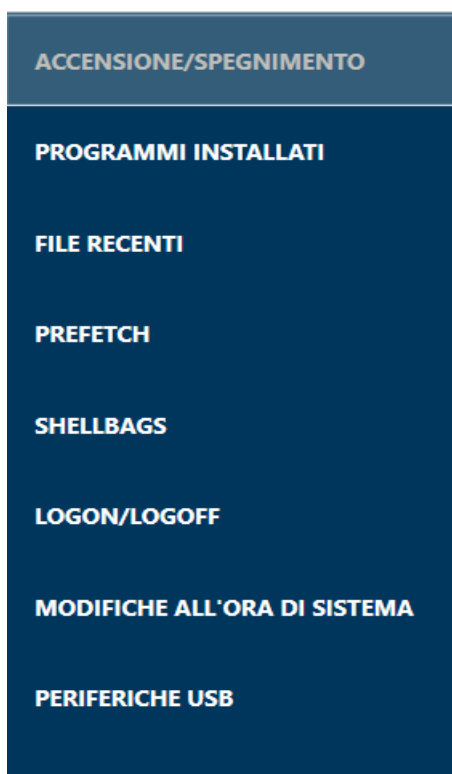


Figura 2 – Menu delle funzionalità



La funzione di ricerca si avvia attraverso l'apposito pulsante *Cerca* posto nella parte in alto dell'interfaccia:

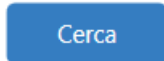


Figura 3 – Funzione di ricerca

Alla fine di ogni elaborazione, per ogni funzionalità, viene elaborata una tabella contenente i risultati prodotti dalla ricerca.

Solo una volta che la tabella è stata elaborata si abiliterà il pulsante di *Esporta*.

A questo punto sarà possibile salvare i risultati in un file csv:

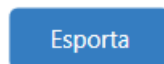


Figura 4 – Funzione di esportazione

La funzionalità di esportazione CSV creerà, per ogni ricerca effettuata, un file con estensione .csv nella cartella Output dell'applicazione. **Esportando nuovamente uno stesso file precedentemente esportato nella cartella, il nuovo andrà a sovrascrivere il file esistente.**

Ogni funzionalità per essere eseguita può richiedere fino ad alcuni secondi, dipendentemente dalla potenza della macchina e dalla mole di dati da elaborare.

La componente “business” lavora su un *thread* differente rispetto a quello dell'interfaccia pertanto non vi sono operazioni bloccanti. Per operazioni bloccanti si intende che non ci sono operazioni che bloccano l'interfaccia finchè non vengono prodotti i risultati.

## Funzionalità di Accensione/Spegnimento

È la funzionalità che consente di determinare tutti gli intervalli temporali indicanti il momento in cui il PC è stato acceso fino al momento in cui è stato spento.

In questi log si tiene conto anche degli eventuali log indicanti i riavvii di sistema e inizio/fine della fase di *standby*.

Ogni intervallo è quindi composto da una data di accensione ed una di spegnimento.

Le date sono indicate nel formato *gg/mm/aaaa* e l'orario rappresentato attraverso lo standard *GMT* indicante l'ora locale e lo scostamento rispetto il Meridiano

Fondamentale (+1 nel caso di Roma).

Lo scostamento indica invece GMT+2 nel caso di ora legale.

Ai risultati prodotti si aggiungono un campo indicante la durata di ogni sessione e il nome del PC su cui la rilevazione è stata effettuata.



# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

I risultati vengono elaborati monitorando alcuni eventi della sezione *Sistema* e riguardanti il registro eventi di Windows. In particolare:

ID Evento	Descrizione evento
1	Il sistema è stato ripreso dalla sospensione.
41	Il sistema è stato riavviato senza essere stato prima spento in modo pulito.
42	Il sistema sta entrando in sospensione.
1072	Invocata operazione di riavvio/arresto/spegnimento.
6006	Il registro eventi è stato arrestato. E' il momento in cui il PC è stato spento.

Ogni evento è caratterizzato anche da una categoria. Nella determinazione delle attività dell'utente sono stati esclusi tutti gli eventi con categoria 5, in quanto rappresentanti eventi riferiti ad attività di sistema e non dell'utente.

ACCENSIONE/SPEGNIMENTO	Accensione	Spegnimento	Durata	Nome macchina
	25/11/2021 22:12:36 GMT+1	26/11/2021 01:00:02 GMT+1	02:47:26	MSI
PROGRAMMI INSTALLATI	26/11/2021 14:30:37 GMT+1	26/11/2021 16:25:26 GMT+1	01:54:49	MSI
	26/11/2021 16:26:13 GMT+1	26/11/2021 17:33:23 GMT+1	01:07:10	MSI
FILE RECENTI	26/11/2021 21:29:43 GMT+1	26/11/2021 22:24:54 GMT+1	00:55:11	MSI
PREFETCH	27/11/2021 17:54:38 GMT+1	27/11/2021 20:22:28 GMT+1	02:27:50	MSI
SHELLBAGS	28/11/2021 11:06:22 GMT+1	28/11/2021 12:01:12 GMT+1	00:54:50	MSI
	28/11/2021 14:28:53 GMT+1	28/11/2021 15:54:34 GMT+1	01:25:41	MSI
LOGON/LOGOFF	28/11/2021 21:11:16 GMT+1	28/11/2021 23:10:34 GMT+1	01:59:18	MSI
	28/11/2021 23:11:00 GMT+1	28/11/2021 23:13:45 GMT+1	00:02:45	MSI
	29/11/2021 10:07:41 GMT+1	29/11/2021 15:47:05 GMT+1	05:39:24	MSI
	29/11/2021 17:52:36 GMT+1	29/11/2021 18:02:39 GMT+1	00:10:03	MSI
	29/11/2021 18:03:07 GMT+1	29/11/2021 20:09:47 GMT+1	02:06:40	MSI
	29/11/2021 21:16:34 GMT+1	29/11/2021 22:08:22 GMT+1	00:51:48	MSI
	30/11/2021 20:36:25 GMT+1	30/11/2021 23:24:11 GMT+1	02:47:46	MSI
	01/12/2021 18:37:33 GMT+1	01/12/2021 19:49:33 GMT+1	01:12:00	MSI
	01/12/2021 23:26:38 GMT+1	02/12/2021 00:07:12 GMT+1	00:40:34	MSI
	02/12/2021 00:07:27 GMT+1	02/12/2021 01:07:16 GMT+1	00:59:49	MSI
	02/12/2021 21:38:10 GMT+1	03/12/2021 00:25:21 GMT+1	02:47:11	MSI
	03/12/2021 20:59:13 GMT+1	03/12/2021 21:53:57 GMT+1	00:54:44	MSI
	04/12/2021 10:17:34 GMT+1	04/12/2021 10:58:20 GMT+1	00:40:46	MSI
	04/12/2021 12:19:45 GMT+1	04/12/2021 13:12:24 GMT+1	00:52:39	MSI
	04/12/2021 13:20:23 GMT+1	04/12/2021 14:30:35 GMT+1	01:10:12	MSI
	05/12/2021 10:22:03 GMT+1	05/12/2021 12:35:35 GMT+1	02:13:32	MSI
	05/12/2021 13:35:44 GMT+1	05/12/2021 13:35:43 GMT+1	00:16:48	MSI

Figura 5 – Esempio risultato sezione Accensione/Spegnimento



## Programmi installati

Conoscere le attività svolte da un utente passa necessariamente per la ricerca dei programmi che potrebbero essere stati installati su un PC.

Per conoscere i programmi installati su una macchina è necessario incrociare le informazioni che provengono dal registro di sistema con le informazioni che provengono dagli eventi di Windows.

Per quanto riguarda le informazioni provenienti dal registro è sufficiente tenere a mente che quasi tutti i programmi installati creano delle voci in specifiche aree del registro. Le voci di registro coinvolte nelle installazioni di un programma sono essenzialmente due:

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall`

La ricerca va ad analizzare tutte le sottochiavi create nei percorsi appena citati e tiene conto della possibilità in Windows di installare un applicativo sia a livello di singolo utente che a livello di macchina (e quindi rendendo il software disponibile a tutti gli utenti).

Per quanto riguarda le informazioni provenienti dagli eventi invece, vengono analizzati tutti quegli eventi con ID 11707.

Ogni evento di questo tipo viene scritto quando l'installazione di un software viene portata a termine con successo lanciando il processo da file con estensione .msi. Questo metodo si è rivelato utile anche nell'intercettare l'installazione di software *stealth* i quali operano in modalità "nascosta" non lasciando traccia nel registro di sistema.

In questo caso il software restituisce come risultato una tabella valorizzata con il nome del file, il percorso all'interno del registro di sistema, il percorso nel file system e la data di installazione.

E' bene precisare che campi come il nome del file, la data di installazione e il percorso nel file system a volte possono mancare in quanto ogni installazione creerà certamente nuove voci nel registro ma le chiavi create per ogni voce non sono standard. per questo, ciò che certamente non mancherà sarà, sarà il percorso all'interno del registro.



# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Activities Inspector

Esporta Cerca

ACCENSIONE/SPEGNIMENTO	Nome file	Sorgente	Percorso	Data
PROGRAMMI INSTALLATI	Microsoft .NET Host FX Resolver - 5.0.12 (x86)	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BAA79920-74A8-4801-BB8A-469498D4F729}		24/11/2021
FILE RECENTI	Microsoft ASP.NET Core 5.0.12 Shared Framework (x86)	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BF6D285-A887-3668-9E97-6BF040A60FBD}		24/11/2021
PREFETCH	Microsoft Windows Desktop Runtime - 3.1.21 (x86)	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{C415FE88-468C-475B-BC30-DAF6687EEF1F}		24/11/2021
SHELLBAGS	Microsoft .NET Framework 4 Multi-Targeting Pack	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CE4F48A8-BFB8-3EAC-8BA5-DE4F8AA267CE}		24/11/2021
LOGON/LOGOFF	Update for (KB2504637)	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CE4F48A8-BFB8-3EAC-8BA5-DE4F8AA267CE}.KB2504637		
	aTube Catcher versione 3.8	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{D43B360E-722D-421B-BC77-2089E0F886CD}_is1	C:\Program Files (x86)\DsNET CorpiaTube Catcher 2.0\	13/1/2022
	Microsoft .NET Framework 4.8 SDK (Italiano)	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{DD882274-C40D-4DCF-ACD9-7B54280A3811}		24/11/2021
	Microsoft .NET Core Runtime - 3.1.21 (x86)	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{DEB99C7D-471C-49C5-AE30-4E166160BF03}		24/11/2021
	vs_tipsmsi	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{E208E682-50EE-4F2F-9860-C91B9068BA03}		24/11/2021
	Microsoft .NET Framework Cumulative Intellisense Pack per Visual Studio (Italiano)	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EC91F894-D583-4F20-B1C1-A530FB4140E0}		24/11/2021
	MSI SDK	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{EE7D557C-3AE7-4348-8DCA-3AB9790D0002}_is1	C:\Program Files (x86)\MSI\One Dragon Center\	13/1/2022
	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows		11/12/2021

Figura 6 – Esempio risultato sezione Programmi installati

## File recenti

Questa funzionalità è stata implementata per tenere traccia degli ultimi file aperti da un utente.

Ogni volta che un file viene aperto, Windows crea una sorta di collegamento allo stesso. Il collegamento viene creato in una specifica cartella adibita a contenere tutti i collegamenti ai file aperti di recente.

La cartella in cui vengono creati questi collegamenti si trova al percorso  
*C:\Users\[NOME PROFILO]\Recent.*

Il software va alla ricerca dei file contenuti in questa cartella, file il cui formato è *.lnk*.

I file *Ink* sono file di scorciatoia associati a Windows. *Ink* è l'acronimo di *link* e costituiscono un riferimento al file originale (il file aperto dall'utente).

Un file *Ink* è un file di tipo binario e contiene proprietà come tipo di file, posizione, dimensione e il programma che apre il file di destinazione.

Dopo aver ricercato tutti i file con formato *.lnk* il software costruisce per ognuno di essi una riga della tabella.

Ogni risultato della tabella è costituito dal nome del file aperto di recente, la full path del file nella cartella Recent, il percorso del file originale aperto di recente e la data





# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

dell'ultima apertura del file (nello standard GMT spiegata precedentemente).

	Nome file	Sorgente	Percorso	Data
ACCENSIONE/SPEGNIMENTO	christmas-star-jazzhop-background-music-for-video-12073.mp3	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\christmas-star-jazzhop-background-music-for-video-12073.mp3.lnk	C:\Users\anton\Downloads\christmas-star-jazzhop-background-music-for-video-12073.mp3	23/12/2021 00:13:40 GMT+1
PROGRAMMI INSTALLATI	TrueArtRealAffectionPart4 - Noir Et Blanc Vie.mp3	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\TrueArtRealAffectionPart4 - Noir Et Blanc Vie.mp3.lnk	C:\Users\anton\Downloads\TrueArtRealAffectionPart4 - Noir Et Blanc Vie.mp3	23/12/2021 00:13:50 GMT+1
FILE RECENTI	The Night Falling - JR Tundra.mp3	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\The Night Falling - JR Tundra.mp3.lnk	C:\Users\anton\Downloads\The Night Falling - JR Tundra.mp3	23/12/2021 00:15:12 GMT+1
PREFETCH	Soul and Mind - E's Jammy Jams.mp3	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\Soul and Mind - E's Jammy Jams.mp3.lnk	C:\Users\anton\Downloads\Soul and Mind - E's Jammy Jams.mp3	23/12/2021 00:17:15 GMT+1
SHELLBAGS	Ersatz Bossa - John Deley and the 41 Players.mp3	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\Ersatz Bossa - John Deley and the 41 Players.mp3.lnk	C:\Users\anton\Downloads\Ersatz Bossa - John Deley and the 41 Players.mp3	23/12/2021 00:17:21 GMT+1
LOGON/LOGOFF	Book Bag - E's Jammy Jams.mp3	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\Book Bag - E's Jammy Jams.mp3.lnk	C:\Users\anton\Downloads\Book Bag - E's Jammy Jams.mp3	23/12/2021 00:17:47 GMT+1
	Frame-8.276-1.png	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\Frame-8.276-1.png.lnk	C:\Users\anton\OneDrive\Desktop\Frame-8.276-1.png	23/12/2021 00:18:18 GMT+1
	QuangerineCream - Noir Et Blanc Vie.mp3	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\QuangerineCream - Noir Et Blanc Vie.mp3.lnk	C:\Users\anton\Downloads\QuangerineCream - Noir Et Blanc Vie.mp3	23/12/2021 00:20:43 GMT+1
	red-wine-2443699.jpg	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\red-wine-2443699.jpg.lnk	C:\Users\anton\Downloads\red-wine-2443699.jpg	23/12/2021 00:28:03 GMT+1
	Download (2)	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\Download (2).lnk	C:\Users\anton\Downloads	23/12/2021 00:35:37 GMT+1
	free4pc.org_Wondershare Filmora _ 10.7.7.9 With Filmora 9 _ Download [Latest].rar	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\free4pc.org_Wondershare Filmora _ 10.7.7.9 With Filmora 9 _ Download [Latest].rar.lnk	C:\Users\anton\Downloads\free4pc.org_Wondershare Filmora _ 10.7.7.9 With Filmora 9 _ Download [Latest].rar	23/12/2021 00:50:03 GMT+1
	VE Project 1-converted.wfp	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\VE Project 1-converted.wfp.lnk	C:\Users\anton\OneDrive\Documents\Wondershare Filmora\Projects\VE Project 1-converted.wfp	23/12/2021 00:57:08 GMT+1
	Projects	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\Projects.lnk	C:\Users\anton\OneDrive\Documents\Wondershare Filmora\Projects	23/12/2021 00:57:08 GMT+1
	Desktop	C:\Users\anton\AppData\Roaming\Microsoft\Windows\Recent\Desktop.lnk	C:\Users\anton\OneDrive\Desktop	23/12/2021 01:00:32 GMT+1

Figura 7 – Esempio risultato sezione File recenti

## File prefetch

I file di prefetch vengono utilizzati da Windows per velocizzare l'esecuzione delle applicazioni. Ogni volta che un utente esegue un'applicazione (file .exe), viene generato un file con estensione .pf rappresentante, appunto, un file prefetch.

I file prefetch vengono salvati nella cartella `C:\Windows\Prefetch`.

Si tratta in ogni caso di file compressi; la compressione utilizzata dipende dal sistema operativo in uso pertanto la procedura tiene conto dei sistemi operativi Windows 7, Windows 8, Windows 10, Windows 11.

All'interno della cartella Prefetch possono esserci anche dei collegamenti relativi ad applicazioni non più installate nel PC in uso.

Ogni file all'interno della suddetta cartella viene analizzato ricavando da esso una stringa di byte.

Ogni file ha una struttura ben precisa. Tale struttura prevede che all'offset 0 e per i primi 4 byte viene indicata la versione del formato la quale dipende dal sistema operativo:

- 17 (0x00000011) for Windows XP;



# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

- 23 (0x00000017) for Windows Vista, Windows 2008, Windows 7 and Windows 2012 (note Windows 2012 has not been confirmed)
- 26 (0x0000001a) for Windows 8.1 (note this could be Windows 8 as well but has not been confirmed)
- 30 (0x0000001e) for Windows 10.

A partire dall'offset 4 ci sono altri 4 byte indicati la firma del file ("SCCA").

Le informazioni ricavabili da ogni file .pf sono le seguenti:

- Nome del file;
- Numero di volte che l'applicazione a cui il file si riferisce è stata eseguita;
- Informazioni sull'unità di memorizzazione fisica su cui l'applicazione è salvata;
- Data di ultima esecuzione dell'applicazione.

	Nome file	Sorgente	Estensione	Data ultima esecuzione
ACCENSIONE/SPEGNIMENTO	FILECOAUTH.EXE	C:\Windows\prefetch\FILECOAUTH.EXE-6DB49DE7.pf	.EXE	25/2/2022 21:53:58 GMT+1
PROGRAMMI INSTALLATI	FILECOAUTH.EXE	C:\Windows\prefetch\FILECOAUTH.EXE-6DB49DE7.pf	.EXE	24/2/2022 23:06:32 GMT+1
FILE RECENTI	FILECOAUTH.EXE	C:\Windows\prefetch\FILECOAUTH.EXE-6DB49DE7.pf	.EXE	20/2/2022 09:51:59 GMT+1
PREFETCH	FILMORA_64BIT_FULL1085.TMP	C:\Windows\prefetch\FILMORA_64BIT_FULL1085.TMP-AB0562B6.pf	.TMP	23/12/2021 00:12:25 GMT+1
SHELLBAGS	FILMORA_64BIT_FULL846.EXE	C:\Windows\prefetch\FILMORA_64BIT_FULL846.EXE-B6E6F116.pf	.EXE	23/12/2021 00:52:40 GMT+1
LOGON/LOGOFF	FILMORA_64BIT_FULL846.EXE	C:\Windows\prefetch\FILMORA_64BIT_FULL846.EXE-B6E6F116.pf	.EXE	23/12/2021 00:52:36 GMT+1
MODIFICHE ALL'ORA DI SISTEMA	FILMORA_64BIT_FULL846.TMP	C:\Windows\prefetch\FILMORA_64BIT_FULL846.TMP-3EC4464D.pf	.TMP	23/12/2021 00:52:37 GMT+1
PERIFERICHE USB	FILMORA_64BIT_FULL846.TMP	C:\Windows\prefetch\FILMORA_64BIT_FULL846.TMP-D5539279.pf	.TMP	23/12/2021 00:52:41 GMT+1
	FILMORA_SETUP_FULL1085.EXE	C:\Windows\prefetch\FILMORA_SETUP_FULL1085.EXE-023907CB.pf	.EXE	23/12/2021 00:08:44 GMT+1
	FKL-SETUP (PASSWORD=2017).EXE	C:\Windows\prefetch\FKL-SETUP (PASSWORD=2017).EXE-0440C66A.pf	.EXE	23/2/2022 21:46:41 GMT+1
	FNATIVEWEBENGINEEXE.EXE	C:\Windows\prefetch\FNATIVEWEBENGINEEXE.EXE-98E44026.pf	.EXE	23/12/2021 00:26:23 GMT+1
	FNATIVEWEBENGINEEXE.EXE	C:\Windows\prefetch\FNATIVEWEBENGINEEXE.EXE-98E44026.pf	.EXE	23/12/2021 00:14:45 GMT+1
	FONDUE.EXE	C:\Windows\prefetch\FONDUE.EXE-F93829DA.pf	.EXE	12/2/2022 17:00:14 GMT+1
	FONTDRVHOST.EXE	C:\Windows\prefetch\FONTDRVHOST.EXE-8152304A.pf	.EXE	24/2/2022 00:10:58 GMT+1
	FONTDRVHOST.EXE	C:\Windows\prefetch\FONTDRVHOST.EXE-8152304A.pf	.EXE	20/2/2022 11:30:33 GMT+1
	FONTDRVHOST.EXE	C:\Windows\prefetch\FONTDRVHOST.EXE-8152304A.pf	.EXE	20/2/2022 01:51:25 GMT+1
	FREEMAKEVIDEOCONVERTER.EXE	C:\Windows\prefetch\FREEMAKEVIDEOCONVERTER.EXE-34248820.pf	.EXE	13/1/2022 22:00:51 GMT+1
REPORT	FREEMAKEVIDEOCONVERTER.EXE	C:\Windows\prefetch\FREEMAKEVIDEOCONVERTER.EXE-34248820.pf	.EXE	13/1/2022 20:44:59 GMT+1

Figura 8 – Esempio risultato sezione File prefetch

## Shellbags

Ogni volta che viene aperta una cartella attraverso la funzione “Esplora risorse”, Windows salva le impostazioni di questa directory nel registro di sistema.

Lo scopo di questa funzionalità è quello di conoscere i percorsi, nomi e data di apertura delle cartelle aperte sia sul disco fisso che su dispositivi USB.

Le informazioni relative alle cartelle vengono memorizzate in chiavi di registro, quali:

- HKEY\_CURRENT\_USER \ Software \ Microsoft \ Windows \ Shell \ Bags;



- E' importante analizzare queste chiavi in quanto siamo in grado anche di rilevare eventuali azioni di un utente malevolo anche quando questo ha cancellato i file e le cartelle da esso visitate.

Activities Inspector						Esporta	Cerca
	Percorso assoluto	Data accesso	Data di creazione	Data ultima scrittura	Percorso nel registro		
ACCENSIONE/SPENIMENTO	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	09/01/2022 15:52:30 GMT+1	22/12/2021 23:52:54 GMT+1	09/01/2022 15:53:19 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\1\0\0\0		
PROGRAMMI INSTALLATI	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	09/01/2022 15:52:30 GMT+1	22/12/2021 23:52:54 GMT+1	09/01/2022 15:53:24 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\1\0\0\1		
FILE RECENTI	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	09/01/2022 15:52:30 GMT+1	22/12/2021 23:52:54 GMT+1	09/01/2022 15:53:27 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\1\0\0\2		
PREFETCH	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	09/01/2022 15:52:30 GMT+1	22/12/2021 23:52:54 GMT+1	09/01/2022 15:53:29 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\1\0\0\3		
SHELLBAGS	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	09/01/2022 15:52:30 GMT+1	22/12/2021 23:52:54 GMT+1	09/01/2022 15:53:31 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\1\0\0\1		
LOGON/LOGOFF	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	09/01/2022 15:52:30 GMT+1	22/12/2021 23:53:04 GMT+1	09/01/2022 15:53:46 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\1\0\0\2		
MODIFICHE ALL'ORA DI SISTEMA	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	09/01/2022 15:52:30 GMT+1	22/12/2021 23:53:04 GMT+1	09/01/2022 15:53:48 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\1\0\0\3		
PERIFERICHE USB	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	09/01/2022 15:52:30 GMT+1	22/12/2021 23:53:04 GMT+1	09/01/2022 15:53:49 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\1\0\0\0		
	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	19/02/2022 20:49:00 GMT+1	19/02/2022 20:48:52 GMT+1	19/02/2022 20:54:39 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\2\1\0\0\0		
	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	17/12/2021 21:30:38 GMT+1	05/06/2021 12:10:50 GMT+1	10/01/2022 08:18:44 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\3\1\0\0\0		
	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	17/12/2021 22:04:14 GMT+1	24/11/2021 20:33:10 GMT+1	17/12/2021 22:06:21 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\3\1\0\0\1		
	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	17/12/2021 20:29:38 GMT+1	24/11/2021 20:36:04 GMT+1	17/12/2021 22:06:21 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\3\1\0\0\2		
	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	17/12/2021 22:04:38 GMT+1	24/11/2021 20:36:04 GMT+1	17/12/2021 22:06:21 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\3\1\0\0\3		
	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	17/12/2021 21:41:52 GMT+1	24/11/2021 20:37:44 GMT+1	17/12/2021 22:06:21 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\3\1\0\0\0		
REPORT	(My Computer)\C\Program Files (x86)\Windows Defender\Films\resources\audio_effect\yweb_bg_small	17/12/2021 20:29:39 GMT+1	24/11/2021 20:37:44 GMT+1	17/12/2021 22:06:21 GMT+1	HKEY_USERS\5-1-5-21-2817601148-354038585-229292267-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\3\1\0\0\1		

*Figura 9 – Esempio risultato sezione Shellbags*

Questa funzionalità ha lo scopo di determinare tutti gli accessi di un utente ad un PC. Per accesso non si intende l'accensione del PC stesso, ma l'operazione di scelta, ed eventualmente autenticazione, di un account.

La funzionalità di ricerca si basa sui log di sistema. In particolare vengono presi come riferimento gli eventi della categoria “Sicurezza”. Gli eventi in questione sono i seguenti:

ID Evento	Descrizione evento
4624	Un account è stato connesso correttamente.
4647	Disconnessione avviata dall'utente.

Una volta determinati gli eventi, vengono applicati ulteriori filtri agli stessi. Per quanto riguarda la funzionalità di *LogOn* viene applicato un primo filtro sul campo “*Tipo di accesso*” in quanto, altrimenti, ritroveremo sia operazioni effettuate dal sistema che operazioni effettuate dall'utente. Nel nostro caso ci servono solo le operazioni effettuate dall'utente.

Attraverso la documentazione Microsoft, le tipologie di accesso che ci servono sono le seguenti:

- 2: indica che l'utente ha effettuato l'accesso inserendo fisicamente le proprie credenziali attraverso tastiera o schermo collegati al PC.
- 4: il tipo di accesso batch viene utilizzato dai server batch, in cui i processi possono essere esecutori per conto di un utente senza l'intervento diretto.
- 8: un utente ha eseguito l'accesso al computer dalla rete.
- 9: un utente ha clonato il token corrente di autenticazione e specificato nuove credenziali per le connessioni in uscita. La nuova sessione di accesso ha la stessa identità locale ma utilizza credenziali diverse per altre connessioni di rete.
- 10: un utente si è connesso al PC mediante Desktop Remoto o servizi terminal.
- 11: un utente si è connesso al PC attraverso le proprie credenziali collegate ad un account Microsoft.
- 12: un utente si è connesso al PC mediante Desktop Remoto o servizi terminal, utilizzato per il controllo interno.
- 13: accesso workstation.

Queste informazioni appena descritte compaiono anche come *tooltip* tenendo fermo il puntatore del mouse al corrispondente valore della voce della colonna “Tipo di accesso” della tabella dei risultati.

Un ulteriore filtro viene applicato anche al nome dell'utente rilevato dai log. Nello specifico vengono scartati tutti i log in cui il nome utente inizia per “UMFD” e “DWM”



# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

perché si tratta di account fittizi creati da Windows e non corrispondono ad alcun account utente del PC.

La corrispondenza fra un evento di LogOn al relativo evento di LogOff viene stabilita attraverso un ID dell'evento stesso. In altre parole, se un evento di LogOff ha lo stesso ID di un altro evento di LogOn sappiamo l'inizio e la fine di una sessione utente.

Ogni risultato è costituito dai seguenti valori:

- Utente: nome dell'utente che ha effettuato l'accesso. Se l'account del PC è collegato ad un account *Microsoft* leggeremo l'indirizzo *e-mail* dell'account *Microsoft*.
- Dominio: contiene il nome del PC, oppure la scritta "*Microsoft Account*" nel caso di account Microsoft.
- Nome macchina: contiene il nome del PC.
- Data di accesso: la data e ora in cui l'accesso è avvenuto.
- Ora di disconnessione: data e ora di disconnessione.
- Durata: durata della sessione calcolata come differenza fra la data di disconnessione e quella di connessione.
- Indirizzo di rete: contiene l'indirizzo "*127.0.0.1*" se l'accesso è stato effettuato in locale, altrimenti conterrà un altro indirizzo se l'accesso viene effettuato da remoto.

Ad esempio, se tramite *VPN*, viene effettuato un accesso remoto vedremo comparire un indirizzo relativo alla rete privata e non *localhost*.

- Tipo di accesso: mostra il tipo di accesso secondo quanto riportato sopra.



# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Activities Inspector

	Utente	Domínio	Nome macchina	Ora di accesso	Ora di disconnessione	Durata	Indirizzo di rete	Tipo di accesso
ACCENSIONE/SPEGNIMENTO	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	20/2/2022 09:51:26 GMT+1	20/2/2022 11:30:38 GMT+1	0 giorno/i - 1 ora/e - 39 minuti - 12 secondi.	127.0.0.1	Cached interactive (11)
PROGRAMMI INSTALLATI	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	20/2/2022 13:27:20 GMT+1	20/2/2022 17:39:39 GMT+1	0 giorno/i - 4 ore/e - 12 minuti - 19 secondi.	127.0.0.1	Cached interactive (11)
FILE RECENTI	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	20/2/2022 20:35:55 GMT+1	24/2/2022 00:11:04 GMT+1	3 giorno/i - 3 ore/e - 35 minuti - 9 secondi.	127.0.0.1	Cached interactive (11)
PREFETCH	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	24/2/2022 21:21:09 GMT+1	24/2/2022 23:47:16 GMT+1	0 giorno/i - 2 ore/e - 26 minuti - 7 secondi.	127.0.0.1	Cached interactive (11)
SHELLBAGS	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	19/2/2022 12:33:00 GMT+1			127.0.0.1	Cached interactive (11)
LOGON/LOGOFF	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	20/2/2022 01:39:54 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	20/2/2022 09:51:35 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	20/2/2022 13:27:26 GMT+1			127.0.0.1	Cached interactive (11)
MODIFICHE ALL'ORA DI SISTEMA	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	20/2/2022 20:38:44 GMT+1			127.0.0.1	Cached interactive (11)
PERIFERICHE USB	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	21/2/2022 21:20:35 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	22/2/2022 20:26:08 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	23/2/2022 21:12:00 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	24/2/2022 21:21:17 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	25/2/2022 21:53:34 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	25/2/2022 21:53:50 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	26/2/2022 10:40:30 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	26/2/2022 18:06:14 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	26/2/2022 20:30:46 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	27/2/2022 10:30:39 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	27/2/2022 14:28:09 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	27/2/2022 22:27:44 GMT+1			127.0.0.1	Cached interactive (11)
	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	28/2/2022 21:37:20 GMT+1			127.0.0.1	Cached interactive (11)
REPORT	antonio.argentieri@hotmail.it	MicrosoftAccount	MSI	01/3/2022 19:44:01 GMT+1			127.0.0.1	Cached interactive (11)

Figura 10 – Esempio risultato sezione LogOn/LogOff

## Modifiche all'ora di sistema

All'avvio dell'applicazione, il software verifica che l'ora e la data del sistema siano genuine comunicando eventuali manomissioni da parte dell'utente.

Questa operazione è molto importante perché può farci capire se anche i log possono aver subito delle alterazioni riportando dei dati non veritieri.

La verifica delle modifiche a ora e data viene effettuata ricavando l'ora esatta del sistema e confrontando la stessa con l'ora e data restituita dal *server NTP* di Windows (*time.windows.com*).

Effettuando il controllo, nel momento in cui la discrepanza fra i due orari è maggiore di 1 minuto il software rileva che ci sono delle manomissioni riportando il seguente messaggio:

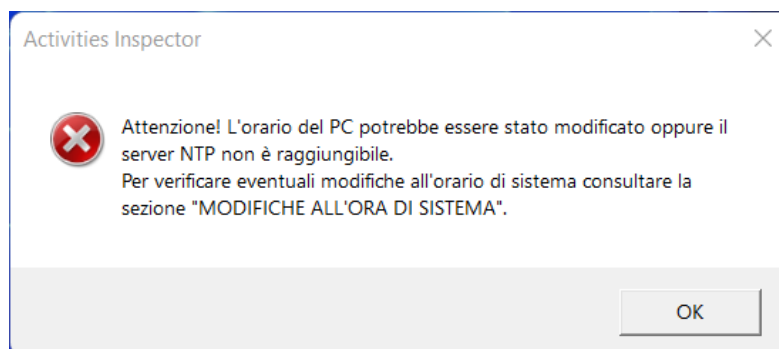


Figura 11 – Warning per possibile alterazione all'ora di sistema



# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Come apprendiamo dallo stesso messaggio, questo tipo di errore ci può essere restituito anche nel momento in cui non è stato possibile interrogare il server NTP perché il PC in questione non è connesso ad Internet oppure ci sono dei problemi sul server stesso.

Per avere la certezza che vi siano state delle manomissioni è possibile recarsi nella sezione "MODIFICHE ALL'ORA DI SISTEMA" in cui è possibile visualizzare tutte le eventuali modifiche manuali dove per modifiche manuali intendiamo tutte le quelle effettuate dall'utente tralasciando quelle che il sistema effettua in automatico.

Per effettuare tale verifica vengono consultati tutti i log con ID 4616 della sezione "Sicurezza".

Questi log, presi nel loro insieme, restituiscono anche tutte le modifiche all'ora che Windows stesso effettua in automatico anche solo per risincronizzarsi col server di riferimento.

Dovendo tener conto solo delle operazioni effettuate dall'utente, il software filtra questi log escludendo tutti quelli che riportano alla voce "Subject\Security ID" il valore "LOCAL SERVICE" e i risultati che alla voce "processo\Nome" riportano il valore "C:\Windows\System32\svchost.exe".

Se la sezione appena citata non presenta alcun risultato allora è molto probabile che non vi siano state alterazioni da parte dell'utente ma semplicemente, non è stato solo possibile effettuare il confronto con il server o che tali log siano stati eliminati dall'utente svuotando il registro eventi.

La tabella dei risultati riporta in questo caso il nome dell'utente che ha fatto l'eventuale modifica, l'ora in cui è stata effettuata l'operazione, l'ora iniziale del PC prima della modifica e l'ora del PC dopo la modifica.



# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Activities Inspector

Esporta Cerca

	Nome utente	Ora evento	Orario precedente	Nuovo orario
ACCENSIONE/SPEGNIMENTO	anton	05/3/2022 15:05:18 GMT+1	05/03/2022 16:05:23 GMT+1	05/03/2022 15:05:18 GMT+1
PROGRAMMI INSTALLATI	anton	07/3/2022 10:36:21 GMT+1	07/03/2022 10:38:25 GMT+1	07/03/2022 10:36:21 GMT+1
FILE RECENTI				
PREFETCH				
SHELLBAGS				
LOGON/LOGOFF				
MODIFICHE ALL'ORA DI SISTEMA				
PERIFERICHE USB				
REPORT				

Figura 12 – Esempio risultato sezione Modifiche all'ora di sistema

## Periferiche USB

La seguente funzionalità riporta tutte le periferiche USB che sono state connesse/rimosse dal PC in questione.

Le periferiche rilevate riguardano chiavette e Hard Disk esterni.

La ricerca delle periferiche USB interroga i log di sistema al percorso *"Microsoft-Windows-DriverFrameworks-UserMode/Operational"* della sezione *"Registri applicazioni e servizi"*:





# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

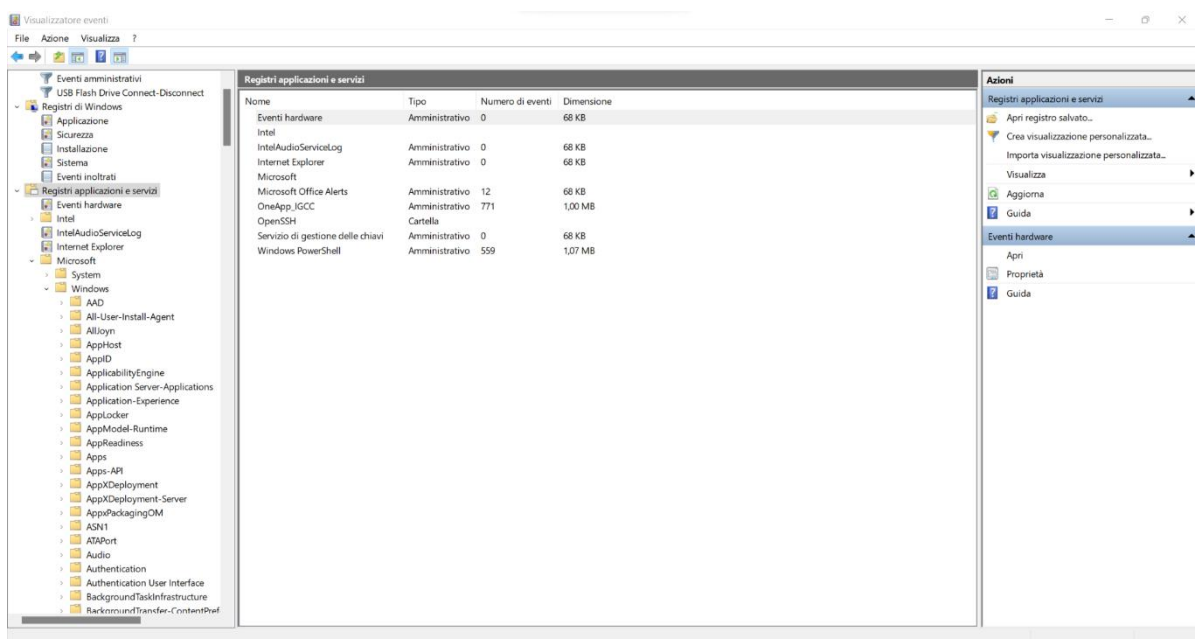


Figura 13 – Sezione eventi Registri applicazioni e servizi

E' molto importante precisare che questo tipo di log sono disabilitati di *default* pertanto, a meno che non vengano espressamente abilitati in precedenza, non sarà possibile recuperare eventuali informazioni circa i dispositivi USB.

Gli ID evento presi in considerazione sono i seguenti:

ID Evento	Descrizione evento
2003	Un dispositivo USB è stato connesso al PC.
2102	Dispositivo USB rimosso dal PC.

Per considerare l'evento di disconnessione corrispondente ad un evento di connessione è sufficiente verificare che i valori del campo *LifetimeId* coincidano. Nel momento il valore di disconnessione relativo ad un evento di inserimento di una periferica non esista, significa che tale periferica è ancora collegata al PC oppure che il PC sia stato spento prima che la periferica sia stata rimossa.



# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

Activities Inspector

Esporta Cerca

	Data inserimento	Data rimozione	Dispositivo	Nome macchina
ACCENSIONE/SPEGNIMENTO	07/03/2022 12:26:56 GMT+1	07/03/2022 12:27:25 GMT+1	SWD(WPDRUSENUM_77 _USBSTORADISK&VEN_SANDISK&PROD_CRUZER_EDGE&REV_1.18&2006 0164401395324ACD&WP3F36307-86BF-11D0-94F2-00A0C91E78BB)	MSI
PROGRAMMI INSTALLATI				
FILE RECENTI				
PREFETCH				
SHELLBAGS				
LOGON/LOGOFF				
MODIFICHE ALL'ORA DI SISTEMA				
PERIFERICHE USB				
REPORT				

Figura 14 – Sezione eventi Registri applicazioni e servizi

## Generazione del report finale

La funzionalità di generazione della reportistica consente di generare un file PDF contenente tutte le informazioni ricercate fino a quel momento.

Per generare il report è sufficiente cliccare l'apposito pulsante situato in basso nella colonna a sinistra dell'interfaccia:




Figura 15 – Pulsante per generazione report PDF

A questo punto si aprirà una nuova finestra in cui sarà necessario inserire tutti i campi relativi all'anagrafica dell'investigatore, descrizione del caso e tipologia di prestazione. Tutti i campi sono obbligatori e devono essere settati al fine di poter procedere alla generazione del documento abilitando automaticamente il pulsante "Genera report".



# UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

 Activities Inspector - Report ×

Investigatore

Cognome

Mario

Nome

Rossi

Qualifica

Ingegnere

Descrizione caso

>Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

☐ CONSULENZA TECNICA D'UFFICIO

☒ CONSULENZA TECNICA DI PARTE

☐ PERIZIA

☐ PARERE PRO VERITATE

☐ Altro:

Genera report

Figura 16 – Finestra per l’inserimento dei dati per la generazione del report

Una volta che tutti i campi risulteranno essere compilati, il pulsante “Genera report” risulterà abilitato. Una volta scelto il percorso in cui salvare il file, sarà possibile avviare la procedura.

A questo punto sarà sufficiente attendere fino al completamento (un apposito messaggio comunicherà l’esito della procedura), il file PDF verrà così generato.