

Artifacts ▾

MATCHING RESULTS 1,846

REFINED RESULTS 15

Facebook URLs 15

WEB RELATED 109

Chrome Cache Records 4

Chrome Downloads 3

Chrome Last Tabs 10

Chrome Web History 16

Chrome Web Visits 76

MEDIA 36

DOCUMENTS 2

OPERATING SYSTEM 1,684

Jump Lists 2

LNK Files 6

Prefetch Files - Windows 8/10 44

Shellbags 2

SRUM Application Resource Usage 492

SRUM Energy Usage 14

SRUM Energy Usage (Long Term) 1

SRUM Network Connections 6

SRUM Network Usage 144

SRUM Push Notification Data 3

System Services 1

Windows Event Logs 953

Windows Event Logs - Networking Events 5

Windows Event Logs - Office Alert Events 4

Windows Event Logs - Service Events 4

Windows Event Logs - Storage Device Events 1

Windows Search - Image 1

Windows Timeline Activity 1

MATCHING RESULTS (953 of 230,688)

Event ID	Event Name	Security Identifier	Created Date/Time	Level	Event Description
12289	LocalSystem		1/17/2023 9:59:33.656 PM	255	Information
12290	LocalSystem		1/17/2023 9:59:33.657 PM	256	Information
12290	LocalSystem		1/17/2023 9:59:33.657 PM	257	Information
811	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 9:59:33.661 PM	525	Information
812	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 9:59:33.662 PM	526	Information
811	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 9:59:33.662 PM	527	Information
812	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 9:59:33.664 PM	528	Information
0			1/17/2023 9:59:33.665 PM	91	Information
12289	LocalSystem		1/17/2023 9:59:33.689 PM	258	Information
12290	LocalSystem		1/17/2023 9:59:33.690 PM	259	Information
12290	LocalSystem		1/17/2023 9:59:33.690 PM	260	Information
12290	LocalSystem		1/17/2023 9:59:33.690 PM	261	Information
12290	LocalSystem		1/17/2023 9:59:33.690 PM	262	Information
11004	LocalSystem		1/17/2023 9:59:36.103 PM	696	Wireless security stopp...
7021			1/17/2023 9:59:36.114 PM	17603	Information
7003			1/17/2023 9:59:36.124 PM	17604	Information
11010	LocalSystem		1/17/2023 9:59:36.131 PM	697	Wireless security started.
11005	LocalSystem		1/17/2023 9:59:36.147 PM	698	Wireless security succe...
50067	LocalService		1/17/2023 9:59:36.151 PM	315	Dhcp has received net...
50065	LocalService		1/17/2023 9:59:36.151 PM	316	Dhcp has found match...
30810	LocalSystem		1/17/2023 9:59:37.318 PM	679	Information
1014	NetworkService		1/17/2023 9:59:41.377 PM	17605	Name resolution timed...
6062			1/17/2023 9:59:51.554 PM	17606	Warning
105	LocalSystem		1/17/2023 10:00:10.388 PM	285	Information
209	LocalSystem		1/17/2023 10:00:10.388 PM	729	Information
209	LocalSystem		1/17/2023 10:00:10.388 PM	730	Information
103	LocalSystem		1/17/2023 10:00:10.405 PM	286	Information
101	LocalSystem		1/17/2023 10:00:10.405 PM	731	Information
40961	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 10:00:13.279 PM	12193	Information
53504	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 10:00:13.326 PM	12194	Information
40962	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 10:00:13.361 PM	12195	Information
3033	LocalSystem		1/17/2023 10:00:23.015 PM	694	Error
3089	LocalSystem		1/17/2023 10:00:23.015 PM	695	Information
3089	LocalSystem		1/17/2023 10:00:23.015 PM	696	Information
3089	LocalSystem		1/17/2023 10:00:23.015 PM	697	Information
40961	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 10:01:13.669 PM	12196	Information
53504	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 10:01:13.719 PM	12197	Information
40962	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 10:01:13.762 PM	12198	Information
28017	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 10:01:54.007 PM	1857	Information
28032	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 10:01:54.060 PM	1858	Information
28117	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 10:01:54.066 PM	1859	Information
28032	S-1-5-21-1038817553-3078799560-1216074279-1001		1/17/2023 10:01:54.084 PM	1860	Information

811

Samsung 1024GB NVME image.E01 - Partition 3 (952.62 GB)_decrypted

DETAILS

ARTIFACT INFORMATION

Event ID 811

Security Identifier S-1-5-21-1038817553-3078799560-1216074279-1001

Created Date/Time 1/17/2023 9:59:33.661 PM

Event Record ID 525

Level Information

Keywords 0x400000000010000

Provider Name Microsoft-Windows-Winlogon

Task Category 811

Computer DESKTOP-DG6QN3J

```

Event Data <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="Microsoft-Windows-Winlogon"
Guid="d8e9b383-7cf3-4331-91cc-a3cb16a3b538" />
<EventID>811</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>811</Task>
<OpCodes>1</OpCode>
<Keywords>0x400000000010000</Keywords>
<TimeCreated
SystemTime="2023-01-18T02:59:33.6616273Z" />
<EventRecordID>525</EventRecordID>
<Correlation />
<Execution ProcessID="908" ThreadID="21048" />
<Channel>Microsoft-Windows-Winlogon/Operational</
Channel>
<Computer>DESKTOP-DG6QN3J</Computer>
<Security
UserID="S-1-5-21-1038817553-3078799560-1216074279-1001" />
</System>
<EventData>
<Data Name="Event">5</Data>
<Data Name="SubscriberName">Sens</Data>
</EventData>
</Event>
    
```

Artifact type Windows Event Logs

Item ID 474388

EVIDENCE INFORMATION

Source Samsung 1024GB NVME image.E01 - Partition 3 (952.62 GB)_decrypted.img - Entire Disk (Microsoft NTFS, 952.62 GB) Windows-SSD\Windows\System32\winevt\Logs\Microsoft-Windows-Winlogon%4Operational.evtx

Recovery method Parsing

Deleted source

Location File Offset 219604